METODOLOGIA PARA LA EVALUACION DEL CUMPLIMIENTO Y EL RIESGO ASOCIADOS A LA GESTION DE LA INFORMACION EN ENTIDADES DEL SECTOR PÚBLICO MEDIANTE LA AUDITORIA DE SISTEMAS

JUAN CARLOS ANGARITA CASTELLANOS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO MECÁNICAS
ESCUELA DE INGENIERIA DE SISTEMAS
BUCARAMANGA
2012

METODOLOGIA PARA LA EVALUACION DEL CUMPLIMIENTO Y EL RIESGO ASOCIADOS A LA GESTION DE LA INFORMACION EN ENTIDADES DEL SECTOR PÚBLICO MEDIANTE LA AUDITORIA DE SISTEMAS

JUAN CARLOS ANGARITA CASTELLANOS

Trabajo de grado presentado como requisito para optar al título de MAGISTER EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

Director
FERNANDO ROJAS
INGENIERO DE SISTEMAS, M.Sc.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO MECÁNICAS
ESCUELA DE INGENIERIA DE SISTEMAS
BUCARAMANGA
2012

DEDICATORIA

Este trabajo está dedicado, en su orden a:

- Dios, el gran arquitecto del universo, por el privilegio de la inteligencia, la creatividad y la perseverancia;
- Mis padres Carlos y Carmen Lucila, por su constante apoyo y guía;
- Mi amada esposa María Ximena, por su incalculable afecto, incondicional apoyo y la confianza depositada aún en los momentos difíciles;
- Mis hermosas hijas Sara Camila, María Fernanda y Daniela, quienes con su sonrisa y cariño especial son la más grande motivación para seguir luchando;
- Mi director y guía técnico-espiritual, Fernando, a quien agradezco no solo sus buenas ideas y oficios en el desarrollo de este trabajo, también el proporcionar ánimo, pautas y empuje para el desarrollo de éste y muchos otros proyectos, incluyendo el ánimo a seguir creciendo como investigador;

AGRADECIMIENTOS

El autor, se permite ofrecer agradecimientos al cuerpo docente y administrativo de la Universidad Industrial de Santander, principalmente en la escuela de Ingeniería de Sistemas – Programa de maestría en ingeniería área informática y ciencias de la computación, con especial mención a mi director de trabajo, el profesor Fernando Rojas, a mis docentes de maestría, los jurados asignados tanto en la aprobación del plan de trabajo como del trabajo final de investigación, a la directora de la maestría, por su amplia colaboración, apoyo y acompañamiento.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ADMINISTRACIÓN DEL RIESGO: Actividades dirigidas a dirigir una organización frente a sus riesgos.

AMENAZA: Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

ANÁLISIS DE RIESGOS: uso sistemático de información para identificar fuentes de riesgo y para estimar el riesgo.

CONSECUENCIA: Resultado de un evento (de riesgo)

CUMPLIMIENTO: Indica el grado de implementación de las exigencias aplicables a una organización.

EVENTO: Ocurrencia de un conjunto particular de circunstancias.

FUENTE: Elemento o actividad que posee un potencial para generar una consecuencia.

GESTIÓN DEL RIESGO: Actividades enfocadas a identificar, caracterizar, cuantificar y analizar el riesgo para establecer elementos de control y mitigación.

GRUPOS DE INTERÉS: Cualquier individuo, grupo u organización que puede verse o sentirse afectada por un riesgo.

IMPACTO: consecuencia de la materialización de una amenaza.

PROBABILIDAD: Extensión en la cual un evento (de riesgo) puede suceder.

RIESGO: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

VULNERABILIDAD: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

TÉCNICA: es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad.

INFORMÁTICA: es la tecnología que estudia el tratamiento de la información mediante el uso de máquinas automáticas. Entre las tareas más populares que ha facilitado esta tecnología se encuentran: elaborar documentos, enviar y recibir correo electrónico, dibujar, crear efectos visuales y sonoros, maquetar folletos y libros, manejar la información contable en una empresa, reproducir música, controlar procesos industriales y jugar.

NORMA TÉCNICA: Documento formal dictado por una autoridad competente mediante el cual se establece lineamientos, exigencias y deberes sin plantear una metodología para el logro de tales requerimientos.

TECNOLOGÍA DE LA INFORMACIÓN: Hace referencia al procesamiento, el almacenamiento y la transmisión de información, e incluye entonces la tecnología de los computadores y las diferentes tecnologías de comunicación.

RESUMEN EN ESPAÑOL

TITULO METODOLOGIA PARA LA EVALUACION DEL CUMPLIMIENTO Y EL RIESGO ASOCIADOS A LA GESTION DE LA INFORMACION EN ENTIDADES DEL SECTOR PÚBLICO MEDIANTE LA AUDITORIA DE SISTEMAS. *

AUTOR JUAN CARLOS ANGARITA CASTELLANOS **

PALABRAS CLAVE AUDITORIA, CUMPLIMIENTO, INFORMACIÓN, NORMATIVIDAD, RIESGO, OBLIGATORIEDAD

El concepto de cumplimiento se desarrolla sobre el de obligatoriedad, es decir, el conjunto de aspectos exigidos por una autoridad – privada o pública – a través de un ejercicio normativo o contractual, de manera directa o delegada, en ámbitos nacionales e incluso regionales, sobre un grupo específico o determinado de organizaciones según su naturaleza jurídica, actividad socio económica y entorno en el cual se desarrolla.

La gestión del cumplimiento en las organizaciones actuales en términos de información enfrenta un número creciente de autoridades, privadas y públicas, que realizan actividades regulatorias y normativas, a nivel nacional y supranacional, así como un extenso universo de normas legales, técnicas y regulatorias, incluyendo especificaciones técnicas y mejores prácticas, aplicables a la forma de hacer y de entregar productos y servicios. Además, existe un mejor ejercicio de regulación, vigilancia y control por parte del estado, entes delegados y entidades supranacionales, frente a numerosos escándalos corporativos de gran impacto social y económico.

Los anteriores aspectos adquieren mayor complejidad al considerar las características de la información y los procesos asociados al cumplimiento, los cuales impactan los procesos misionales y participan dentro de los procesos estratégicos institucionales, en términos de complejidad, heterogeneidad, volumen, credibilidad, integridad, seguridad, disponibilidad y autenticidad de la información.

Por lo tanto, las organizaciones necesitan metodologías, métodos y herramientas técnicas para evaluar el grado de cumplimiento frente a las obligaciones normativas, regulatorias, técnicas y contractuales que le sean aplicables, haciendo de la evaluación del cumplimiento y su riesgo asociado, un área crítica a nivel empresarial, de continua investigación, desarrollo e innovación.

---

* Trabajo de investigación (tesis)

** Facultad de ingenierías físico mecánicas, Escuela de Ingeniería de Sistemas, Director: Ing. Fernando Rojas (UIS)

RESUMEN EN INGLÉS

TITULO METODOLOGIA PARA LA EVALUACION DEL CUMPLIMIENTO Y EL RIESGO ASOCIADOS A LA GESTION DE LA INFORMACION EN ENTIDADES DEL SECTOR PÚBLICO MEDIANTE LA AUDITORIA DE SISTEMAS. *

AUTOR JUAN CARLOS ANGARITA CASTELLANOS **

PALABRAS CLAVE AUDITORIA, CUMPLIMIENTO, INFORMACIÓN, NORMATIVIDAD, RIESGO, OBLIGATORIEDAD

The compliance concept is built over the concept of mandatory, making reference to those aspects required by a public or private authority through a normative or contractual structure, using direct or delegated mechanisms, at national or supranational scope, applicable in a general or specific manner over some organizations depending on its legal nature, business activity or environment.

The compliance management in current organizations, in IT, faces a growing number of authorities, public and private, who make normative and regulatory activities, at legal, technical and regulatory levels, including technical specifications and best practices, about how to do and deliver products and services. Beyond that, there is a better surveillance and control function performed by the state, its delegated entities as well as supranational organisms, trying to avoid new corporate scandals having great social and/or economic impact.

Those aspects acquire bigger complexity considering information features and the process which are related to compliance, which directly impact business mission objectives making part of strategic process in the organization, in terms of how complex, heterogeneous, volume, credibility, integrity, security, availability and authenticity is the information.

Therefore, nowadays organizations need methodologies, methods and technical tools designed to assess the compliance level considering the normative, technical, regulatory and contractual obligations, making the compliance management a critical business area, demanding continuous research and development.

---

* Trabajo de investigación (tesis)

** Facultad de ingenierías físico mecánicas, Escuela de Ingeniería de Sistemas, Director: Ing. Fernando Rojas (UIS)

INTRODUCCION

El concepto de cumplimiento está íntimamente ligado al de obligatoriedad, expresión que además de expresar algo obligado, igualmente plantea la existencia de una autoridad que establece el aspecto obligatorio y exige de manera directa o delegada su cumplimiento. En el ámbito empresarial, los aspectos obligatorios se expresan en términos normativos o contractuales, generando obligaciones y la necesidad del cumplimiento.

La necesidad del cumplimiento en las organizaciones se ha visto incrementada de forma dramática en los últimos años debido a un creciente número de autoridades que realizan actividades regulatorias y normativas, a nivel nacional y supranacional; la dinámica legal y técnica de los mercados; un extenso universo de diversas normas legales, regulaciones y técnicas[1], incluyendo especificaciones técnicas y mejores prácticas, aplicables a la forma de hacer y de entregar productos y servicios, o realizar procesos, las cuales son exigibles según el sector socio económico en el cual opere la organización; un mejor ejercicio de regulación, vigilancia y control por parte del estado, entes delegados y organismos supranacionales; y los numerosos escándalos corporativos de gran impacto social y económico; espacios donde la mayor exigencia y responsabilidad reposa sobre la gestión adecuada de la información.

Los anteriores aspectos adquieren mayor complejidad al considerar las características y retos propios de la información así como los procesos asociados al cumplimiento, los cuales impactan los procesos misionales y participan dentro de los procesos estratégicos institucionales.

[1] Norma, es sinónimo de mandato, de regla, de actuación y la norma jurídica puede ser definida como precepto general cuyo fin es ordenar la convivencia social, y cuya realización puede ser impuesta coacti vamente por el poder correspondiente. DE CASTRO Y BRAVO, F.: Derecho civil de España, t. I, Instituto de Estudios Políticos, Madrid, 1955.

Es tan amplio el impacto del cumplimiento en tecnologías de la información que solo por concepto de herramientas tecnológicas insuficientes para lograr las metas institucionales y cumplir con las exigencias aplicables, en la tercera conferencia internacional en gobernabilidad, riesgo y cumplimiento y su aplicación en los sistemas de información[2], en Túnez, se estableció que el mercado global de gobernabilidad, riesgo y cumplimiento supera los 32 billones de dólares.

Lo anterior conlleva a concluir que las organizaciones necesitan metodologías, métodos y herramientas técnicas para evaluar el grado de cumplimiento frente a las obligaciones normativas, regulatorias, técnicas y contractuales que le sean aplicables, haciendo de la evaluación del cumplimiento y su riesgo asociado, un área crítica a nivel empresarial, de continua investigación, desarrollo e innovación.

La gestión del cumplimiento trae necesariamente la necesidad de una metodología formal que basada en la gestión del riesgo, apoye la evaluación y control del seguimiento en organismos públicos dentro de la función relacionada con Tecnología de Información y de las comunicaciones.

[2] ONTOLOGY RESEARCH. 3rd International Workshop on Governance Risk and Compliance – Applications in Information Systems (GRCIS'10). Hammamet, Tunisia: http://ontology-research.com/2010/01/international-workshop-on-governance-risk-and-compliance-caise2010/, 2010

1. TEORIA DE LA INFORMACION Y LAS COMUNICACIÓNES

La comunicación, del latín *communis* o común[3], según la Real Academia de la Lengua, corresponde a la transmisión de señales mediante el uso de un código común al emisor y al receptor[4], siendo tales señales un conjunto de símbolos y sistemas de mensajes que se intercambian de una entidad a otra[5].

La teoría de la comunicación aparece con Aristóteles en su obra La Retórica (Tratado Ars Rhetorica)[6] con un modelo de tres elementos (Fuente – Mensaje – Destinatario); Nyquist (1924) y Hartley (1928), posteriormente, al analizar el flujo de datos en redes telegráficas, sentaron las bases teóricas del canal de datos en comunicaciones[7] [8]; Shannon y Weaver (1949), describieron el proceso general para la comunicación usando un modelo que añade tres componentes adicionales (Transmisor – Receptor – Ruido o interferencia)[9] dando nacimiento a la teoría de la información[10] la cual se define como la ciencia de la compresión, almacenamiento y transmisión de información; Schramm (1954) introdujo un concepto adicional sobre el contexto y la conducta cíclica del proceso comunicativo a través de la realimentación[11] lo cual fue complementado por Goffman (1959) y Lanham (2003) al introducir la necesidad de no separar el contexto de la información[12] [13].

[3] http://etimologias.dechile.net
[4] www.rae.es
[5] FERRER, Eulalio. Información y comunicación. México, Fondo de Cultura Económica. 1997
[6] ARISTOTLE.. Retorica. Gredos. 1997
[7] NYQUIST, Harry. Certain Factors Affecting Telegraph Speed. 1924
[8] HARTLEY, Ralph. Transmission of Information. 1928
[9] SHANNON, C.. WEAVER, W. The mathematical theory of communication. . Urbana, IL: University of Illinois Press. 1949
[10] WEISSMAN, Tachy. Nformation Theory. Stanford University. 2010
[11] SCHRAMM, W.. How communication works. In W. Schramm (Ed.), The process and effects of mass communication. Urbana, IL: University of Illinois Press. 1954
[12] GOFFMAN, Erwin. The Presentation of Self in Everyday Life. New York, NY: Doubleday, 1959. 73
[13] LANHAM, Richard. Analyzing Prose' 2nd (2003): 7, 10

1.1. EL MENSAJE

Del latín tardío *messàgium* o *missàgium*, basado en *missus*, participio del verbo *mittere*[14], mandar. El mensaje es el objeto de la comunicación y corresponde a la información - o conjunto de elementos informativos - plasmada en el documento, de forma independiente al canal (soporte) y código (lenguaje) empleados, la cual el emisor envía al receptor a través de un canal determinado o medio de comunicación, con influencia del contexto, tanto lingüístico (la presentación del mensaje y los símbolos utilizados para transmitir el mensaje), como social (respecto a los paradigmas propios del receptor quien interpreta el mensaje recibido) o geográfico (que relaciona la información con su entorno). Por lo tanto, es sólo a través del mensaje que el fenómeno comunicativo puede generarse ya que de otro modo no se estaría estableciendo necesariamente conexión alguna.[15]

1.2. EL CODIGO

Del latín *codicillus*, codex, conjunto de reglas[16], el concepto de código corresponde al grupo de reglas que permite formular y comprender un mensaje[17] y en el cual se basa la codificación de la información intercambiada entre la fuente (el emisor) y el destino (el receptor) de un lazo informático, que implica (a) el reconocimiento y comprensión del significado y la estructura del código por quienes intervienen en el proceso comunicativo[18], (b) la existencia de mecanismos de control y/o verificación del mensaje codificado, (c) la posible sucesiva codificación en diversos sistemas de codificación, en especial ámbitos informáticos, donde es factible la conversión a ciertos formatos de datos, la posterior compresión de datos, encripción, etc..

---

[14] http://etimologias.dechile.net
[15] LITTLEJOHN, S. W.,Theories of human communication. 7th edition, Belmont, CA: Wadsworth, 2002
[16] http://etimologias.dechile.net
[17] www.rae.es
[18] SUÁREZ, Yadira. La comunicación y las relaciones públicas. Universidad Camagüey. Cuba. 2006

1.2.1. El símbolo. Del latín *symbŏlum*[19] que proviene del griego *σύμβολον* que deriva del verbo συμβαλλειν, compuesto por los términos *συμ* (junto) y βαλλειν (lanzar/arrojar). Su definición etimológica habla del símbolo como objeto, partido en dos, que portan dos personas, de forma que éstas se reconozcan entre sí, que lleva al acuerdo actual de usar símbolos comunes, compartidos y conocidos por las partes, de modo que el símbolo expresa una idea concreta o abstracta, que es reconocible y entendible por las partes con mínima –nula – distorsión del mensaje.

La evolución del símbolo ha seguido el desarrollo tecnológico humano, partiendo de semejanzas, reales o imaginadas, con lo significado, como los pictogramas egipcios o ideogramas chinos, hasta llegar a expresiones idiomáticas donde se simbolizan conceptos usando complejos conjuntos de símbolos abstractos unidos siguiendo reglas semánticas relacionadas con la simbología elegida y estructuras informáticas codificadas usando normas de índole técnico, expresadas comúnmente en formatos de flujos de datos accesibles mediante diversas herramientas, incluyendo las de software, preparadas para decodificar formatos específicos según el tipo de archivo o el flujo de datos y la tecnología aplicable. A lo anterior puede sumarse procesos adicionales como la compresión o la encripción de datos, usados desde la antigüedad.

1.2.2. El signo. Del latín *signum*, marca o seña, implica la definición de significado o seguimiento. Debe diferenciarse el signo del símbolo. Los primeros "significan", “señalan”, sirven como referentes o imágenes de una cosa siendo específicos de un cometido o una circunstancia; mientras los segundos, a más de significar, "simbolizan", trasmiten un mensaje que constituye la idea simbolizada por el símbolo, mensaje que constituye su simbolismo, pudiendo estar constituidos por signos. En el caso informático, los signos tienen su expresión en las expresiones binarias y representación en juegos de caracteres, como ASCII[20] o el Unicode[21].

[19] http://etimologias.dechile.net
[20] **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange o ANSI_X3.4-1968

1.3. EL CANAL

Conducto, soporte o medio por el cual circula el mensaje[22] estableciendo una conexión entre el emisor y el receptor. Cuando la comunicación es interpersonal - entre personas y sin ningún medio electrónico de por medio – el canal mantiene su nombre, pero cuando la comunicación se realiza por medio de artefactos o instancias artificiales, o electrónicas, al canal se le denomina Medio. El canal, o medio, puede ser continuo cuando existe o bien un emisor transmitiendo información o un receptor a la escucha de la misma, o temporal si el canal – o medio – se establece de forma explícita y finita entre las partes.

1.4. EL DOCUMENTO

Un documento es todo objeto que ofrece información. Su origen etimológico deriva de la palabra latina "*docere*" que significa "enseñar". Al respecto, diversos autores lo definen como "todo escrito que sirve de prueba o información"[23], "elemento de conocimiento o fuente de información registrada, materialmente susceptible de usarse para consulta, estudio o prueba"[24], "todo mensaje - icónico o simbólico - incorporado a un soporte y empleado con finalidad informativa"[25], “información registrada la cual puede ser tratada como una unidad”[26], “Información registrada, cualquiera que sea su forma o el medio utilizado”[27], “todo objeto mueble que tenga carácter representativo o declarativo”[28] así como "información registrada que puede considerarse como unidad en un proceso de documentación"[29] entendiendo

---

[21] ISO/IEC 10646
[22] www.rae.es
[23] Diccionario Robert
[24] Union Française d'Organismes de Documentation
[25] Martínez Comenche
[26] ISO 15489-1
[27] Acuerdo 027 de 2006 expedido por el Archivo General de la Nación (Colombia)
[28] Código de Procedimiento Civil (Colombia) Art. 251
[29] Norma UNE 50-113-92/1

la documentación como el proceso de "recogida y tratamiento de información registrada, de forma continua y sistemática y que permita su almacenamiento, recuperación, utilización y transmisión" y gestión documental como “actividades administrativas y técnicas, tendientes a planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final con el objeto de facilitar su utilización y conservación”[30] donde resalta la presencia de información en la forma de mensaje, el uso de un soporte - no necesariamente material - sobre el cual se plasma el mensaje para conformar un documento, la presencia de símbolos que hacen parte de un lenguaje a través de los cuales se codifica el mensaje, la autoría del documento expresada en la referencia a los nombres de sus autores y algún mecanismo de “firma” que sustente su originalidad (como el caso de certificados informáticos), la fecha de producción explícita o referenciable y el contexto, usualmente expresado en la locación en la cual fue producido el documento. La noción de documento ha estado unida a la de escrito, donde el concepto de escritura ha adquirido una perspectiva más amplia y es denominado documento a la conjunción de cualquier tipo de material susceptible de vehicular información.

1.4.1. El soporte. El soporte documental (canal de información) se tiene como el medio en el cual se contiene la información, según los materiales empleados.

Con base en el concepto de soporte, Martín Vega[31] plantea que todo documento incluye tres tipos de componentes:

a) Componentes físicos o materiales. Todo documento se asienta en una determinada clase de soporte ofreciendo cualidades de peso, tamaño, sustancia material, etc., así sean éstos análogos o digitales (finalmente los medios de almacenamiento son físicos)

[30] Ley 594 de 2000, Ley General de Archivos (Colombia)
[31] MARTÍN VEGA, A. Fuentes de información general. Gijón: TREA. 1995.

b) Componentes formales. Los documentos adquieren una estructura. La materia básica que los sustenta se dispone de cierta manera (grabando sobre piedra, dando forma gráfica con la tinta, digitalizando datos en un ordenador...) para mostrar un contenido, adquirir un sentido, tener un significado, transmitir un conocimiento.

c) Componentes conceptuales. Todos los documentos proporcionan un significado.

De igual manera, López Yepes[32] plantea que el documento tiene una triple dimensión, que sirve para fijar su tipología:

a) Soporte físico. La fijación del mensaje en un soporte permite, precisamente, que ese contenido pueda ser recuperado y reutilizado por el usuario, hecho que facilitan las unidades informativas al someter los documentos al proceso informativo-documental.

b) Mensaje informativo.

c) Posibilidad de transmisión o difusión del conocimiento sustentado en el documento y actualizado en el proceso documental.

1.4.2. Documentos analógicos y documentos digitales. Codina[33] plantea la oposición entre medios analógicos y medios digitales, sin importar que sean audiovisuales o bibliográficos, es decir, entre átomos y bits según Negroponte[34]. No obstante, se debe señalar que los adjetivos “electrónico”, “informático” y

[32] LÓPEZ YEPES, J. Teoría de la documentación. Pamplona: EUNSA, 1978
[33] CODINA, L. El libro digital y la WWW. Madrid: Tauro, 2000
[34] NEGROPONTE, N. El mundo digital. Barcelona: Ediciones B., 1995

"digital" también se intercambian[35], llegando a ser común incluso la referencia a "magnético" u "óptico" vinculando el documento a su tradición de soporte; así como los documentos que suelen llamarse "impresos", "físicos" o analógicos.

El concepto de documento digital es amplio y engloba al documento digital o informático (relativo a sistemas de información) y al audiovisual, mientras que el análogo reúne al físico e impreso. Lo que caracteriza a los medios analógicos es que representan la información mediante una relación de parecido o de analogía: se mantiene cierta semejanza entre la información y su codificación, aunque sea remota. En cambio, en los medios digitales, que utilizan bits para representar la información, cualquier semejanza entre información y representación está dada (representada) por series de ceros y unos.

En los medios analógicos, sin embargo, cada morfología o código y cada soporte exige una forma de codificación propia. De hecho, ningún soporte analógico resulta adecuado para todas las morfologías de la información. Por el contrario, los medios digitales pueden contener cualquier morfología de la información y cualquier combinación entre ellas. El documento digital, según Schamber[36], como características peculiares: es manipulable, es enlazable interna y externamente, es rápidamente transformable, es ágil y fácilmente accesible, instantáneamente transportable e infinitamente replicable.

De estas características se deduce que la gran diferencia de los documentos digitales frente a los analógicos estriba en que en ellos se produce una disociación entre soporte y el contenido. Las peculiaridades listadas por Schamber se refieren a los contenidos, los soportes han perdido relevancia, de hecho, los mensajes que

[35] RODRÍGUEZ BRAVO, Blanca. REVISIÓN DE LAS CLASIFICACIONES DOCUMENTALES BASADAS EN EL SOPORTE. Área de Biblioteconomía y Documentación. Facultad de Filosofía y Letras. Universidad de León. correo-e: dphbrb@unileon.es. 17-1-2002.

[36] SCHAMBER, L.. What is a document? Rethinking the concept in uneasy times. Journal of the American Society for Information Science, 1996, vol. 47, n. 9, p. 669-671

contienen se copian con facilidad en otro soporte volviéndolos transformables, manipulables y transportables. Este aspecto es lo que el legislador colombiano ha identificado en la Ley 527 de 1999 al tratar los mensajes de datos y otorgarles calidad probatoria al igual que el soporte tradicional.

La separación entre contenido y soporte hace que estos documentos sean compuestos (distintos códigos), distribuidos (en varios archivos) y dinámicos (fácilmente modificables). De allí surgen las posibilidades que ofrecen: capacidad de almacenamiento, actualización, virtualidad y accesibilidad a distancia; así como la dificultad para preservarlos y garantizar su integridad y autenticidad. La facilidad que tienen los mensajes para cambiar de soporte y su fácil manipulación son el origen tanto de sus ventajas como de sus inconvenientes.

De esa manera, Sagredo[37] distingue en función de su materialidad y de la intermediación para acceder a su contenido, tres tipos de documentos que denomina, real, irreal y virtual:

a) El documento real es aquél con un soporte material sobre el que se inscribe o reposa un documento decodificable directamente por los sentidos. El documento bibliográfico, que surge con la aparición de la escritura, sería el documento real por excelencia.

b) El documento irreal cuenta con un soporte material pero el usuario no puede acceder directamente a la información contenida, necesita la intermediación de dispositivos de lectura. Incluye los soportes utilizados desde finales del siglo XIX (el microfilm), las diapositivas, los discos, casetes, vídeos y también los disquetes, el CD-ROM y el DVD.

[37] SAGREDO FERNÁNDEZ, F. Documento y sistema virtual. En TRAMULLAS, J. (ed.), Tendencias de investigación en Documentación, Zaragoza: 1996, p. 9-17

c) El documento virtual aquél del cual no se dispone in situ, ni del soporte tangible, ni del mensaje, y que para acceder a este último se necesita de periféricos, comunicaciones y recursos adecuados que permitan entrar en cualquier momento en el depósito irreal, donde se conservan todos los documentos.

Estos documentos virtuales, accesibles y manipulables a distancia por procedimientos en línea y en tiempo real, son fácilmente copiables, con lo que con el mismo contenido se obtendría un documento tangible - irreal -, o tangible y decodificable directamente - real -.

Como plantea Sagredo, el documento virtual está en potencia en todos y cada uno de los repositorios de información (bases de datos, Internet…), con la peculiaridad que a partir de él el usuario puede crear un nuevo ejemplar documental, que a su vez puede ser almacenado, y así sucesivamente. El usuario se puede convertir en creador y emisor en el proceso informativo documental, ventaja indudable, teniendo como contrapartida la poca permanencia del documento hasta ahora garantía referencial última.

Con base en lo anterior y los planteamientos de Codina así como los de Sagredo y Rodríguez, se tienen cuatro criterios de clasificación según su combinación:

a) Que exista analogía entre la información y su codificación, lo que divide a los documentos en analógicos y digitales.

b) Que su soporte permita descifrar el mensaje directamente por los sentidos, o necesite mediar con aparatos. Este criterio diferencia al documento bibliográfico de los demás.

c) Que su soporte sea tangible o intangible. En este caso es el documento digital que se transmite por Internet (intangible) el que se distingue de los restantes.

d) Que su soporte sea estable o inestable. La estabilidad del soporte ha disminuido con la evolución de los tipos documentales.

Lo cual conlleva a obtener la siguiente clasificación:

a) Documentos analógicos directamente decodificables: documentos bibliográficos y gráficos que no necesitan aparatos mediadores para acceder a su mensaje. Su soporte es el papel o similares de tipo físico, soporte tangible y estable.

b) Documentos analógicos no decodificables por los sentidos directamente sino a través de aparatos de lectura: diapositivas, vídeos, discos, microfilm… Su soporte es tangible y medianamente estable.

c) Documentos digitales con soporte tangible pero no de lectura directa, necesita de un computador y dispositivos lectores (CD-ROM, DVD o BlueRay). La estabilidad del soporte es también mediana.

d) Documentos digitales con soporte intangible, el documento virtual, que no se decodifica directamente, también necesitado de computador y conexión a la red en este caso. Son los documentos que circulan por Internet, y son muy inestables.

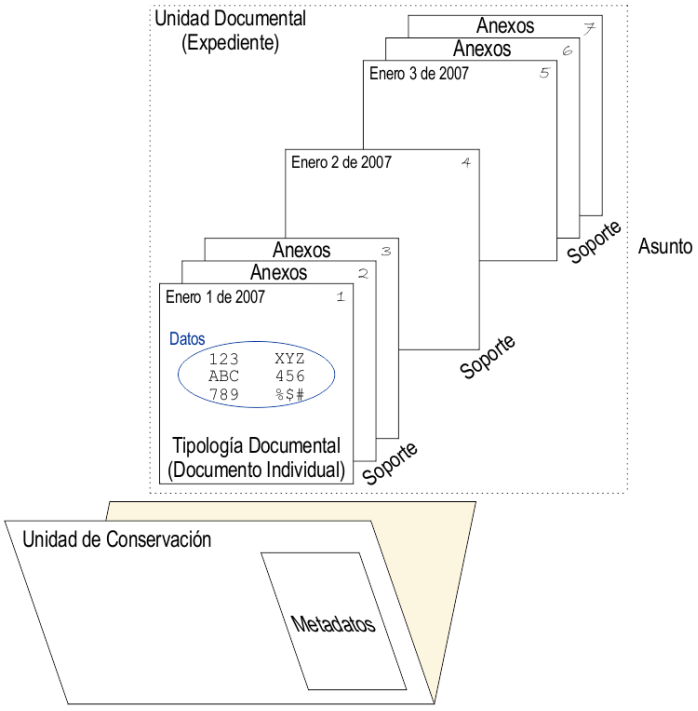
1.4.3. Unidades documentales. La ejecución de un procedimiento o actividad formal (en una organización) o de una tarea informal, en cada una de sus ocurrencias - o asunto -, puede producir un único documento o grupo de documentos que conforman el resultado del ejercicio realizado y evidencian los diversos pasos recorridos para el desarrollo de tal emprendimiento, sin importar que los documentos que le integran puedan ser analógicos o digitales.

Tal conjunto de documentos producidos o recibidos en el desarrollo de un único asunto conforman la unidad documental: unidad de análisis en la identificación y caracterización documental. La unidad documental puede ser simple, si está constituida por un solo tipo documental, o compleja, cuando la constituyen varios, formando un expediente[38] el cual es aquella unidad documental compleja formada por un conjunto de documentos, y sus anexos, generados orgánica y funcionalmente por un ente productor en la resolución de un mismo asunto, donde pueden participar varias personas produciendo documentos. Lo anterior posiciona al documento como resultado más que como un medio (al considerar al documento por si solo) incorporando el contexto del asunto por el cual fue producido.

Considerando el carácter probatorio que exhiben los documentos (Los aportados por las partes para ser incorporados en un expediente judicial - con fines probatorios - se reputarán auténticos, sin presentación personal ni autenticación, sin perjuicio de los documentos emanados de terceros[39]) incluyendo los de tipo digital (Los mensajes de datos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Capítulo VII del Título XIII del Código de Procedimiento Civil Colombiano[40]), la Las buenas prácticas en materia documental y archivística exigen la aplicación de los principios de Procedencia y de Orden original[41], definidos como “los documentos producidos por una institución y sus dependencias, en ejercicio de un asunto, no deben mezclarse con los de otras” y “la disposición física de los documentos debe respetar la secuencia de los trámites que los produjo” respectivamente.

[38] Acuerdo 027 de 2006, emitido por el Archivo General de la Nación (Colombia)
[39] Ley 446 de 1998 (Colombia) Art. 11 sobre el principio de autenticidad
[40] Ley 527 de 1999 (Colombia) sobre mensajes de datos electrónicos
[41] Ley 594 de 2000 (Colombia)

Figura 1. Integración de conceptos documentales



Fuente: ANGARITA, Juan Carlos. Diplomado de Gestión Documental. Solutions. Bucaramanga, 2007

1.5. LOS METADATOS

Los metadatos se definen como los datos sobre los datos[42], o específicamente aquellos datos que describen el contexto, contenido y estructura de registros y su gestión a través del tiempo[43] así como recursos y servicios asociados[44] para resolver preguntas como[45]:

- El qué: Nombre y descripción del dato.
- El quién: Creador y administrador de los datos.

[42] ISO 19115
[43] ISO 15489-1:2001
[44] ISO. Introduccion a la normalización Geográfica: La familia ISO 19100
[45] SHANKARANARAYAN G., ZIAD, M., WANG, R., Managing Data Quality in dinamyc decision environments. Journal of database management 14. 2003. 14-32

- El cuándo: Fecha de creación (datos), actualización, validez, vigencia…
- El dónde: Extensión geográfica, contexto
- El cómo: Modo de obtención del dato, calidad, formato o estructura de datos.
- El con qué: Recursos y servicios asociados.

El FGDC[46] reconoce que la creación de metadatos - geográficos - persigue tres objetivos (y a su vez beneficios) principales:

a) Organizar y mantener la inversión en datos hecha por una organización: los metadatos buscan fomentar la reusabilidad de datos sin tener que recurrir al equipo humano que se encargó de su creación inicial. Aunque la creación de metadatos parezca un coste adicional, el valor de los datos a la larga es dependiente de su documentación.

b) Publicitar la existencia de información: Al publicar recursos de información disponibles a través de un catálogo de metadatos, las organizaciones pueden encontrar datos a usar, otras organizaciones con las que compartir datos y esfuerzos de mantenimiento y clientes para esos datos. En general, permiten a los usuarios utilizar los datos de un modo más eficiente, determinando si serán de utilidad para ellos.

c) Proporcionar información que ayude a la transferencia de datos: los metadatos deberían acompañar siempre a los datos. Los metadatos facilitan el acceso a los datos, su adquisición y su mejor utilización logrando una interoperabilidad de la información cuando esta procede de fuentes diversas, como base para la gestión de flujos de datos como mensajes o paquetes de información. Los metadatos ayudan al usuario u organización que los recibe en procesamiento, interpretación, y el almacenamiento de los datos en repositorios internos.

[46] FEDERAL GEOGRAPHIC DATA COMMITTEE. Content Standard for Digital Geospatial Metadata (FGDC-STD-001-1998). Federal Geographic Data Committee. Washington. 1998

La utilidad expresada por el FGDC redunda sobre la necesidad de acceder fácilmente a la información pues no basta con tener a la mano documentos (con los datos allí contenidos) dada la cantidad abrumadora de documentos de la mano de una alta dispersión, así como la complejidad y diversidad de formatos y expresiones, lo cual se traduce en una costosa y difícil recuperación de información si la búsqueda se realiza de forma iterativa o lineal, uno a uno, explorando su contenido, para determinar su uso y aplicación.

1.6. EL CONTEXTO

La palabra contexto viene de las raíces latinas *cum* (con) y *texere* (tejer, fabricar), sugiriendo un entretejido[47] siendo la raíz texere también el origen de las palabras texto y tecnología. El contexto reúne el significado de un mensaje (como una oración), su relación a otras partes del mensaje (como un libro), el ambiente en el cual la comunicación ocurrió, y cualquier percepción que pueda ser asociada con la comunicación[48].

El contexto modela el contenido de un documento y, análogamente, el contenido implica un contexto. No hay información sin contexto[49], sin embargo, es común observar que la fascinación por la forma del contenido y el dato en sí, sesga este equilibrio hacia el lado de la información, sin necesariamente aumentarla.

En la práctica, cuando hay problemas de información, tenemos que agregar más información. Sin embargo, según Brown y Duguid, la historia de la documentación y de la humanidad misma se ha desarrollado en la dirección contraria, menos información y más contexto.

[47] http://www.dcc.uchile.cl/~rbaeza/inf/contexto.html
[48] VIAGGIO, S., A general theory of interlingual mediation, Frank & Timme GmbH, 2006
[49] BROWN, Duguid. La Vida Social de la Información, Harvard University Press, 2000

A su vez, la información no es un recurso en sí misma, sino que lo será en un contexto determinado. De aquí se deduce la necesidad de conocer el contexto y las prácticas de la organización o del individuo, es decir, se debe saber qué información es relevante para lograr el objetivo de la persona[50] (sea ésta natural o jurídica). Lo anterior concuerda con el planteamiento de Horton: la información no es un recurso en sí misma, sino que lo es en el contexto de un proceso o tarea específica[51]. Este mismo concepto aplica al contexto jurídico y técnico en el cual se desarrollan los procesos que generan la información.

En efecto, el mismo concepto de contexto incide en reforzar la dimensión social de la información frente al énfasis excesivo en el modelado de procesos: no se debe olvidar que no todos los procesos son “estructurados” y que la mayor parte de las actividades y tareas orientadas a crear, compartir y distribuir información y conocimiento se desarrollan siguiendo pautas y redes “informales”. En este sentido, tan importante como mantener estas pautas es el hecho de hacerlas conocidas y ser capaces de darles un contexto en las actividades de la organización o del individuo.

1.7. EL PROCESO COMUNICATIVO

Los procesos de comunicación son interacciones mediadas por signos entre al menos dos agentes que comparten el mismo conjunto de signos con reglas semióticas comunes. En el proceso comunicativo, la información es incluida por el emisor en un paquete y canalizada hacia el receptor a través del medio. Una vez recibido, el receptor decodifica el mensaje y proporciona una respuesta[52] [53]

[50] El profesional de la información, v. 12, n. 4, julio-agosto 2003. Pag 305
[51] HORTON, Forest W. "Information architectures: the information resources entity (IRE) modeling approach". En: Aslib proceedings, 1989, nov-dic, v. 41, n. 11/12, pp. 313-318.
[52] GALINDO, Jesús. Comunicación, ciencia e historia. Mcgraw hill. 2008
[53] MILLER, K., Communication Theories: Perspectives, processes, and contexts. 2nd edition. New York: McGraw-Hill, 2005

1.7.1. Elementos del proceso

- Emisor: Es quien emite el mensaje, puede ser un dispositivo o una persona. Es el lugar de donde emana la información, los datos, el contenido que se enviará, en conclusión: de donde nace el mensaje primario.

- Fuente o Transmisor: Es el punto (persona, organización) que elige y selecciona los signos adecuados para transmitir su mensaje; es decir, los codifica para poder enviarlo de manera entendible - siempre que se maneje el mismo código entre el emisor y el receptor - al receptor. No existe un iniciador en el proceso comunicativo, a lo sumo existe una instancia primaria de emisión - que se confunde con el que "habló primero" - pero la comunicación debe ser entendida como un proceso dinámico y circular, sin principio ni fin. Podemos iniciar el acto comunicativo preguntando la hora a alguien, pero inevitablemente la comunicación comenzó mucho antes, al ver a la persona, al acercarse prudentemente a la distancia mínima – Proxémica - de dos personas desconocidas, al mirar a la persona a los ojos, al insinuar que se quiere hablar o al realizar contacto entre máquinas. Como se puede ver, la comunicación no se limita al habla o a la escritura: es un complejo proceso interminable de interacción mutua.

- Receptor o decodificador: Es quien, o el dispositivo que, recibe la información. Dentro de una concepción primigenia de la comunicación es conocido como Receptor, pero dicho término pertenece más al ámbito de la teoría de la información. Es el punto (persona, organización, dispositivo) al que se destina el mensaje, realiza un proceso inverso al del emisor ya que en él está el descifrar e interpretar lo que el emisor quiere dar a conocer. Existen dos tipos de receptor, el pasivo que es el que sólo recibe el mensaje, y el receptor activo o perceptor ya que no sólo recibe el mensaje sino que lo percibe, lo almacena, e incluso da una respuesta, intercambiando los roles. En este caso, donde un

receptor o perceptor se transforma en emisor al producir y codificar un nuevo mensaje para ser enviado al ente emisor - ahora devenido en receptor - es donde se produce el feed-back o retroalimentación; y es lo que comúnmente sucede en cualquier comunicación.

- Interferencia, barrera o ruido: Cualquier perturbación que sufre la señal en el proceso comunicativo, se puede dar en cualquiera de sus elementos. Son las distorsiones del sonido en la conversación, o la distorsión de la imagen de la televisión, la alteración de la escritura en un viaje, la afonía del hablante, la sordera del oyente, la ortografía defectuosa, la distracción del receptor, el estudiante que no atiende aunque esté en silencio o la interferencia electrónica. También suele llamarse ruido[54] [55]

1.7.2. Fases del proceso

1. Desarrollo de una idea.- Este primer paso es el que le da sentido a la comunicación, puesto que primero se debe reflexionar y desarrollar la idea que se desea transmitir con determinada intención, si esto no existe, la comunicación no tendría caso.

2. Codificación.- Consiste en codificar o cifrar el mensaje, es decir, ponerlo en un código común para el emisor y el receptor: palabras (de un idioma común), gráficas, archivos u otros símbolos conocidos por ambos interlocutores. En este momento se elige también el tipo de lenguaje que se utilizará: oral, escrito, gráfico, etc. y el formato específico: oficio, circular, memo, póster, folleto, llamada telefónica, dibujo, video…

[54] OLIVAR ZÚÑIGA, Antonio (2006). Fundamentos teóricos de la comunicación
[55] GRIFFIN, E. A., A first look at communication theory. 3rd edition, New York: McGraw-Hill, 1997

3. Transmisión.- Una vez desarrollado y elaborado el mensaje, se transmite usando el lenguaje, formato y código seleccionado, enviándolo a través de un Canal o vehículo de transmisión, eligiendo el canal más adecuado, con mínimas barreras, previniendo o controlando las posibles interferencias.

4. Recepción.- El paso anterior permite a otro participante recibir el mensaje a través de un Canal de recepción. Entre más órganos o dispositivos sensoriales intervengan en la recepción, mejor se recibirá el mensaje, pero esto no es suficiente; el receptor debe estar dispuesto a recibir el mensaje, para que éste llegue más fácilmente. Si el receptor no funciona bien, o pone una barrera, el mensaje se pierde.

5. Descifrado o Decodificación.- En este paso del proceso el receptor descifra el mensaje, lo decodifica e interpreta, logrando crear o más bien reconstruir una idea del mensaje. Si esa idea es equivalente a lo que transmitió el emisor se puede lograr la comprensión del mismo.

6. Aceptación.- Una vez que el mensaje ha sido recibido, descifrado e interpretado, entonces viene la oportunidad de aceptar o rechazar el mensaje, bajo el concepto del no repudio.

   La aceptación es una decisión que admite grados y depende de la forma en que fue percibido el mensaje, la apreciación que se hace de su exactitud y veracidad, la opinión previa o prejuicio que se tenga sobre el mismo, la autoridad del emisor y las propias creencias y valores del receptor y sus implicaciones. Si el mensaje es aceptado, entonces se logra el efecto deseado y el verdadero establecimiento de la comunicación.

7. Uso.- Este es el paso decisivo de acción, la reacción que se logra en el receptor y el uso que él le da a la información contenida en el mensaje recibido.

8. Retroalimentación.- La retroalimentación es el paso final que cierra el ciclo con la respuesta del receptor, que en este momento toma el papel de emisor, estableciendo así la interacción bilateral: la comunicación en dos direcciones. Si la retroalimentación no se diera, entonces la comunicación no se estableció plenamente y sólo se quedó a nivel unilateral como información. Retroalimentación es el término que se utiliza precisamente para llamar a la información recurrente o información de regreso, y es muy necesaria porque es la que indica al emisor si el mensaje fue recibido, si fue bien interpretado, si se aceptó y utilizó. Cuando la comunicación es completa, ambos interlocutores estarán más satisfechos, se evitará la frustración y se podrá acordar mejor la relación personal o laboral que se tenga, mejorando consecuentemente los resultados de la relación[56].

[56] BERLO, D. K. (1996). El proceso de la comunicación. México, El Ateneo

2. AUTORIDADES

El proceso de normalización, o estandarización, no surge por sí solo. Los estándares o normas técnicas son desarrollados por organismos, públicos o privados, reconocidos de manera amplia, son producto de normas legales, regulaciones, otros estándares o por exigencia de los usuarios, la comunidad, el mercado o cuando los productos, procesos o servicios no están adecuadamente normalizados o los estándares existentes son insuficientes, obsoletos o inadecuados.

Del latín "*auctoritas*", la autoridad es el poder, la potestad, la legitimidad o la facultad, y por lo general se refiere a aquellos que gobiernan o ejercen el mando, otorgado en algunos casos por la normatividad o los acuerdos basados en la ley, o al prestigio ganado por una persona u organización gracias a su calidad o a la competencia de cierta materia.

En el ámbito de la normalización técnica, el concepto de autoridad une ambos ámbitos al considerar organismos, públicos o privados, que cuentan con un amplio reconocimiento y competencia en la materia en la cual producen las normas.

2.1. JERARQUIA DE AUTORIDADES

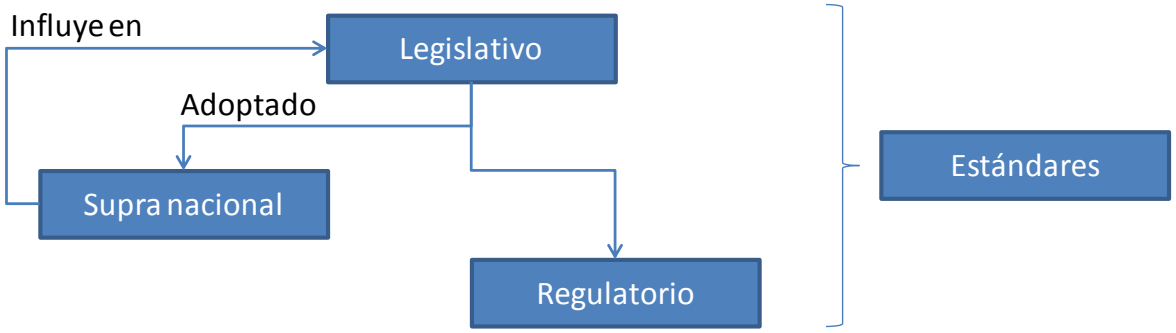
Según la autoridad involucrada en el proceso de normalización, las normas expresadas como actos legislativos poseen un nivel jerárquico superior frente a las regulaciones, las cuales son confeccionadas para desarrollar, regular y/o controlar los actos legislativos, estando subordinadas a éstos últimos.

Tabla 1. Clasificación jerárquica

Nivel	Origen	Nivel de autoridad	Alcance	Fuerza
Legislativo	Público	A nivel de congreso o parlamento.	Nacional	Mandatorio
Regulatorio	Público	Agencia regulatoria de tipo gubernamental.	Nacional	Mandatorio
Supranacional	Público / privado	Acuerdos internacionales Organismos internacionales.	Supranacional	Opcional
Estándar	Público / privado	Organismo de acreditación.	Supranacional	Opcional

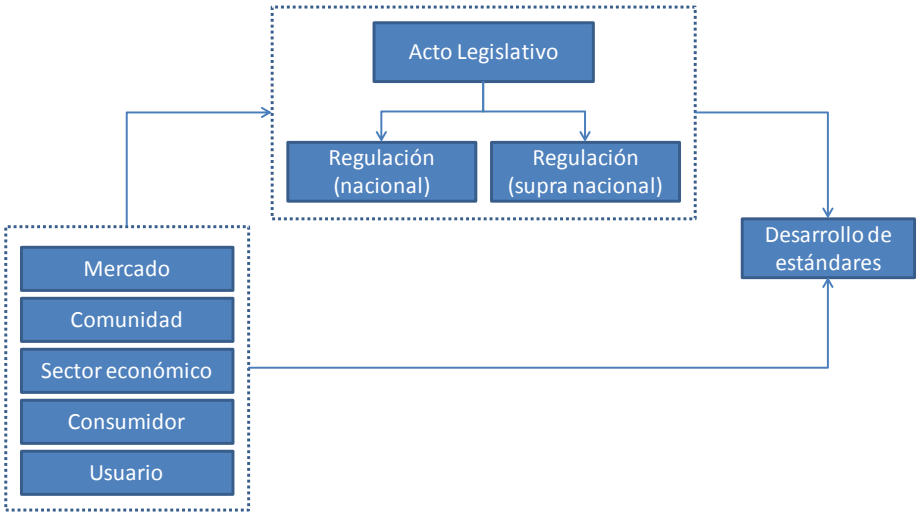
En ambos casos, los estándares son un complemento técnico de los actos legislativos, regulaciones y acuerdos supra nacionales, adoptados formalmente en algunos casos.

Figura 2. Estándares y sus grupos de interés en general



Los estándares tienen un ciclo externo respecto a los grupos de interés donde las normas técnicas funcionan como anexos o complementos técnicos a la normatividad y/o como respuesta al mercado, la comunidad, un sector económico, consumidor o usuario.

Figura 3. Estándares y sus grupos de interés



2.2. AUTORIDADES JURIDICAS

2.2.1. Supranacionales y comunitarios. Los sistemas jurídicos de tipo supranacional o comunitario superan la soberanía absoluta del estado nación, y pueden ser expresados en sistemas políticos comunitarios o en tratados internacionales.

2.2.1.1. Sistema político comunitario. Este esquema traza un sistema de organización, gestión política y de gobierno fundamentado en una conciliación estructurada de intereses diversos de los países miembro que aceptan el sistema.

Este sistema político se manifiesta en instituciones y órganos comunes que se integran en un marco jurídico y político compartido, adoptan decisiones vinculantes para todos, en ámbitos de competencia determinados, sin que los países miembro puedan desacatar o renunciar a las decisiones adoptadas por dichos órganos.

Su constitución y funcionamiento reposan de manera necesaria y obligatoria sobre los principios de la democracia cooperativa, la diversidad cultural y la solidaridad política, así como un sistema jurídico común que, sin perjuicio de su coexistencia con otros, goce de primacía o prevalencia sobre cualquier otro, en el ámbito de sus competencias.

El exponente de este sistema es el sistema comunitario de la Unión Europea, único en el mundo, sistema híbrido de gobierno transnacional con elementos de cooperación multilateral, fuertemente estructurada e institucionalizada con otros de tipo supranacional, regidos ambos por una dinámica de integración regional muy acentuada[57].

2.2.1.2. Tratados internacionales. Un tratado internacional es un acuerdo escrito entre ciertos sujetos de Derecho internacional, que puede constar de uno o varios instrumentos jurídicos conexos, y siendo indiferente su denominación. Lo más común es que tales acuerdos se realicen entre Estados, aunque pueden celebrarse entre Estados y organizaciones internacionales. Los primeros están regulados por la Convención de Viena sobre el Derecho de los Tratados de 1969; los segundos, por la Convención de Viena sobre el Derecho de Tratados celebrados entre Estados y Organizaciones Internacionales de 1986[58].

Los tratados internacionales deben diferenciarse según su connotación[59] según el tipo de obligaciones creadas:

a. Los Tratados-ley establecen normas de aplicación general entre dos o más estados, normas que jurídicamente se encuentran en un pedestal superior a las leyes internas de los países firmantes, con un ámbito mayor o menor de

[57] TRATADO DE LISBOA: la Unión Europea en el Mundo. Portal de la Unión Europea. 2009
[58] http://www.derechos.org/nizkor/ley/viena.html
[59] http://www.enciclopedia-juridica.biz14.com/d/tratados/tratados.htm

obligatoriedad. Estas normas jurídicas suponen un sometimiento de los Estados que las aceptan (y en algunos casos otros) y tienen una virtualidad más o menos definida pero con trascendencia posterior. Son un acuerdo de voluntades concurrentes en ciertos intereses, de modo que no hay oposición, sino coincidencia, y la intención no es simplemente contractual, sino que en esencia es «legislativa».

b. Los Tratados-contrato son un intercambio de prestaciones entre partes contratantes. Son instrumentos mediante los cuales se crean obligaciones jurídicas entre los Estados o, en término más amplios, se crean obligaciones y derechos concretos entre ellos, de modo que cumplidos, pierden su virtualidad.

En la actualidad, Colombia ha suscrito diversos acuerdos internacionales, principalmente de índole económico, entre los cuales se incluyen[60]:

- Organización Mundial del Comercio (OMC)
- El Andean Trade Preference Act (ATPA) con Estados Unidos.
- El Andean Trade Preference & Drug Erradication Act (APTDEA) Estados Unidos.
- El Sistema Generalizado de Preferencias para los Países Andinos (SGP ANDINO) con la Unión Europea.
- La Asociación Latinoamericana de Integración (1980) (ALADI)
- Comunidad Andina de Naciones (CAN), con Bolivia, Ecuador y Perú.
- Tratado de Libre Comercio de los Tres (TLC-G3), con México y Venezuela.
- La Comunidad del Caribe (CARICOM)
- Área de Libre Comercio de las Américas (ALCA)
- El acuerdo de Colombia en la Cuenca del Pacífico.
- Acuerdo de Complementación Económica MERCOSUR y Colombia.
- Tratado de Libre Comercio Colombia-Estados Unidos.
- Acuerdo de Complementación Económica con Chile.

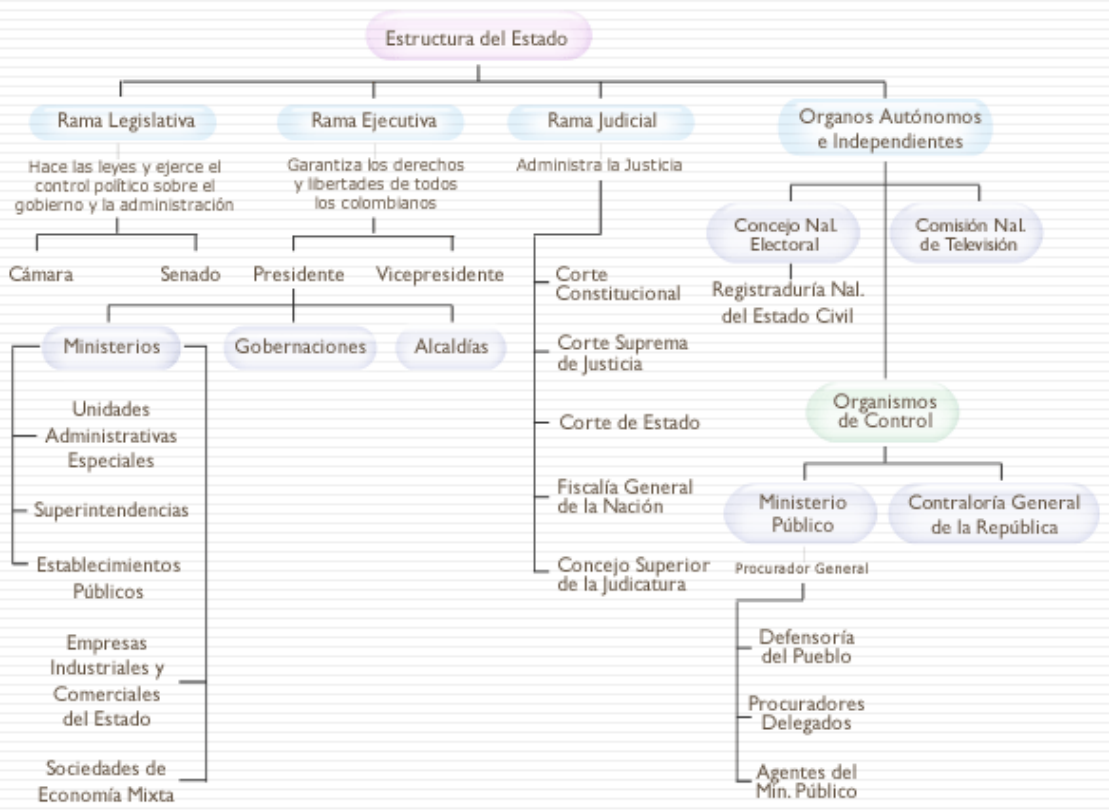
[60] http://www.productosdecolombia.com/main/guia/Acuerdos_Preferencias_Arancelarias.asp

- Tratado de Libre Comercio Colombia - Unión Europea.

2.2.2. Nacionales - caso Colombiano.

El estado colombiano, como estado social de derecho, con plena autonomía de sus entes territoriales y siguiendo los preceptos de democracia participativa y pluralista[61], está organizada en las siguientes ramas (legislativa, ejecutiva y judicial) así como por órganos independientes y autónomos, incluyendo los de control y vigilancia[62]:

Figura 4. Estructura del gobierno colombiano



Fuente: DAFP. Departamento Administrativo de la Función Pública.

[61] http://hermesoft.esap.edu.co/esap/hermesoft/portal/home_1/rec/arc_1623.pdf
[62] http://blogjus.wordpress.com/2007/04/01/conozcamos-nuestra-democracia/

2.2.2.1. Rama legislativa. La rama legislativa está representada por el Congreso de la República que lo integran el Senado y la Cámara de Representantes. Corresponde al Congreso de la República reformar la Constitución, hacer las leyes y ejercer control político sobre el gobierno y la administración[63].

Funciones:

a. Función Constituyente: reformar la Constitución Política mediante actos legislativos.
b. Función legislativa: elaborar, interpretar, reformar y derogar las leyes y códigos en todos los ramos de la legislación.
c. Función de control político: Requerir y emplazar a los Ministros del Despacho y demás autoridades y conocer de las acusaciones contra altos funcionarios del Estado.
d. Función judicial, para juzgar excepcionalmente a los altos funcionarios del Estado por responsabilidad política.
e. Función electoral: Elegir Contralor General de la República, Procurador General de la Nación, Magistrados de la Corte Constitucional y de la Sala Jurisdiccional Disciplinaria del Consejo Superior de la Judicatura, Defensor del Pueblo, Vicepresidente de la República, cuando hay falta absoluta.
f. Función administrativa: Establecer la organización y funcionamiento del Congreso Pleno, el Senado y la Cámara de Representantes.
g. Función de control público: Emplazar a cualquier persona, natural o jurídica, a efecto de que rindan declaraciones, orales o escritas, sobre hechos relacionados con las indagaciones que la Comisión adelante.
h. Función de protocolo: Recibir a Jefes de Estado o de Gobierno de otras naciones.

[63] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Estructura del estado colombiano. Bogotá. 2006

2.2.2.2. Rama ejecutiva. La Rama Ejecutiva del Poder Público en el orden nacional, está integrada por los siguientes organismos y entidades:

1. Del Sector Central:
   a) La Presidencia de la República;
   b) La Vicepresidencia de la República;
   c) Los Consejos Superiores de la administración;
   d) Los ministerios y departamentos administrativos;
   e) Superintendencias y unidades administrativas especiales, sin personería jurídica.

2. Del Sector descentralizado por servicios:
   a) Los establecimientos públicos;
   b) Las empresas industriales y comerciales del Estado;
   c) Superintendencias y unidades administrativas especiales, con personería jurídica;
   d) Empresas sociales del Estado;
   e) Empresas oficiales de servicios públicos domiciliarios;
   f) Los institutos científicos y tecnológicos;
   g) Las sociedades públicas y las sociedades de economía mixta;
   h) Las demás entidades administrativas nacionales con personería jurídica que cree, organice o autorice la ley para formar parte de la Rama Ejecutiva del Poder Público

Dentro de las funciones constitucionales de la rama ejecutiva, resaltan las siguientes:

1. Sancionar las leyes.
2. Promulgar las leyes, obedecerlas y velar por su estricto cumplimiento.
3. Ejercer la potestad reglamentaria, mediante la expedición de los decretos, resoluciones y órdenes necesarios para la cumplida ejecución de las leyes.

Esa potestad reglamentaria, es la que el presidente delega en los organismos y entidades del sector central y descentralizado por servicios, permitiendo a cada uno de ellos generar las normas legales necesarias para desarrollar el servicio público a su cargo.

2.2.2.3. Rama Judicial. Es la parte de la función pública que cumple el Estado encargada por la Constitución Política y la Ley, de hacer efectivos los derechos, obligaciones, garantías y libertades consagrados en ellas, con el fin de realizar la convivencia social, lograr y mantener la concordia nacional.

Le integran los siguientes estamentos, donde se resaltan las funciones que impliquen elaborar cualquier tipo de acto administrativo, directriz o política:

Tabla 2. Rama judicial

Organismo	Objeto
Consejo Superior de la Judicatura	Administrar la Rama Judicial. Ejercer la función disciplinaria.
Consejo de Estado	Es el máximo órgano de la Jurisdicción Contencioso Administrativa, resuelve en última instancia los procesos que involucran al Estado y a los particulares, o los procesos que involucran a dos Entidades Estatales, pudiendo establecer jurisprudencia. Cumple una función consultiva pues es el órgano al que debe recurrir el Gobierno antes de tomar ciertas decisiones, no para pedir autorización, sino para saber de su consejo, dictamen u opinión en ciertos asuntos.
Corte Constitucional	Ejercer la guarda de la integridad y supremacía de la Constitución, de los estrictos y precisos términos (artículos 241 al 244) de la Constitución Política. Proferir decisiones de tutela o resolver acciones o recursos previstos para aplicar derechos constitucionales, sentando jurisprudencia.

Fiscalía General de la nación	Investigar delitos, declarar precluidas las investigaciones realizadas, realizar la acusación de los presuntos infractores ante los juzgados y tribunales competentes, excepto los delitos cometidos por miembros de la fuerza pública en servicio activo y en relación con el servicio.
Instituto Nacional de Medicina Legal y Ciencias Forenses	Prestar auxilio y soporte técnico y científico a la Administración de Justicia en todo el territorio nacional, en lo concerniente a la Medicina Legal y las Ciencias Forenses.

2.2.2.4. Organismos de control.

Le integran los siguientes estamentos, frente a los cuales se resaltan las funciones que impliquen la elaboración de cualquier tipo de acto administrativo, directriz o política:

Tabla 3. Organismos de control

Organismo	Funciones
Procuraduría General de la Nación	Formular las políticas generales y criterios de intervención del Ministerio Público en materia de control disciplinario, vigilancia superior con fines preventivos, actuación ante las autoridades administrativas y judiciales y centros de conciliación, y promoción, protección y defensa de los derechos humanos. Expedir, en ejercicio de la suprema dirección del Ministerio Público, los actos administrativos, órdenes y directrices necesarios para señalar las políticas generales y criterios orientadores de actuación de la Defensoría del Pueblo en la promoción, ejercicio y divulgación de los derechos humanos.

Auditoría General de la república	Ejercer la vigilancia de la gestión fiscal de los organismos de control señalados en el Artículo segundo, conforme a los procedimientos, sistemas y principios establecidos en la Constitución, para lo cual el Auditor General fijará las políticas, prescribirá los métodos y la forma de rendir cuentas y determinará los criterios que deberán aplicarse para la evaluación financiera, de gestión y de resultados, entre otros.
Contraloría General de la República	Ejercer la vigilancia de la gestión fiscal del Estado a través, entre otros, de un control financiero, de gestión y de resultados, fundado en la eficiencia, la economía, la equidad y la valoración de los costos ambientales. Ejercer la vigilancia de la gestión fiscal conforme a los sistemas de control, procedimientos y principios que establezcan la Ley y el Contralor General de la República mediante resolución. Ejercer el control posterior sobre las cuentas de cualquier entidad territorial en los casos previstos por la Ley. Ejercer de forma prevalente y en coordinación con las contralorías territoriales, la vigilancia sobre la gestión fiscal y los resultados de la administración y manejo de los recursos nacionales que se transfieran a cualquier título a las entidades territoriales de conformidad con las disposiciones legales. Advertir sobre operaciones o procesos en ejecución para prever graves riesgos que comprometan el patrimonio público y ejercer el control posterior sobre los hechos así identificados. Conceptuar sobre la calidad y eficiencia del control interno en los términos previstos en la Constitución Política y la Ley

Defensoría del pueblo	Diseñar y adoptar con el Procurador General de la Nación las políticas de promoción y divulgación de los Derechos Humanos en el país, en orden a tutelarlos y defenderlos. Hacer las recomendaciones y observaciones a las autoridades y a los particulares en caso de amenaza o violación a los Derechos Humanos y para velar por su promoción y ejercicio. El Defensor podrá hacer públicas tales recomendaciones e informar al Congreso sobre la respuesta recibida. Dictar los reglamentos necesarios para el eficiente y eficaz funcionamiento de la Defensoría del Pueblo, lo relacionado con la organización y funciones internas y la regulación de trámites administrativos en lo no previsto en la ley.

Como se puede observar, cada organismo de éstos tiene potestad legal para producir actos administrativos de impacto general público. En el caso de la rama legislativa, la capacidad legal de producir normas es inherente a su función, sin embargo, en la ejecutiva es mediante delegación de las funciones del presidente y en el caso de la rama judicial y/o los organismos de control, la capacidad de generar normas obedece a sus propias funciones orientadas principalmente al control y vigilancia, tal como sucede con las directivas que emite la Procuraduría General de la Nación en diversos aspectos tales como el documental y riesgos.

2.3. AUTORIDADES TÉCNICAS

La necesidad de garantizar la repetitividad[64] en los procesos hacia productos o servicios uniformes bajo criterios unificados en las diversas industrias; la exigencia de trazabilidad o rastreabilidad como la "aptitud para rastrear la historia, la

[64] ISO 3534-2

aplicación o la localización de una entidad mediante indicaciones registradas"[65]; los requisitos de optimización en cuanto a eficiencia y reducción del error mediante el uso de especificaciones comunes para mecanismos, dispositivos y tecnologías, así como productos e insumos, de forma que se facilite la concurrencia de procesos, partes e incluso datos, entre otros, conllevó a que diversas organizaciones industriales y tecnológicas así como gubernamentales se hayan aliado para establecer pautas comunes y públicas al mercado, en un proceso abierto y formal, con el propósito de facilitar el intercambio internacional de bienes y servicios, y para desarrollar la cooperación en la esfera de la actividad intelectual, científica, tecnológica y económica[66].

En ese ámbito han surgido organizaciones a niveles nacionales, regionales o comunitarios así como internacionales de amplia adopción.

2.3.1. Internacionales. Ciertas organizaciones han evolucionado para alcanzar un nivel global bien sea por el prestigio en su sector o como efecto de la asociación entre entes de normalización regionales o nacionales, quienes se han puesto de acuerdo para promover normas de amplia aceptación.

Varios de estos organismos de normalización internacional han establecido acuerdos formales a nivel gubernamental, lo cual les otorga respaldo, amplia adopción y solidez a la tarea de normalización.

El siguiente esquema presenta la interrelación de autoridades de nivel internacional en aspectos relacionados con tecnologías de la información y las comunicaciones:

[65] ISO 8402
[66] http://www.eveliux.com/mx/historia-de-la-iso.php

Tabla 4. Participación de autoridades internacionales

<table>
<tr><td colspan="2"></td><td colspan="3">INTERNACIONAL</td><td>EUROPA</td></tr>
<tr><td colspan="2">GENERAL</td><td colspan="3">IEC / ISO</td><td>CEN</td></tr>
<tr><td rowspan="2">IT</td><td>WWW</td><td rowspan="3">IEEE
TIA / TTC</td><td rowspan="2">ITU-T</td><td>W3C /
IETF</td><td rowspan="2">ETSI</td></tr>
<tr><td>Otros</td><td></td></tr>
<tr><td colspan="2">Electricidad - Electrónica</td><td colspan="2"></td><td>UL</td></tr>
</table>

Respecto al anterior esquema, se tienen las siguientes entidades participantes:

IEC International Electrotechnical Commission.
ISO International Organisation for Standarisation
IEEE Institute of Electrical and Electronic Engineers
ITU Unión Internacional de Telecomunicaciones (engloba CCITT y CCIR).
TIA Telecommunications Industry Association
TTC Telecommunication Technology Committee
IETF Internet Engineering Task Force

2.3.2. Regionales. A nivel regional o comunitario, a partir de acuerdos supranacionales, tal como se referenció anteriormente, se tienen organismos de normalización que actúan como autoridades a nivel regional a partir de tratados internacionales que permiten emitir normas que son aceptadas e incluso de obligatoria implementación en los países que hacen parte o participan en el organismo de normalización.[67]

67 http://www.wssn.net/WSSN/listings/links_regional.html

Tabla 5. Organismos de normalización regional

Región	Autoridades regionales	
Africa	ARSO	African Regional Organization for Standardization
Americas	COPANT	Comisión Panamericana de Normas Técnicas
	AMN	Asociación MERCOSUR de Normalización
	CROSQ	Caribbean Organisation for Standards and Quality
	RAN	Red Andina de Normalizacion
USA	ACI	American Concrete Institute.
	API	American Petroleum Institute.
	ASCE	American Society of Civil Engineering.
	ASME	American Society of Mechanical Engineers.
	OFTA	Office of the Telecommunication Authority.
	MPT	Ministry of Posts and Telecommunications.
	FCC	Federal Communications Commission.
	PKCS	Public Key Cryptography Standards.
	ASTM	ASTM International.
	NEMA	National Electrical Manufacturers Association.
	NFPA	National Fire Protection Association.
	HL7	Health Level Seven Inc.
Arabia	AIDMO	Arab Industrial Development and Mining Organization
Asia y Pacific	ACCSQ	ASEAN Consultative Committee for Standards and Quality
	PASC	Pacific Area Standards Congress
	APEC	Asia-Pacific Economic Cooperation
Europa	CEN	Comité Européen de Normalisation
	CENELEC	Comité Européen de Normalisation Electrotechnique
	ETSI	European Telecommunications Standards Institute
	UN/ECE	UN Economic Commission for Europe
	EASC	Euroasian Interstate Council for Standardization, Metrology and Certification
	ERC/ERO	European Radiocommunications Committee
	CEPT	European Conference of Postal and Telecommunications
	UL	Underwriters Laboratories Inc.

Es común que normas dictadas para una región sean adoptadas directamente, o luego de un proceso de adaptación, a las circunstancias de otras autoridades de normalización o estados, situación igualmente necesaria en el evento en el cual una organización desea entrar a un mercado con un diferente esquema de estándares técnicos.

2.3.3. Nacionales a nivel nacional. Con mayor frecuencia, las naciones han desarrollado organismos que se comportan como autoridades de normalización, muchos de los cuales obrando en armonía con autoridades internacionales de normalización. Sin embargo, a nivel nacional suelen existir otros organismos, incluidas los entes descentralizados del sector público, que también actúan como autoridades técnicas y producen normas que pueden ser de obligatoria adopción e implementación a nivel nacional. Ver anexo B.

2.3.4. Organismos profesionales o gremiales. Siendo muy frecuente en el sector de tecnologías de la información y telecomunicaciones, existen diversas agrupaciones de índole profesional, integrados por empresas y expertos de un tema quienes concurren y mantienen sus propias normas técnicas, actuando como autoridades técnicas.

WSSN World Standards Services Network
ISACA Information Systems Audit and Control Association
PMI PROJECT MANAGEMENT INSTITUTE

Puede suceder que las recomendaciones o aspectos normalizados por estas autoridades, o parte de tales documentos, sean adoptados a nivel gubernamental como normas de necesaria adopción o prácticas recomendadas, bien sea por su recomendación directa o mediante el extracto de elementos clave. Un ejemplo de

esta afirmación es lo que ha hecho la Superintendencia Financiera de Colombia a través de la Circular externa 052 de 2007, la cual incorpora elementos clave de COBIT versión 4.0[68].

2.3.5. Organismos académicos. Otro grupo de autoridades lo conforman los grupos e instituciones académicas, donde algunas de ellas han logrado generar normas técnicas, mantenerlas y alcanzar un estatus de autoridad en el tema.

Existe varios ejemplos en este caso, como el modelo de madurez de la capacidad (CMM - Capability Maturity Model) del Carnegie Mellon University - Software Engineering Institute, el cual se ha convertido en un estándar de la industria informática expandiéndose a otras áreas como seguridad, riesgos y procesos, siempre midiendo la capacidad organizacional de mantener en funcionamiento y constante mejora el sistema de gestión analizado. De igual manera, está el modelo del Balanced ScoreCard desarrollado por investigadores de Harvard University, quienes se han convertido en referente internacional en el tema.

En Colombia, si bien las universidades participan en diversos trabajos de consultoría y servicios técnicos incluyendo los de ingeniería, aún no alcanzan el estatus de autoridad técnica que les permita emitir normas y respaldarlas con su nombre.

2.3.6. Organismos empresariales. Finalmente, está el concepto de la autoridad interna. En este caso, es la empresa, la organización en sí misma, quien dicta normas técnicas de uso interno o acepta ciertas condiciones o normas de uso contractual con proveedores o con clientes, y su ámbito de aplicación es inherente al espacio empresarial.

[68] www.superfinanciera.gov.co/ConsumidorFinanciero/ce05207.docx

3. ESTRUCTURA NORMATIVA

3.1. ESTRUCTURA NORMATIVA A NIVEL JURIDICO – COLOMBIA

Una norma jurídica es una regla u ordenación del comportamiento humano dictado por una autoridad competente según la jurisdicción, con un criterio de valor y donde el no cumplimiento trae aparejada una sanción. Generalmente, impone deberes y confiere derechos. La ley es un tipo de norma jurídica, pero no todas las normas son leyes, pues son normas jurídicas también las resoluciones, decretos, acuerdos, ordenanzas, y en general, cualquier acto administrativo que genere obligaciones o derechos.[69]

3.1.1. Ley. Del latin, *lex*, *legis,* es una declaración de la voluntad soberana, un precepto obligatorio dictado por el estamento legislativo o legitimo poder de un país, autoridad competente, por medio de la cual se ordena, regula, permite o prohíbe una cosa o se establecen los órganos necesarios por el cumplimiento de sus fines, en consonancia con la justicia para el bien de los gobernados.

Según el jurista Cesar Quintero, en su libro derecho constitucional, la ley es una "norma dictada por una autoridad pública que a todos ordena, prohíbe o permite, y a la cual todos deben obediencia"[70]. En sentido amplio, la ley es una norma jurídica la cual es expedida o dictada por el legislador, y debe cumplir con las siguientes características.

a) Generalidad: La ley comprende a todos aquellos que se encuentran en las condiciones previstas por ella, sin excepciones de ninguna clase.

69 http://produccionmaslimpia-karenvictoria.blogspot.com/2009/08/diferencia-entre-ley-decreto-resolucion.html

70 http://resolucionleyacuerdo.blogspot.com/2008/04/que-es-ley.html

b) Obligatoriedad: Tiene carácter imperativo-atributivo, es decir, por una parte establece obligaciones o deberes jurídicos y por la otra otorga derechos. Esto significa que siempre hay una voluntad que manda, que somete, y otra que obedece. La ley impone mandatos, incluso en contra de la voluntad de sus destinatarios. Su incumplimiento da lugar a una sanción, a un castigo impuesto por ella misma.

c) Permanencia: Se dictan con carácter indefinido, permanente, aplicable para un número indeterminado de casos y de hechos, y sólo dejará de tener vigencia mediante su abrogación, subrogación o derogación por leyes posteriores.

d) Abstracta e impersonal: Las leyes no se emiten para regular o resolver casos individuales, ni para personas o grupos determinados, su impersonalidad y abstracción las conducen a la generalidad.

e) Se reputa conocida: Nadie puede invocar su desconocimiento o ignorancia para dejar de cumplirla.

f) Esta se debe realizar en consonancia con la justicia y si se incumple debe aplicársele una sanción al infractor.[71]

TIPOS DE LEY

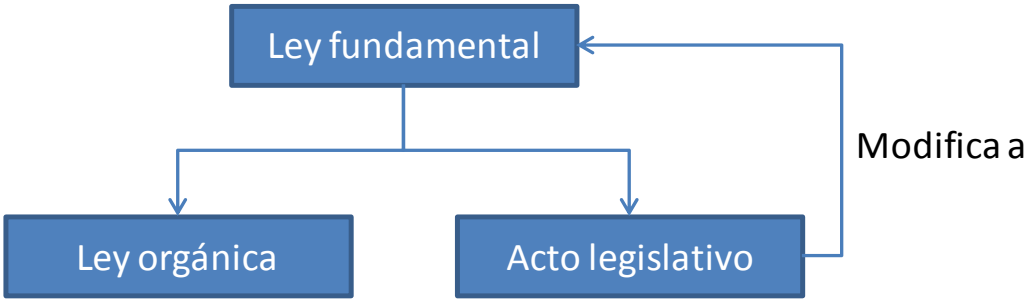
3.1.1.1. Ley fundamental. Es la que establece principios por los que deberá regirse la legislación de un país; suele denominarse constitución. La constitución es la norma suprema del ordenamiento jurídico, define derechos y obligaciones de tipo fundamental y está por encima de cualquier ley.

71 http://www.icesi.edu.co/blogs_estudiantes/pmlefrenvalencia/2009/08/28/ley-norma-decreto-resolucion/

3.1.1.2. Ley orgánica. Corresponde a aquellas leyes que nacen como consecuencia de un mandato constitucional para la regulación de una materia específica.

3.1.1.3. Acto legislativo. El Acto legislativo es el Acto del Congreso por medio del cual se reforma, regula o reglamenta la Constitución Política[72]. Un acto legislativo usualmente está expresado en la forma de una Ley.

Figura 5.Jerarquía a nivel de leyes



3.1.2. Legislación delegada

3.1.2.1. Decreto. Disposición, del tipo acto administrativo, expedida generalmente por el poder ejecutivo en ejercicio de su autoridad para situaciones de urgente necesidad y algunas otras específicamente tasadas, en asuntos de su competencia. Usualmente posee un contenido normativo reglamentario, por lo que su rango es jerárquicamente inferior a las leyes.[73] [74]

72 http://derechoencolombia.net/index.php?title=Acto_legislativo_-definición-
73 http://www.icesi.edu.co/blogs_estudiantes/pmlefrenvalencia/2009/08/28/ley-norma-decreto-resolucion/
74 http://produccionmaslimpia-karenvictoria.blogspot.com/2009/08/diferencia-entre-ley-decreto-

3.1.2.2. Decreto (legislativo). Utilizado por el Gobierno, generalmente el poder ejecutivo, para dictar normas en materia delegada por las Cortes, sobre materias que no necesiten ser reguladas por ley orgánica.[75]

3.1.2.3. Decreto Ley. Delegación expresa y especial del poder legislativo, con fuerza de ley, expedida ante circunstancias excepcionales, a favor del Poder ejecutivo.[76]

3.1.3. Acto administrativo. El acto administrativo es la "declaración unilateral de voluntad realizada en el ejercicio de la función administrativa con efectos jurídicos individuales de forma inmediata", "realizado en ejercicio exclusivo de las potestades y atribuciones inherentes de manera directa e inmediata, respecto de asuntos asignados por la ley, la ordenanza, el acuerdo o el reglamento ejecutivo"[77], conceptos que descarta posibles actividades de la administración que no sean específicamente emanaciones de la voluntad estatal.[78]

3.1.3.1. Resolución. La resolución administrativa consiste en una orden escrita dictada por el jefe de un servicio público, con carácter general, obligatorio y permanente, y refiere al ámbito de competencia del servicio. Las resoluciones se dan para cumplir las funciones que la ley encomienda al servicio público que la genera. En cuanto a su ámbito material, la resolución alcanza a todo aquello que complemente, desarrolle o detalle a la ley en la esfera de competencia del servicio

---

resolucion.html

75 http://produccionmaslimpia-karenvictoria.blogspot.com/2009/08/diferencia-entre-ley-decreto-resolucion.html

76 http://produccionmaslimpia-karenvictoria.blogspot.com/2009/08/diferencia-entre-ley-decreto-resolucion.html

77 Ley 489 de 1998, art. 5

78 http://resolucionleyacuerdo.blogspot.com/2008/04/que-es-ley.html

público. En cuanto al territorio, las resoluciones pueden tener alcance nacional o local, para servicios descentralizados. Las resoluciones tienen impacto en la actividad económica y social, pues tienen un grado de flexibilidad, oportunidad e información que la ley no puede tener, y en ese sentido la complementan[79].

En cuanto a lo judicial, una resolución es un fallo o providencia de una autoridad, entendida como acto procesal proveniente de un tribunal, mediante el cual resuelve las peticiones de las partes, o autoriza u ordena el cumplimiento de determinadas medidas.[80]

3.1.3.2. Acuerdo. Un acuerdo es la manifestación de una convergencia de voluntades, que tienen su origen en entidades estatales, con la finalidad de producir efectos jurídicos, teniendo como principal efecto jurídico del acuerdo su obligatoriedad para las partes que lo otorgan naciendo para las mismas obligaciones y derechos. Se suele usar el término Acuerdo para los concejos municipales y Ordenanza para las asambleas departamentales aun cuando puede igualmente aplicar, en términos generales, a cualquier decisión tomada en común por dos o más personas, por una junta, asamblea o tribunal.

En los acuerdos también concurren los expedidos por entidades privadas y cuyo fin es hacer manifestaciones voluntarias incluyendo los pactos, tratados o resoluciones de organizaciones, instituciones, empresas públicas o privadas. Es válido cualquiera que sea la forma de su celebración, siempre que el consentimiento de los otorgantes sea válido y su objeto cierto, determinado, no esté fuera del comercio o sea imposible.[81]

79 http://resolucionleyacuerdo.blogspot.com/2008/04/que-es-resolucin.html
80 http://produccionmaslimpia-karenvictoria.blogspot.com/2009/08/diferencia-entre-ley-decreto-resolucion.html
81 http://resolucionleyacuerdo.blogspot.com/2008/04/que-es-acuerdo.html

3.1.4. Informativas. Documentos complementarios emitido por autoridades competentes, como complementos a actos administrativos, bien sean leyes, decretos, resoluciones o acuerdos, con carácter meramente informativo o de tipo obligatorio.

3.1.4.1. Circulares. Dentro de los documentos informativos, las circulares son usadas principalmente para informar, comunicar, reportar e incluso notificar a un grupo abierto o cerrado de personas (naturales o jurídicas) sobre el contenido de una decisión, situación o circunstancia, el cual puede estar contenido en la circular o estar anexa a ella. De manera general, la circular va dirigida a aquellas personas que puedan ser, o estén, afectadas por el contenido de la misma.

3.1.4.2. Directrices. Las directrices son documentos informativos mediante los cuales la persona responsable o titular de la función administrativa hace una declaración unilateral de carácter decisorio sobre aspectos que deben desarrollarse, prohibiciones que deben acatarse o regulaciones que deben desarrollarse. Cuando se emiten estas directrices a nivel del poder ejecutivo, suelen contener un mensaje hacia los demás poderes y órganos del estado para desarrollar los aspectos contemplados en la directriz.

3.1.4.3. Guías. Las guías se comportan como documentos técnicos informativos muchas veces exigidos, considerándolos al nivel de normas técnicas, expedidas por autoridades del servicio público directamente relacionado con el objeto sobre el cual la guía está planteando instrucciones, pasos, definiciones e incluso controles.

3.2. ESTRUCTURA NORMATIVA A NIVEL TECNICO

3.2.1. Norma. El documento ISO/IEC Guide 2:1996 define "norma" o “estándar” a aquel documento, establecido por consenso y aprobado por un organismo reconocido, o autoridad, que establece reglas, pautas o especificaciones para actividades generalizadas y frecuentes y para sus resultados. Lo anterior con objeto de lograr un nivel de orden óptimo en un contexto dado.[82] El proceso de normalización da como resultado una norma. La Norma por su forma de elaboración y por el ámbito en que se realiza es de «carácter voluntario» y refleja el «estado del arte» en un lugar y momento determinado.

Las normas pueden indicar especificaciones técnicas para un área de actividad, pueden establecer los requisitos que aseguran la aptitud para el uso de un producto o servicio y la aptitud de un proceso o producto, y que cumple, entre otras, las siguientes condiciones:

- Haber sido establecida con la participación de todos los sectores involucrados
- Haber sido aprobada por consenso
- Tener como objetivo el beneficio de la comunidad
- Estar a disposición de todos los interesados
- Ser elaborada y publicada por un organismo de normalización reconocido[83]

Una norma puede ser declarada de cumplimento obligatorio (por organismos con potestades legislativas o reglamentarias) por razones de salud pública, bioseguridad, protección del medio ambiente, protección del consumidor, etc. En efecto, en los países desarrollados es hábito el reglamentar en estas áreas con referencia a normas técnicas.

82 http://www.termiumplus.gc.ca/didacticiel_tutorial/espanol/lecon5/page5_2_2_s.html
83 http://www.unit.org.uy/proyecto_fomin-bid/index.php?O=4&S=0

Su utilización puede ser igualmente impuesta de manera contractual, cuando, por ejemplo el estado o un comprador las autoimpone en sus compras o procesos. En cualquier caso la norma refleja e induce las necesidades, hábitos y exigencias del mercado, por lo que el proveedor debe cumplirlas para asegurar la satisfacción de sus clientes[84].

El British Standard Institute[85] (BSI) define a los estándares, acuerdos documentados de tipo formal producidos por autoridades de la industria, contienen especificaciones técnicas u otros criterios específicos diseñados para ser usados consistentemente como reglas, guías o definiciones que permitan homogeneizar, repetir y trazar la forma de hacer algo, mejorando la confiabilidad y efectividad de procesos, productos y servicios, y determinando un mecanismo para verificar la conformidad de un proceso, producto o servicio a sus especificaciones.

Los estándares se crean al unir la experiencia y experticia de los grupos de interés (stakeholders), tales como productores, vendedores, consumidores, usuarios, reguladores y el público general, sobre un material, producto, proceso o servicio.

Generalmente los estándares son diseñados y emitidos para uso y adopción voluntaria sin imposición. Sin embargo, algunas normas y regulaciones hacen referencia a determinados estándares de forma que para lograr el formal cumplimiento de una norma sea necesaria su adopción e implementación[86].

Finalmente, puede existir una jerarquía entre estándares: la norma internacional prima sobre la regional, ésta sobre la nacional y las de asociación. Sin embargo, es posible encontrar diferentes especificaciones a diferente nivel.

---

84 http://www.unit.org.uy/proyecto_fomin-bid/index.php?O=4&S=1

85 BSI. Product definitions. Londres: www.bsigroup.com/en/Standards-and-Publications/About-standards/Product-definitions/, 2010

86 BSI. Product definitions. Londres: www.bsigroup.com/en/Standards-and-Publications/About-standards/Product-definitions/, 2010

Figura 6.Jerarquía a nivel de normas técnicas

Fuente: BSI

3.2.1.1. Norma técnica. Las normas técnicas establecen por consenso, las características o especificaciones de un producto, servicio, proceso o sistema terminológico [87]

3.2.1.2. Norma terminológica. Las normas terminológicas son normas fundamentales. Especifican, según acuerdo, el vocabulario común que debe utilizarse en una norma o familia de normas. Las normas terminológicas, en lugar de precisar las especificaciones de un producto, servicio o proceso, especifican los términos por utilizar y sus definiciones (las especificaciones del término), con el ánimo que todos los usuarios comprendan de igual manera los conceptos fundamentales en una norma o familia de normas dada.

Las normas terminológicas pueden estar vinculadas a una norma de manera específica e incorporarse en una sección de una norma técnica; o bien, pueden aplicarse a una serie de normas y presentarse en un documento independiente que señale todos los términos y definiciones que regirán específicamente dicha serie de normas. Estas normas son por lo general *de jure*, es decir producidas en

87 http://www.termiumplus.gc.ca/didacticiel_tutorial/espanol/lecon5/page5_2_3_s.html

derecho por un organismo de normalización u órgano oficial. Son el fruto de un proceso de normalización organizado y formal.

3.2.1.3. Estándares de facto. De facto es una locución latina que significa «de hecho», esto es, sin reconocimiento formal, por la fuerza de los hechos. Los estándares de facto suelen surgir cuando una tecnología se impone en el mercado como predominante, con sus propias normas, la terminología que le es propia se convierte en norma de facto.[88]

3.3. CLASIFICACIÓN DE ESTÁNDARES

El BSI establece la siguiente clasificación de los estándares a nivel internacional:

a. Especificaciones. Dicta requerimientos detallados a ser aplicados y satisfechos por un producto, material, proceso, servicio o sistema, así como los procedimientos para confirmar la conformidad respecto a dichos requerimientos.

b. Métodos. Proporciona una completa descripción sobre la forma en la cual una actividad es realizada (e incluso, si es aplicable, los tipos de equipo y herramienta requeridos), especificaciones, mediciones, así como resultados y grado de precisión previsto.

c. Guía. Suministra información amplia y general sobre un tema técnico y sus bases de conocimiento relacionadas.

d. Vocabulario. Lista definiciones de términos empleados en un sector, campo o disciplina particular. Busca establecer un lenguaje común.

88 http://www.termiumplus.gc.ca/didacticiel_tutorial/espanol/lecon5/page5_2_3_s.html

e. Código de práctica. Incluye recomendaciones de buenas prácticas realizadas por la industria a partir de los resultados de la experiencia práctica y conocimiento adquirido por participantes idóneos, competentes y conscientes en la técnica.

f. Clasificación. Descripción de diversos grados, tipos o niveles de un producto o material, ordenándolo en una manera jerárquica.

3.3.1. Clasificación de normas y métodos en informática

En cuanto a las diferentes áreas de informática, se tiene un gran universo de normas que han sido generadas por diversas autoridades: [89] [90] [91] [92] [93] [94] [95] [96] [97] [98] [99] [100] [101] [102] [103]

---

[89] ALDEGANI, Gustavo. Seguridad Informática VIII. Buenos Aires: MP Ediciones. 1997.

[90] DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION – DCSSI. Typologie des normes et methods. Paris: DCSSI, 2002.

[91] ENISA. Agencia Europea Seguridad Informática. Heraklion: http://www.enisa.europa.eu/, 2010

[92] FIRTMAN, Sebastian. Seguridad Informática, Manuales USERS: Las amenazas y vulnerabilidades más peligrosas al desnudo. Texas: M.P. Ediciones, 2005.

[93] GARTNER. Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms. Nueva York: Thomson Reuters, 2009

[94] ICONTEC. NTC 5254. Norma colombiana de gestión del riesgo. Bogotá: ICONTEC, 2004

[95] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 10196; ISO 12142; ISO 12037; ISO 18942, ISO 23081. Normas técnicas en gestión documental y archivística. Ginebra: http://www.iso.org/, 2010

[96] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 14000. Norma de gestión ambiental. Ginebra: http://www.iso.org/, 2007

[97] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 2700x. Conjunto de normas en gestión de la seguridad de la información. Ginebra: http://www.iso.org/, 2007

[98] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 25999. Norma técnica en continuidad del negocio en gestión de información. Ginebra: http://www.iso.org/, 2008

[99] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. ISO 31100:2009. Norma de gestión del riesgo. Ginebra: http://www.iso.org/, 2009

[100] PAGE, Stephen. Achieving 100% Compliance of Policies and Procedures. Los Angeles: Process Improvement Pub, 2007.

[101] SILVERMAN, Michael. Compliance Management for Public, Private, or Non-Profit Organizations. Nueva York: McGraw Hill, 2008.

[102] STANDARDS AUSTRALIA LIMITED. ASNZ 4360:2004 - Gestión del riesgo. Sidney: Standards Australia Limited, 2004.

[103] TARANTINO, Anthony. Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB's A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices,

Tabla 6. Clasificación de normas y métodos en informática

Clase	Normas existentes
Buenas prácticas (medición de la seguridad)	IT Baseline Protection Manual (BSI Alemania), ISO 17799, ISO 13335, ACSI 33 (DSD Australia), CM 5515 (Otan)
Control Interno Informático	Massia (DGA), ERSI (Foro de competencias), IPAK (CSI), SP800-26 (NIST), MECI 1000:2005 (Colombia)
Gestión informática	COBIT
Normas específicas	Redes MG-1 (CSE Canadá), sitios RFC 2196 (IEFT), interconexión AC35-D/1027 (OTAN), de madurez SSE-CMM (ISSEA), de dominio específico Messedi, Muse.
Riesgo informático	EBIOS (DCSSI), Marion, Mehari (Clusif), Melisa, MV3 (CF6), Cramm, Ninah (XP CONSEIL), Risk Management Guide, MG-2 (CSE Canadá), SP800-30 (NIST), IAM (NSA), Buddy System, ISO 31000:2009; ISO 31100:2009; COSO; CMMI, ASNZ 4360:2004; NTC 5254; OCTAVE II.
Integración informática	DSIS (DCSSI), Incas (Clusif), Orion (Cersiat)
Guías de documentación	Feros, SSRS, SP800-18
Políticas de seguridad	PSI (DCSSI), ISPME (CSE Canadá), RFC 1244 (IETF)
Evaluación de productos	TCSEC (DoD US), ITSEC (CEE), ISO 15408
Organizacionales	GMITS, gestión de la seguridad de IT, (ISO/IEC TR 13335), ISO/IEC 17799, BS 7799 Part 1 – 1999.
De criterio	ISO/IEC 15408, ISO/IEC 15947
Diagnóstico de la calidad	ISO/IEC 19011 (Audit), ISO 9004 (Qualité), Garde
Gestión de la calidad	ISO 9001:2008; NTCGP 1000:2004 (Colombia); GTC 200 (Colombia); EFQM
Ambiental	ISO 14000:2007
Ocupacional	OHSAS 18000:2007
Servicios de la información	ISO 27001, 25999; ITIL; OSSTM, NIST 800, ISSAF, TickIT.
Documental	ISO 10196; ISO 12142; ISO 12037; ISO 18942, ISO 23081; MoReq; OAIS; ICA; IASA; HL7; DoD 50152

and Case Studies (Manager's Guide Series). Hoboken, NJ: Wiley, 2006.

Gestión de proyectos	PMBOK 4; PRINCE 2; COCOMO; TOCMP
Enfoque a procesos	Six sigma, BPM, WF, TPM, BSC, RSC (ISO 38500), TOC.
Información en salud	HIPAA
Gestión financiera	SOX, BASEL II, SARLAFT (Colombia), SARO (Colombia)

3.3.2. Objetivos de la estandarización aplicada a la informática.

1- Racionalización del trabajo. Las normas son el elemento de racionalización básico de la producción y de la gestión de la información. Proporcionan una guía útil en cuanto a la forma de plantear procesos productivos y de trabajo.

2- Garantía de calidad.

- Existe la necesidad de evaluar la calidad y cumplimiento de productos, procesos y servicios. Esto precisa de un sistema de calidad reconocido.
- Las normas representan una referencia imprescindible sobre metodologías, técnicas y prácticas, definidas por la comunidad técnica, profesional y científica, y representa la experiencia, estado del arte e investigación en el sector.
- Proporcionan solvencia técnica y profesional.
- Los estándares son convenciones sobre criterios de garantía de calidad y la referencia para comparar la calidad de un producto, proceso o servicio.
- Facilitan el mantenimiento y la continuación de lo realizado por otros.

3- Interoperabilidad (integración)

- Interoperabilidad de procesos. Se facilita la continuación y participación en el proceso por otro equipo o grupo de profesionales.
- Interoperabilidad de profesionales, cuyo conocimiento técnico normativo les permite trabajar en distintos proyectos del sector.
- Solo el uso extensivo del conjunto de normas técnicas precisas puede garantizar esta interoperabilidad.

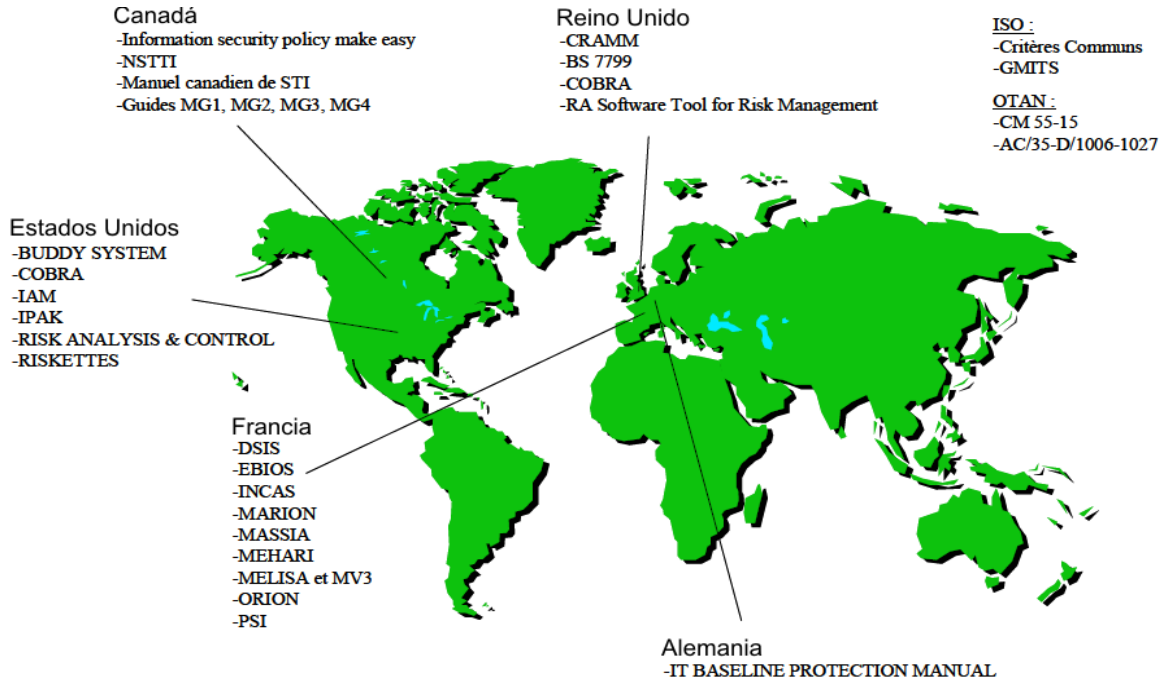
- Interoperabilidad de productos. Los resultados pueden ponerse fácilmente en comunicación, sin trabajo específico añadido. En el caso de la información, se trata de que diversos proyectos o trabajos compartan abiertamente la información de la que disponen, creando redes de sistemas de información.

4- Desarrollo técnico y comunicación

Los beneficios del uso de las normas provienen de la aceptación de las normas como conjunto de reglas que racionalizan el trabajo. Esta aceptación proviene del ámbito supralocal de las normas, que obliga al productor a la comunicación con la comunidad técnica (órganos emisores, grupos de trabajo, fórums)

3.3.3. Cartografía de la normatividad técnica. [104]

Figura 7. Cartografía de la normatividad técnica



Fuente: CIGREF

[104] CIGREF. Sécurité des systems d'information. Quelle politique globale de gestion des risques. Paris: www.cigref.com, 2002.

3.3.4. Por qué escoger una norma o método.[105]

- Obtener una visión homogénea y coherente en el área de aplicación de la norma.
- Establecer un marco de referencia y lenguaje común a los grupos de interés.
- Tener una estructura base para la gestión del riesgo.
- Permitir el aseguramiento de la calidad.
- Certificar la adhesión (cumplimiento) de la norma.
- Como efecto de exigencias de mercado, contractual o legal.

3.3.5. ¿Cuál método? ¿Cuál Norma? Las organizaciones tienden a escoger normas técnicas conforme a la moda, el conocimiento y/o experiencia de su personal vinculado al área de tecnologías de la información, la exigencia específica del mercado, o elaborar o adaptar normas según sus necesidades particulares.

Sin embargo, los criterios comunes para su escogencia, y que deben ser parte de cualquier metodología orientada a evaluar el cumplimiento y el riesgo asociado, son:

a. Objetivos de la norma.
b. El nivel de abstracción.
c. Los dominios incluidos.
d. El grado de cobertura por dominio.
e. El carácter estándar – o no – de la norma o método.
f. El grado de actualización y vigencia.
g. La estabilidad y continuidad.

[105] e-SECURITE. Le choix des normes, outils et méthodes. París: http://www.e-securite.net , 2010

h. La transversalidad – o no – de la norma o método.
i. El nivel de difusión.
j. La capacidad de adaptación.
k. La auditabilidad.
l. La disponibilidad de información y conocimiento.
m. El costo de adquisición.
n. El costo de implementación.
o. El costo de mantenimiento.
p. El costo de certificación.
q. Los organismos involucrados en su mantenimiento.
r. La exigibilidad (según mercados, regulaciones y zonas)

4. LA GESTION DEL RIESGO

Conforme a lo establecida en la guía técnica ISO 73:2002[106] "Vocabulario de la gestión del riesgo", el riesgo se define como la combinación de la probabilidad de un evento y sus consecuencias. OCTAVE II[107] amplia dicha definición al establecer el riesgo como la Posibilidad de materialización de una amenaza en un Impacto determinado (riesgo o pérdida) pudiendo afectar un Activo, un Dominio o toda la Organización. La norma ISO 31000:2009[108] amplía aún más el concepto al definir al riesgo como el efecto de la incertidumbre en la consecución de los objetivos, de forma que en el caso de la empresa serán estos objetivos los de índole corporativo y estratégicos.

Otras autoridades, como el Instituto Internacional de Auditoría (IIA[109]), lo define como la probabilidad que un evento o acción pueda afectar adversamente la organización o la actividad auditada; la Information Systems Audit and Control Association (ahora ISACA[110]) amplia su rango de acción a los sistemas de información. En Colombia, El Departamento Administrativo de la Función Pública (DAFP) lo definió en términos de aquella posibilidad que ocurrencia de una situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos[111].

El planteamiento de la norma ISO 31000:2009, establece tres aspectos clave dentro de la gestión del riesgo:

---

[106] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. Guide 73:2002, Risk managament Vocabulary. Ginebra: http://www.iso.org/, 2002
[107] CERT. OCTAVE II METHOD. http://www.cert.org/octave/methodintro.html. 2001
[108] http://www.iso.org/iso/catalogue_detail?csnumber=43170
[109] http://www.theiia.org/
[110] http://www.isaca.org/
[111] http://www.dafp.gov.co/

1. Incertidumbre (puede que nunca ocurra).
2. El riesgo importa y debe gestionarse porque tiene un efecto (positivo o negativo).
3. Ese efecto es sobre los objetivos fijados.

4.1. LA GESTION DEL RIESGO

4.1.1. Principios de gestión del riesgo. La norma más actual sobre gestión del riesgo, ISO 31000, que reúne e integra la mayoría de aspectos de las normas relacionados con gestión del riesgo, en su cláusula 4 define los siguientes principios de gestión del riesgo:

1. **Crea valor**. Contribuye a la consecución de objetivos así como la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.
2. **Está integrada en los procesos de una organización**. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
3. **Forma parte de la toma de decisiones**. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
4. **Trata explícitamente la incertidumbre**. La gestión del riesgo trata aquellos aspectos de toma de decisiones inciertos, la naturaleza de la incertidumbre y como tratarse.
5. **Es sistemática, estructurada y adecuada**. Contribuye a la eficiencia y a la obtención de resultados fiables, consecuentemente.
6. **Está basada en la mejor información disponible**. Los inputs del proceso de gestión del riesgo están basados en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.

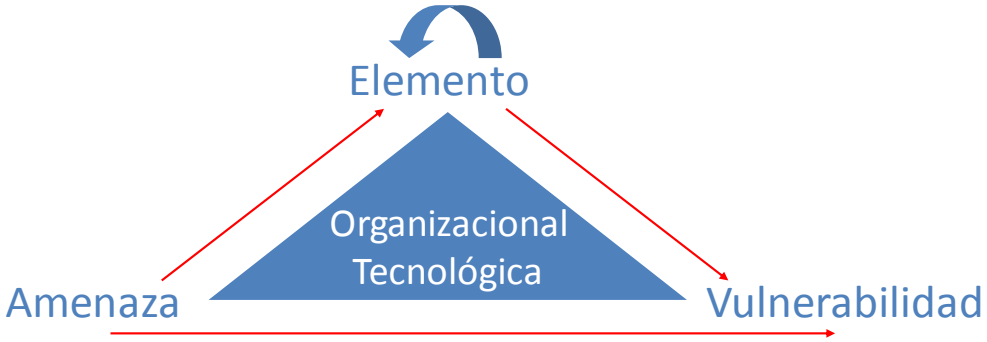
7. **Está hecha a medida**. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.
8. **Tiene en cuenta factores humanos y culturales**. Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna, que puede facilitar o dificultar la consecución de los objetivos de la organización.
9. **Es transparente e inclusiva**. La apropiada y oportuna participación de los grupos de interés (stakeholders) y, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.
10. **Es dinámica, iterativa y sensible al cambio**. La organización debe velar para que la gestión del riesgo detecte y responda a cambios de la empresa.
11. **Facilita la mejora continua de la organización**. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

4.1.2. Conceptos asociados al riesgo. El riesgo reúne varios elementos según el punto de vista o enfoque utilizado:

1. **Respecto al activo**.
   a. Activo o dominio: Elemento, proceso u organización que puede verse afectado por la materialización del riesgo.
   b. Vulnerabilidad: Debilidad del elemento a proteger o de la organización[112] que puede usarse (accidental o intencionalmente) o llevar a que se materialice un riesgo (NIST[113]).
   c. Amenaza: Potencial de desarrollar una vulnerabilidad (NIST) que conforma la causa de un impacto (no deseado) a una organización o sistema (ISO 13335-1[114])

[112] http://www.cert.org/octave/ - Operationally Critical Threat, Asset Vulnerability Evaluation (OCTAVE)
[113] http://www.nist.gov/
[114] ISO 13335-1

Figura 8. Componentes del riesgo según la norma OCTAVE II



2. **Respecto a su ocurrencia**[115].
   a. Probabilidad: Oportunidad de ocurrencia de un evento de riesgo.
   b. Consecuencia o Impacto: Resultado de un evento de riesgo.
   c. Pérdida: Consecuencia negativa.
   d. Control: Proceso, política, dispositivo y acciones que optimizan el riesgo.
   e. Fuente: Elemento o actividad con potencial de generar eventos de riesgo.
   f. Peligro: Fuente de daño (impacto negativo) potencial que puede causar pérdida[116].
   g. Evento: Ocurrencia de un conjunto particular de circunstancias.
   h. Factor de riesgo: Elementos que favorecen la ocurrencia de un riesgo.
   i. Grupos de interés: Personas y organizaciones que pueden afectar, ser afectados o creer estar afectados por un riesgo.

3. **Respecto a su gestión**[117].
   a. Optimización del riesgo: Minimizar las consecuencias negativas y maximizar positivas, y sus probabilidades de ocurrencia
   b. Mitigación: Limitación de consecuencias negativas de un evento negativo.
   c. Tratamiento del riesgo: Proceso de selección e implementación de medidas

[115] ISO Guide 73
[116] ISO Guide 51
[117] ISO Guide 73

para modificar el riesgo[118].

d. Riesgo Residual: Riesgo remanente luego de la implementación del tratamiento[119].

4.1.3. Áreas de materialización del riesgo. La gestión del riesgo, especialmente en sus normas ISO 31000:2009; ISO 31100:2009; COSO; y ASNZ 4360:2004, se tienen los siguientes campos de impacto del riesgo:

Tabla 7. Lista de impactos en gestión del riesgo

MATERIALIZACION	RIESGOS	MATERIALIZADO POR
Pérdida financiera (material)	• Sanciones • Sobrecostos • Merma ingreso/utilidad	• Organismos de control y/o regulación • Relación contractual • Calidad, Especificaciones
Deterioro de la imagen	• Reputación (daño) • Oportunidades (pérdida) • Mercado (participación)	• Prácticas no aceptadas, Investigaciones • Exclusión, Transparencia (problemas)
Afectación del ser humano	• Daño a terceros • Recurso humano (pérdida)	• Muerte, mutilación, incapacidad • Pérdida de conocimiento institucional

El apetito de riesgo, entendido como la cantidad de riesgo que la organización está dispuesta a aceptar cuando se trata de alcanzar sus objetivos[120], debe estar alineado con los objetivos de la organización y es la base para valorar la materialización del riesgo.

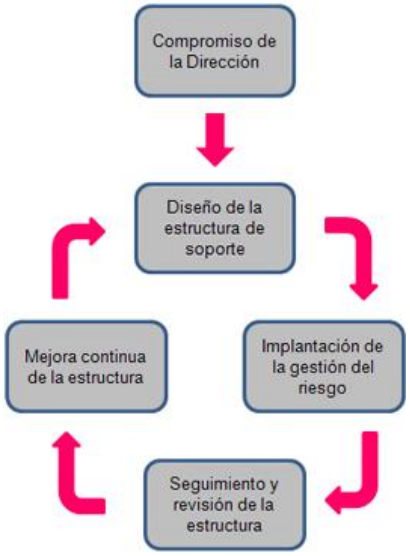
Este análisis, conlleva a que la organización entre a tomar decisiones entre:

[118] AZ/NZS 4360
[119] AZ/NZS 4360
[120] RiskIT

a. Evitar el riesgo: Decisión de no participar o retirarse de situaciones de riesgo[121].
b. Transferir el riesgo: Compartir con un tercero la pérdida o ganancia del riesgo.
c. Aceptar el riesgo: Decisión de aceptar un riesgo[122].
d. Monitorear el riesgo: Revisar, supervisar y observar de forma crítica o medir el progreso de una actividad, acción o sistema de forma regular para identificar cambios que alteren el contexto de riesgo o modifiquen el desempeño.

4.1.4. Estructura para la gestión del riesgo. El concepto de mejora continua introducido en los sistemas de gestión de la calidad ha sido extendido a otros sistemas de gestión, incluyendo el del riesgo. La norma ISO 31000:2009, en su cláusula cinco, plantea un ciclo de mejora continua (PHVA – Planear Hacer Verificar Actuar) en la cual, luego del compromiso de la dirección, se realiza el diseño del sistema (Planear), se implementa (Hacer), se realiza seguimiento y revisión (Verificar) y se mejora de forma continua la estructura (Actuar)

Figura 9. Estructura de gestión del riesgo (ISO 31000)

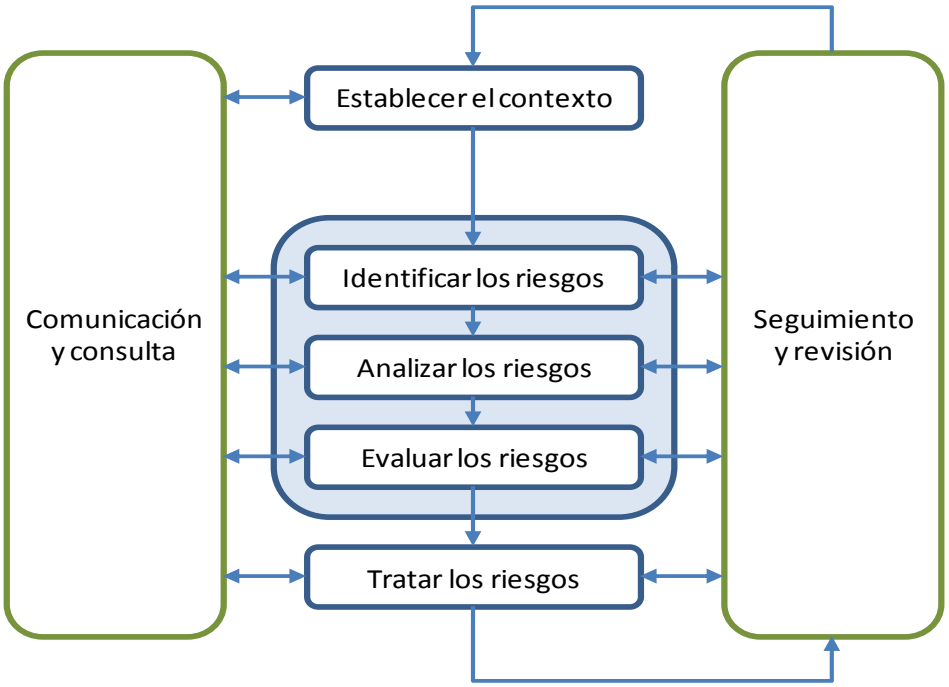


Fuente: ISO 31000

[121] ISO Guide 73
[122] AZ/NZS 4360

4.1.5. El proceso de gestión del riesgo. De igual manera, aplicando el concepto del enfoque basado en procesos y por ende el de mejora continua[123] que integra los sistemas de gestión de la calidad, la norma ISO 31000:2009, en su cláusula seis introduce, el proceso de gestión del riesgo, mostrado en la siguiente figura.

Figura 10. Proceso de gestión del riesgo (ISO 31000)



Fuente: ISO 31000

4.1.6. Riesgo de cumplimiento. El riesgo de cumplimiento sucede al incumplir total o parcialmente leyes, regulaciones, normas técnicas, estándares de auto-regulación de la organización, buenas prácticas y códigos de conducta aplicables a sus actividades.

El riesgo, participa en dos diferentes fases en la organización: Respecto a la obligación legal y/o contractual de adoptar, implementar y usar determinadas normas legales o técnicas, donde se puede configurar el riesgo de cumplimiento;

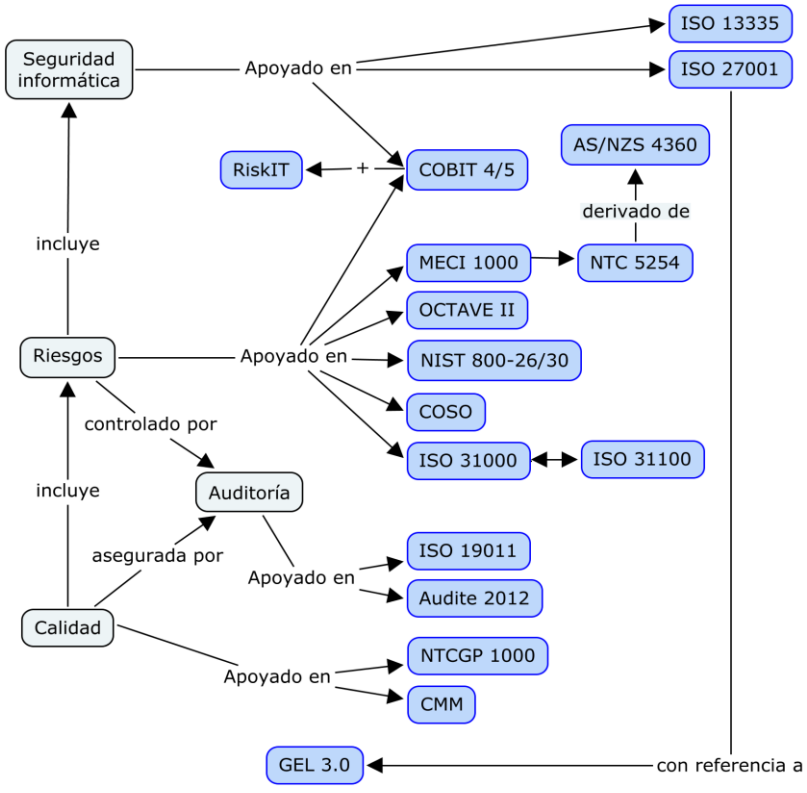
[123] Norma ISO 9001:2008 numeral 0.2

y sobre el riesgo inherente, o riesgo bruto que surge de la misma exposición a los factores de riesgos y que bajo controles conduce al riesgo residual, los cuales, de materializarse producirán un impacto sobre la organización. De tal forma, el riesgo debe analizarse en ambas facetas y considerando la gestión del cumplimiento, incluir necesariamente el riesgo de cumplimiento.

4.1.7. Medición del riesgo. Dentro de diversas mediciones, el Valor en el riesgo (VaR) mide la peor pérdida esperada en un intervalo de tiempo bajo condiciones normales en un nivel de confianza dado[124].

4.2. ARMONIZACION DE NORMAS EN GESTIÓN DEL RIESGO

Figura 11. Armonización de normas en gestión del riesgo

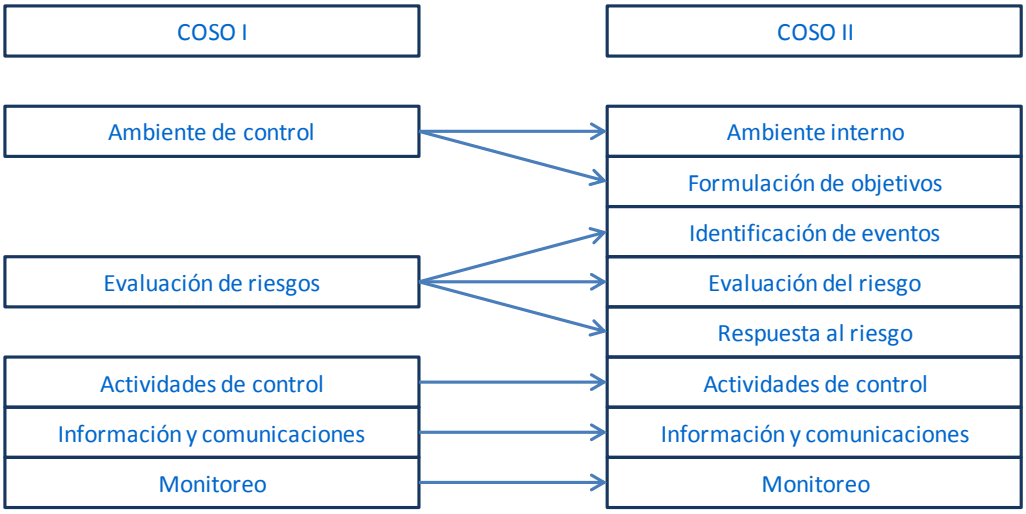


[124] DARLINGTON, Angela, GROUT, Simon. HOW SAFE IS SAFE ENOUGH? The staple in actuarial society. 2001.

El análisis de normas en gestión del riesgo será realizado con base en la norma ISO 31000:2009, frente a la cual se analizará cada una de las normas ampliamente aceptadas en gestión del riesgo.

4.2.1. COSO. El informe COSO (Committee of Sponsoring Organizations) fue creado por la Treadway Commission, originalmente como marco de referencia para el control interno (1992), fue luego ampliado (2004) hacia un marco de referencia en gestión del riesgo.

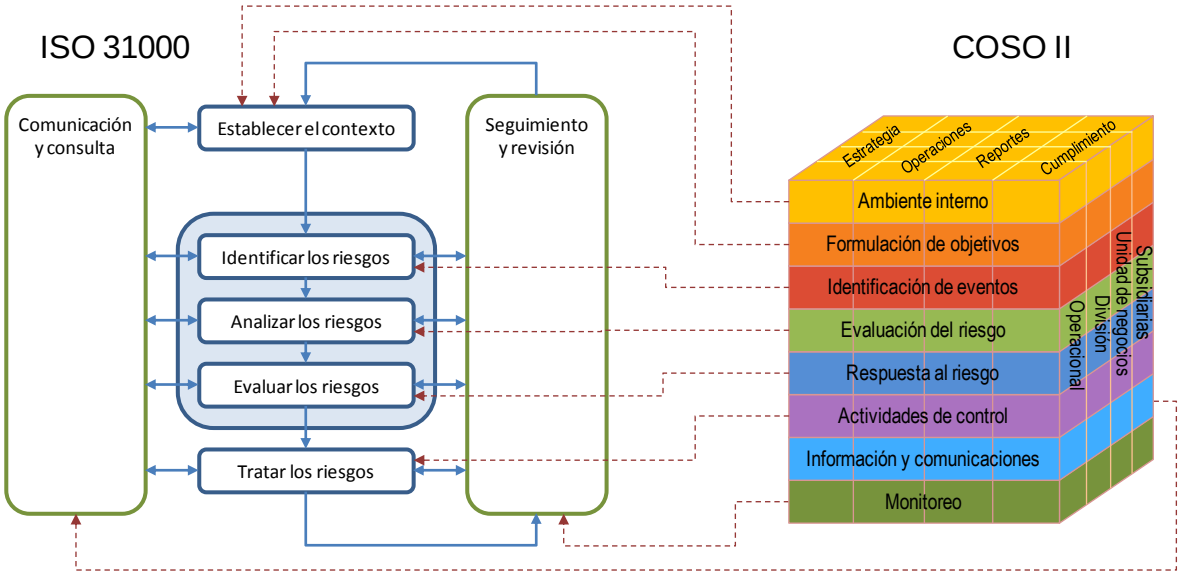
Figura 12. COSO I vs COSO II



Fuente: Comisión COSO

El informe COSO fue desarrollado sobre el de control interno, suministrando principios y conceptos clave, un lenguaje común así como directivas claras y explícitas. Guarda relación con el estándar ISO 31000 tal como se muestra en la siguiente ilustración:

Figura 13. ISO 31000 vs COSO II



Fuente: Comisión COSO

El COSO II tiene los siguientes componentes[125]:

a. Ambiente interno. Abarca el tono de una organización y establece la base de cómo el personal de la entidad percibe y trata el riesgo, incluyendo la filosofía de administración de riesgo, el riesgo aceptado, la integridad, valores éticos y el ambiente donde operan.
b. Formulación de objetivos. Los objetivos deben existir antes que la dirección pueda identificar potenciales eventos que afecten su consecución. La administración de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

[125] AUTOREGULADOR DEL MERCADO DE VALORES COLOMBIANO. Guía de control interno en la intermediación del mercado de valores. Bogotá. 2008

c. Identificación de eventos. Los eventos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades, las cuales revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.
d. Evaluación del riesgo. Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser administrados. Los riesgos son evaluados sobre una base inherente y residual bajo las perspectivas de probabilidad (posibilidad de que ocurra un evento) e impacto (su efecto debido a su ocurrencia), con base en datos internos (pueden considerarse de carácter subjetivo) y externos (más objetivos).
e. Respuesta al riesgo. La dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.
f. Actividades de control. Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo efectivamente.
g. Información y comunicaciones. La información clave se identifica, captura y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación efectiva debe producirse en un sentido amplio, fluyendo hacia abajo, a través, y hacia arriba de la entidad.
h. Monitoreo. Toda la administración de riesgos es monitoreada y efectúan modificaciones necesarias. Este monitoreo se lleva a cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones simultáneamente.

   La administración de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en el cual casi cualquier componente puede e influye en otro.

4.2.2. El Modelo Estándar de Control Interno (MECI). En Colombia, la Ley 87 de 1993 creó la obligatoriedad de implementar el control interno en los entes públicos territoriales y descentralizados. Mediante el Decreto 1599 de 2005, se adoptó por parte del estado colombiano el Modelo Estándar de Control Interno MECI 1000:2005[126] el cual incorpora la necesidad de la gestión del riesgo en las entidades públicas y está íntimamente ligado al modelo COSO y la norma AS/NZS 4360:2004 y su equivalente colombiano, la norma 5254 expedida por ICONTEC.

Tabla 8. ISO 31000 vs COSO II

SUBSISTEMAS	COMPONENTE	ELEMENTOS
De control estratégico	Ambiente de Control	Acuerdos, Compromisos o Protocolos Éticos Desarrollo del Talento Humano Estilo de Dirección
	Direccionamiento Estratégico	Planes y Programas Modelo de Operación por Procesos Estructura Organizacional
	Administración del Riesgo	Contexto Estratégico Identificación del Riesgo Análisis del Riesgo Valoración del Riesgo Políticas de Administración del Riesgo
De control de gestión	Actividades de control	Políticas de Operación Procedimientos Controles Indicadores Manual de Procedimientos
	Información	Información Primaria Información Secundaria Sistemas de Información
	Comunicación pública	Comunicación Organizacional Comunicación Informativa Medios de Comunicación
De control de evaluación	Autoevaluación	Autoevaluación del Control Autoevaluación de Gestión
	Evaluación independiente	Evaluación del Sistema de Control Interno Auditoría Interna
	Planes de mejoramiento	Plan de Mejoramiento Institucional Planes de Mejoramiento por Procesos Planes de Mejoramiento Individual

Fuente: ISO 31000

[126] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Modelo Estándar de Control Interno - MECI 1000:2005. Bogotá, 2005

Es importante observar como este modelo une en un único esquema la administración del riesgo, la gestión de la información tanto en el ámbito información de la información en sí como respecto a los sistemas de información, y de igual manera la evaluación autónoma y la independiente, resaltando allí el ejercicio auditor.

El MECI igualmente plantea una serie de objetivos de control, que incluyen:

a. **Objetivos de control de cumplimiento**, sobre las funciones a su cargo y en cuanto al marco normativo que le sea aplicable.
b. **Objetivos de control estratégico**, que aplica a la organización y estructura de la entidad y a la necesidad de realizar la gestión adecuada del riesgo.
c. **Objetivos de control de ejecución**, orientados a mantener las funciones, operaciones y actividades institucionales, la mejor gestión de los recursos, garantizar la generación y registro oportuno de información de calidad, y asegurar la comunicación.
d. **Objetivos de control de evaluación**, sobre la verificación y evaluación permanente.
e. **Objetivos de control de información**, que versa sobre la producción oportuna de la información que debe producir y manejar la entidad.

Estos objetivos de control plantean la obligatoriedad de la gestión del cumplimiento en las entidades del estado, que corresponde de manera directa a los objetivos de la presente investigación, además exigen la gestión del riesgo, la gestión adecuada de la información y la necesidad de la auditoría de manera continua operando sobre el mismo sistema de control interno - incluyendo la gestión del cumplimiento como la del riesgo - así como sobre la organización.

4.2.3. Objetivos de Control para Tecnología de Información (COBIT). Es un modelo estructurado, lógico, de mejores prácticas de Tecnología de Información, definidas por un consenso de expertos en todo el mundo en aspectos técnicos, seguridad, riesgos, calidad y control, a través de ISACA como autoridad[127]. Durante el proceso de desarrollo de esta investigación estaba en vigencia COBIT versión 4.1 al igual que las normas ValIT 2.0 y RiskIT, las cuales fueron integradas recientemente en la versión 5.0 de COBIT.

COBIT 5.0 cuenta con cinco principios (a diferencia de COBIT 4.1 que tiene cuatro)

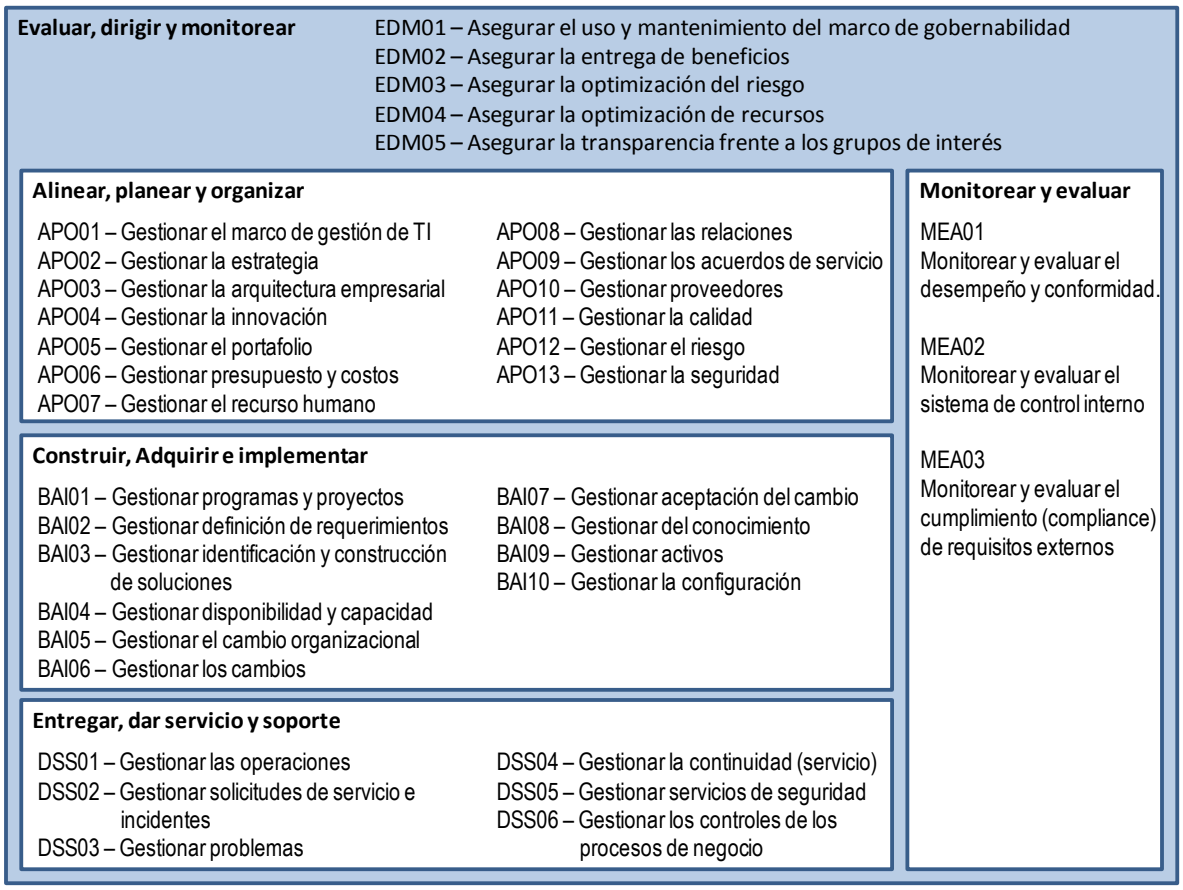
a. **Cumplir con las necesidades de los grupos de interés**. Las organizaciones deben crear valor para sus grupos de interés y mantener un balance entre sus beneficios y la optimización de riesgos y el uso de recursos.
b. **Cubrir todos los aspectos de la empresa**. COBIT plantea integrar la gobernabilidad de TI en la gobernabilidad institucional.
c. **Usar y aplicar un único e integrado marco de referencia**. COBIT busca participar como estándar de alto nivel que integre los aspectos de gobernabilidad de TI.
d. **Usar un enfoque integral**. COBIT busca la participación de los diversos componentes de TI, para lo cual define siete categorías: Principios, políticas y marcos de referencia; Procesos; Estructuras organizacionales; Cultura, ética y comportamiento; Información; Servicios, infraestructura y aplicaciones; así como la gente, destrezas y competencias.
e. **Separar gobernabilidad de la administración**. COBIT establece la diferencia entre la función y procesos de administración y gobernabilidad.

COBIT 5 adopta cinco macro procesos (que reemplazan y equivalen a los cuatro dominios de COBIT 4.1) con sus procesos (que suceden a los objetivos de control

[127] http://www.isaca.org

de COBIT 4.1). El siguiente diagrama muestra los procesos definidos en COBIT 5:

Figura 14. Procesos en COBIT 5



Fuente: ISACA. COBIT 5.

En el mapa de procesos de COBIT 5 resaltan los procesos EDM03, APO11, APO12, APO13, BAI09, BAI10, DSS04, DSS05, DSS06 así como MEA01, MEA02 y MEA03 que tratan directamente los aspectos relacionados con el riesgo. De igual forma, los controles MEA01 y MEA03 hacen referencia explícita al cumplimiento.

En cuanto a la comparación con otros estándares, se tiene que:

Tabla 9. Equivalencia de COBIT con otras normas

NORMA EXTERNA	PROCESOS EN COBIT	DOMINIOS
ISO/IEC 31000	Procesos relacionados con la gestión del riesgo	EDM y APO
ISO/IEC 27000	Procesos relacionados con seguridad y riesgo	EDM, APO, DSS
	Actividades relacionadas con seguridad	BAI
	Actividades de monitoreo y evaluación	MEA

De igual manera, los criterios de la información establecidos en COBIT 4.1 (Efectividad, Eficiencia, Integridad, Confiabilidad, Disponibilidad, Confidencialidad y Cumplimiento) son ahora gestionados como criterios facilitadores de la calidad (en COBIT 5), los cuales son desarrollados en la siguiente tabla.

Tabla 10. Comparación de criterios de información de COBIT 4 y 5.

COBIT 4.1	COBIT 5	
	DESCRIPCION	CRITERIOS DE CALIDAD
Efectividad	La información (como producto) es efectiva si suple las necesidades del consumidor de información.	Cantidad apropiada Relevancia Comprensibilidad Interpretabilidad Objetividad
Eficiencia	Refiere a la facilidad con la que se obtiene información bajo el criterio de información como servicio.	Credibilidad Accesibilidad Facilidad de uso Reputación
Integridad	La información se reputa integra si es libre de errores y es completa.	Completitud Precisión
Confiabilidad	Hace referencia a si la información se considera cierta, es creíble y de fuente confiable	Credibilidad Reputación Objetividad

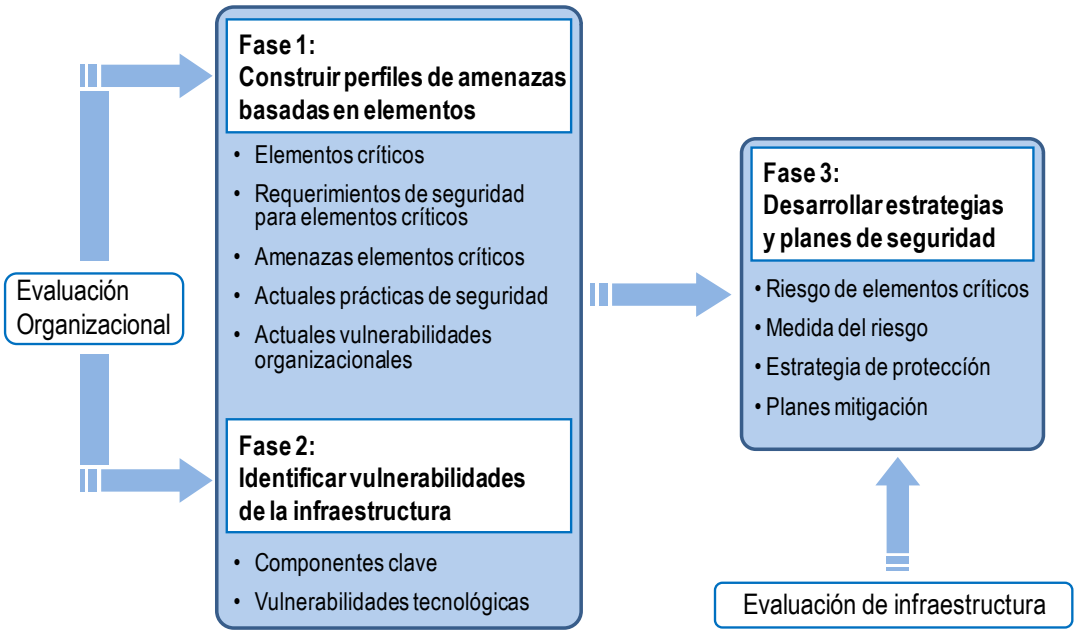
Disponibilidad	Es una meta de calidad de COBIT 5 y une conceptos de Accesibilidad y Seguridad	Accesibilidad
Confidencialidad	Es una meta de calidad de COBIT 5 sobre calidad en el acceso a la información	Accesibilidad
Cumplimiento	La información debe ser conforme (cumplir) respecto a las especificaciones tanto en calidad de información como en cuanto a requerimientos legales	Cumplimiento

Los aspectos de calidad de la información han sido tratados igualmente en este documento desarrollando mecanismos de identificación y cuantificación de criterios de calidad.

4.2.4. Operationally Critical Threat, Asset Vulnerability Evaluation (OCTAVE). Es un modelo en el cual concurren organismos académicos (Carnegie Mellon University) y de tipo público: los Departamentos de Defensa y de Estado de Estados Unidos (DoD y DoS), orientado a la gestión de riesgos asociados a la seguridad de la información.

OCTAVE provee un enfoque para la identificación y tratamiento de los riesgos respecto a la seguridad enfocado a los activos o dominios que pueden ser afectados, desarrollado de manera completa, sistemática, según el contexto y auto-dirigida. OCTAVE está organizado mediante un proceso de tres fases:

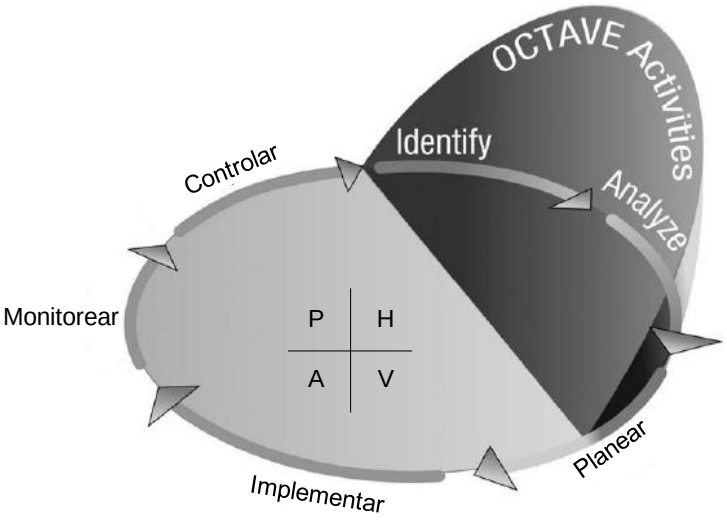
Figura 15. Procesos en OCTAVE



Fuente: OCTAVE

Las tres fases del proceso OCTAVE se integran al ciclo PHVA de la siguiente manera:

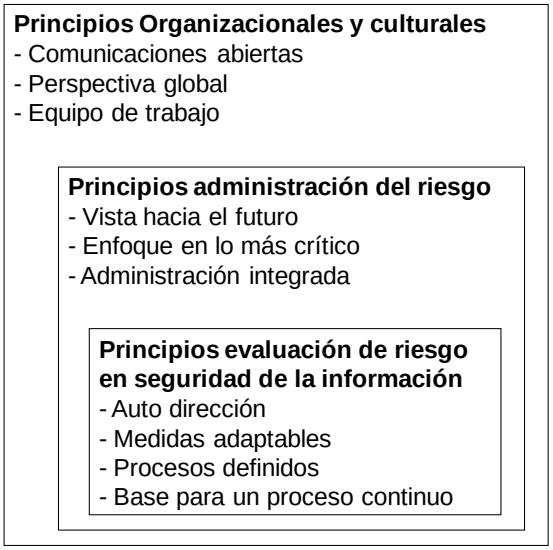
Figura 16. El ciclo de mejora continua en OCTAVE



Fuente: OCTAVE

De igual manera, OCTAVE establece su propio conjunto de principios bajo un modelo de capas envolventes, iniciando, desde afuera, con los organizacionales y culturales, yendo a los de administración del riesgo, para llegar a los de la evaluación del riesgo en seguridad de la información. Los primeros están alineados con los de ambiente interno (COSO) o de establecimiento del contexto (ISO 31000) mientras que los demás desarrollan los demás aspectos de los modelos equivalentes (COSO o ISO 31000)

Figura 17. Principios en OCTAVE



Fuente: OCTAVE

4.3. GESTION DEL RIESGO ORGANIZACIONAL

4.3.1. Oficial de cumplimiento / oficina de cumplimiento. El oficial de cumplimiento (Chief Compliance Officer - CCO) o en su defecto la oficina de cumplimiento (Office of Compliance) son los responsables por determinar, gestionar y desarrollar los aspectos relativos al cumplimiento en una organización. Entre sus funciones pueden incluir:

- Liderar la planeación, implementación, medición y evaluación del desempeño.
- Realizar el monitoreo y evaluación continua del cumplimiento.
- Asesorar en mejores prácticas para el logro del cumplimiento.
- Mejorar la calidad de la información relacionada con cumplimiento.
- Fortalecer el recurso humano a través de programas de capacitación efectivos.
- Apoyar el desarrollo, formulación y mantenimiento de políticas, guías, sistemas, procesos y documentación orientados al cumplimiento.
- Realizar vigilancia tecnológica y técnica sobre nuevos aspectos que impacten los temas de cumplimiento en la organización.
- Controlar los planes de acción, de mejoramiento y de auditoría.
- Promueve la comunicación efectiva a nivel sectorial y gubernamental sobre los aspectos de cumplimiento, herramientas, tecnologías, mejores prácticas y normas aplicables del orden normativo y técnico.
- Mantiene y analiza los registros e indicadores relativos al cumplimiento.

4.3.2. Oficial de riesgo / oficina de gestión del riesgo. El oficial de gestión del riesgo (Chief Risk Officer - CRO) o en su defecto la oficina de gestión del riesgo (Risk management Office) son los responsables de administrar de forma eficiente y efectiva los riesgos de la organización, en sus diferentes categorías: estratégicos, reputacionales, operacionales, financieros, humanos o de cumplimiento. Trabaja de la mano con la alta dirección de la compañía y la oficina de cumplimiento o el oficial de cumplimiento de la organización. Entre sus responsabilidades aparece:

- Liderar la planeación, implementación, medición y evaluación del riesgo.
- Desarrollar e implementar el programa de gestión del riesgo en la organización de tal manera que se proporcione seguridad razonable del logro de los objetivos de la organización mientras cumple con las regulaciones, normas legales y técnicas, así como acuerdos establecidos.

- Desarrolla e implementa sistemas, políticas y procedimientos para la identificación, valoración, análisis y medición de los riesgos.
- Investiga y determina fuentes, causas, factores, patrones y tendencias de riesgo.
- Establece puntos y mecanismos de control así como soluciones efectivas para la mitigación del riesgo.
- Mantiene actualizado y capacitado al personal necesario sobre la gestión del riesgo.
- Multiplica su gestión en las diferentes secciones de la organización buscando la gestión específica del riesgo en cada uno de los departamentos de la entidad.
- Recopila, mantiene y analiza datos relativos a la gestión del riesgo.
- Busca asegurar la calidad de la información relacionada con el riesgo.
- Facilita la comunicación con las partes interesadas, especialmente los accionistas, empleados, proveedores, usuarios, aseguradoras, el estado, entes reguladores y la comunidad en general sobre los riesgos que le puedan impactar.
- Trabaja de manera continua sobre la mejora continua frente al riesgo.
- Realiza auditorias de política y cumplimiento frente a estándares técnicos y normas, desde la óptica del riesgo.

4.3.3. Obligatoriedad de la gestión del riesgo en Colombia. En Colombia, la Ley 87 de 1993 (mediante la cual se crea el Control Interno), su Decreto reglamentario 1599 de 2005 (mediante el cual se adoptó el modelo estándar de control interno MECI 1000:2005), y en especial el Decreto 1537 de 2001 que establece "…la identificación y análisis del riesgo debe ser un proceso permanente…" son las bases legales generales a partir de la cual se establece la obligatoriedad de la gestión del riesgo.

Sin embargo, en otros sectores de la economía, como el financiero, las Circulares 048 y 061 emitidas por la Superintendencia Financiera de Colombia exigen a las entidades vigiladas, la implementación del Sistema de Administración de Riesgo Operativo (SARO), de lavado de activos y financiación del terrorismo (SARLAFT) en el 2007; en el sector salud, el Sistema Obligatorio de Garantía de la Calidad (Decreto 1011 de 2006) y las normas que establecen los requisitos habilitadores para Empresas Promotoras de Salud (EPS y EPS-S, especialmente la Resolución 1740 de 2008) e instituciones prestadoras de servicios de salud (Resoluciones 1043 de 2006 y 2680 de 2007) incluyen la gestión del riesgo como exigencia fundamental en la habilitación institucional; por citar algunos casos.

En cuanto a la gestión de la información, además de los formatos electrónicos de reporte de información establecidos por los diversos entes de control y regulación del estado es numerosa la materia legal sobre información y la necesaria gestión del riesgo, en especial la Ley 1273 de 2009 que crea la Información como bien jurídico tutelado y tipifica los delitos informáticos, el Decreto 2150 de 1995 que autoriza el uso de sistemas electrónicos de archivo y transmisión, el Decreto 1748 de 1995 en el tema de los archivos laborales informáticos, la Ley 270 de 1996 que dicta el uso y valor probatorio de nuevas tecnologías en la administración de justicia, la Ley 527 de 1999 sobre los mensajes de datos electrónicos y comercio electrónico, la ley 594 de 2000 que exige la gestión de los documentos incluyendo soportes digitales, la Ley 573 de 2000 que establece la modernización y tecnificación del estado como mecanismos para lograr la eficacia y eficiencia del estado, la Ley 812 de 2003 que ordena la incorporación de técnicas de gerencia moderna en las entidades del estado, la Ley 962 de 2005 que concretó el principio de neutralidad tecnológica, los Decretos 1094 de 1996, 1165 de 1996, 1001 de 1997 y 1929 de 2007 que reglamentan la factura electrónica en Colombia, la Circular Externa 052 de 2007 de la Superintendencia Financiera de Colombia, que establecen los estándares mínimos de seguridad y calidad para manejo de información en los medios y canales de distribución de productos y servicios.

5. LA AUDITORIA

Conforme a lo establecido en la norma internacional de auditoría en sistemas de gestión ISO 19011:2011[128], se tiene que la auditoría es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoria (3.3) y evaluarlas objetivamente a fin de determinar hasta qué punto los criterios de auditoría (3.2) se cumplen.

5.1. NORMAS DE AUDITORÍA

Así como existe un complejo universo de normas técnicas, igualmente sucede para las normas, guías y métodos de auditoría, donde a nivel nacional e internacional aparecen varias iniciativas, donde se puede resaltar:

5.1.1. Nacional.

a. Las Normas de Auditoría Generalmente Aceptadas[129], aprobadas por el Congreso de la República mediante la ley 43 de 1990 y se dividen en normas generales, normas relativas a la ejecución del trabajo y normas relativas a la información.

b. La Guía de Auditoría Gubernamental con Enfoque Integral – Audite, versión 4.0, establece las actividades primordiales y fases del proceso auditor aplicado a las auditorías realizadas a entidades públicas o vigiladas.

[128] ISO 19011:2011
[129] CUÉLLAR, Guillermo Adolfo. Teoría General de la Auditoría y Revisoría Fiscal. Huila: Universidad del Cauca. 2003.

5.1.2. Internacional.

a. Normas Internacionales de Auditoría (NIA). el Comité Internacional de Normas de Auditoría y Seguridad (IAASB, en inglés), completó el proyecto Clarity[130] (Claridad) por el cual está reformando las NIA y la ISQC 1 (Norma Internacional de Control de Calidad). Estas normas clarificadas son efectivas para realizar auditorías de estados financieros a partir del 15 de diciembre de 2009 y son referencia para las normas locales de varios países.

b. La asociación internacional de auditores de sistemas ISACA establece las guías, principios y metodologías de auditoría[131] [132].

c. El Instituto Internacional de Auditoria, IIA[133], igualmente establece lineamientos base para la realización de auditorías, especialmente en el ámbito financiero.

d. Norma técnica de auditoría de sistemas de gestión. La norma ISO 19011:2002 establece directrices técnicas para realizar auditorías de sistemas de gestión en el ciclo auditor: planeación, realización, informe y revisión de la auditoria.

5.2. CONCEPTUALIZACION

5.2.1. Auditorías de parte. Según el organismo que realiza la auditoría y el propósito de la misma, se tiene la siguiente clasificación:

[130] INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD – IAASB. Proyecto Clarity – Nuevas normas internacionales de auditoría. Nueva York: http://www.ifac.org/iaasb/ProjectHistory.php?ProjID=0024, 2010

[131] ISACA. IT Audit and Assurance Guidelines. Rolling Meadows, IL: http://www.isaca.org, 2009.

[132] ISACA. IT Audit and Assurance Tools and Techniques. Rolling Meadows, IL: http://www.isaca.org, 2009.

[133] THE INSTITUTE OF INTERNAL AUDITORS. International standards for the professional practice of internal auditing (standards). Miami, FL: http://www.theiia.org/, 2009

a. **Primera Parte**: Auditorías internas realizadas por, o en nombre de, la propia organización para la revisión por la dirección y otros fines internos, y pueden ser la base para una auto-declaración de conformidad de la organización.

b. **Segunda Parte**: Externas realizadas por partes que tienen interés en la organización, como los clientes, o por otras personas en su nombre.

c. **Tercera Parte**: Llevadas a cabo por organizaciones auditoras independientes externas, tales como aquellas que ofrecen registro o certificaciones de conformidad de acuerdo con los requisitos de la norma.

d. **Auditoria conjunta**: realizada entre varias organizaciones

5.2.2. Modalidades de auditoría. Según el énfasis en los objetos o temas auditados, se tienen las siguientes modalidades de auditoría:

a. **Regular**: Se aplica al sujeto y/o punto de control por decisión interna o externa, para propósitos de certificación, emitir conceptos sobre la gestión.

b. **Especial**: Cuando existe un interés especial en examinar uno o varios procesos del sujeto o punto de control. Permite focalizar la acción del control y agilizar el desarrollo del proceso auditor. Los resultados de la auditoría especial pueden ser tomados en la auditoría regular como insumo para emitir los pronunciamientos finales sobre la opinión y el concepto que se incluye en el dictamen

c. **Seguimiento**: Se aplica sobre planes de mejora o planes de acción surgidos de manera propia o a partir de otras auditorias.

5.2.3. Participantes de auditoría.

a. **Auditado**: Organización objeto de una auditoria.

b. **Auditor**: Persona con la competencia para realizar una auditoría.

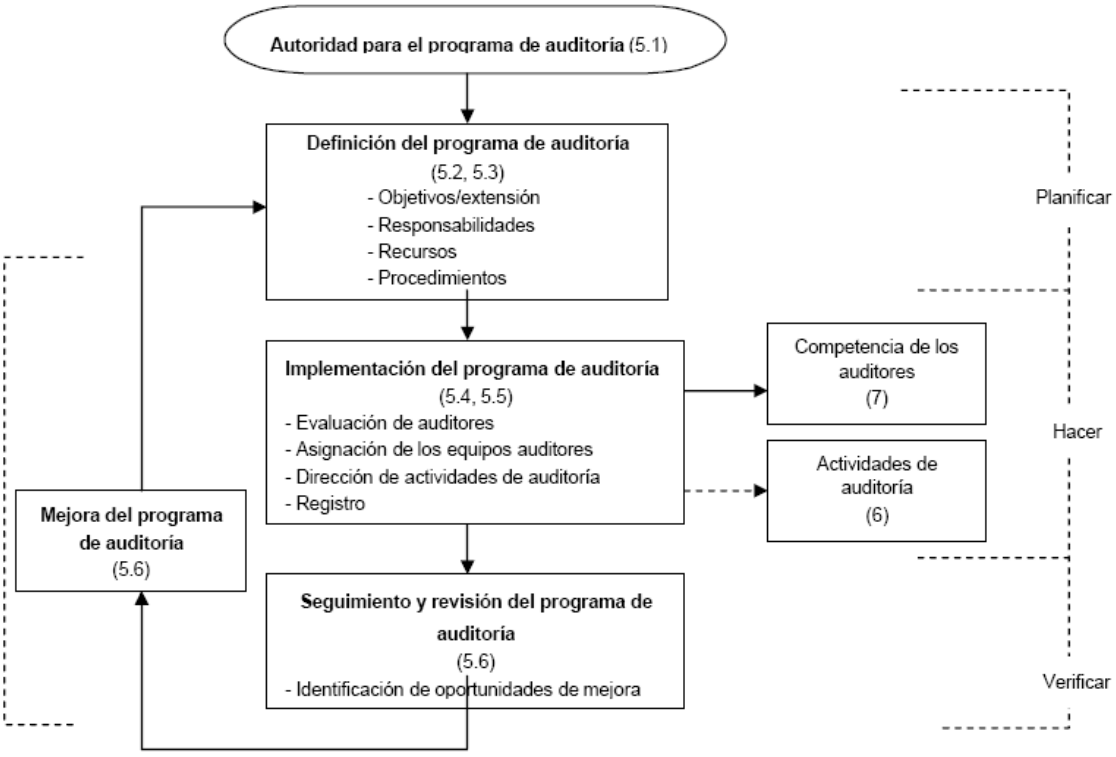
c. **Equipo Auditor**: Uno o más auditores que realizan una auditoria, ayudado por expertos técnicos, si es necesario.
d. **Experto Técnico**: Persona que aporta conocimientos específicos o experiencia al equipo auditor.

5.3. EL PROCESO DE AUDITORIA

Considerando las dos normas generalmente reconocidas, tanto a nivel de sistemas de gestión (ISO 19011:2011) como de auditoría en el sector público (AUDITE), se tiene el siguiente esquema de proceso por norma

5.3.1. ISO 19011. El proceso de auditoría expresado en la norma ISO 19011 consiste en un ciclo de mejora continua (PHVA) donde la planeación se realiza al definir el programa de auditoría (numerales 5.2 y 5.3 de la norma ISO 19011), el componente relativo al hacer se realiza en la implementación del programa de auditoría (numerales 5.4 y 5.5), siendo la fase de verificación la correspondiente al seguimiento y revisión del programa de auditoría (numeral 5.6) y la etapa de mejora continua denominada mejora del programa de auditoría (numeral 5.6). Todo el ciclo, conforme se plantea en las normas de sistemas de gestión, especialmente de calidad, surge de la alta dirección (numeral 5.1) en este caso, la autoridad para el programa de auditoría. En la práctica el ciclo de auditoría hace que coexista el ciclo de gestión del sistema auditado con el de auditoría.

Figura 18. Proceso de auditoría (ISO 19011)

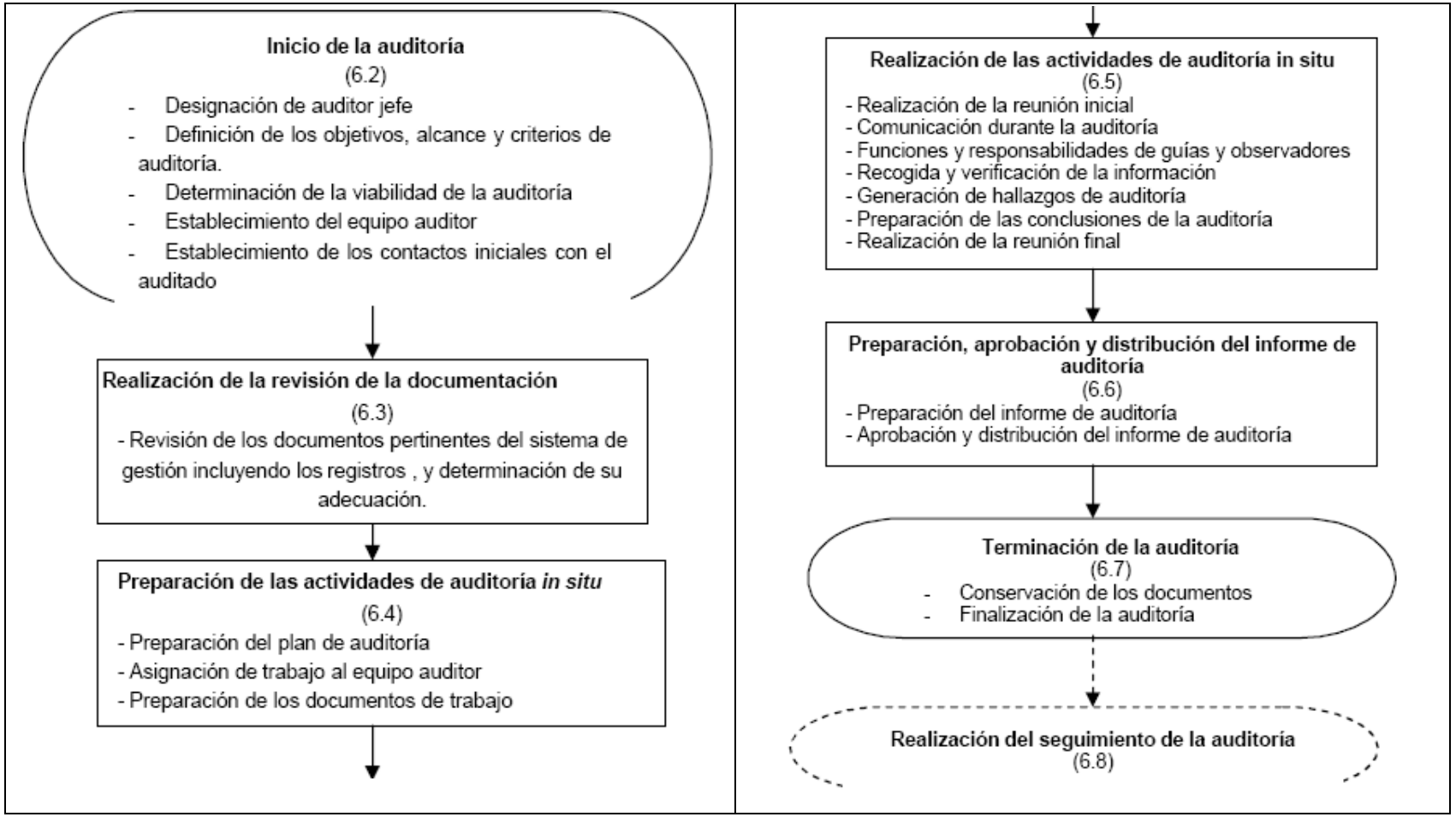


Fuente: ISO 19011

El proceso auditor puede estar orientado a obtener una certificación, o garantía escrita y válida proporcionada por un tercero sobre un producto o servicio al cumplir plenamente los requisitos especificados del área en cuestión (normas).

El proceso de auditoría se despliega de la siguiente forma, tal como lo especifican los numerales 6.2 (planeación), los 6.3 a 6.7 (hacer) y 6.8 (verificación).

Figura 19. Despliegue del proceso de auditoría



Fuente: ISO 19011

Según la norma, el programa de auditoría debe estar orientado a los siguientes aspectos:

a. Prioridades de gestión;
b. Intenciones comerciales;
c. Requisitos del sistema de gestión;
d. Requisitos legales y contractuales;
e. Necesidad de evaluación del proveedor;
f. Requisitos del cliente;
g. Necesidades de otras partes interesadas;
h. Riesgos potenciales a la organización.

De igual manera, la norma establece registros especiales de auditoría, incluyendo:

a. Registros de auditoría individuales:
- planes de auditoría;
- informes de auditoría;
- informes de no-conformidades; y
- informes de acciones preventivas y correctiva;

b. Resultados de la revisión del programa de auditoría;

c. Registros del personal de auditoría:
- evaluación del auditor;
- selección del equipo auditor; y
- formación.

5.3.1.1. Métodos de auditoría. La norma ISO 19011 identifica diversos métodos para llevar a cabo los objetivos de auditoría entre los cuales se incluye:

a. **Examen o prueba**. Herramientas para obtener evidencias que fundamentan conclusiones. Busca analizar y/o poner a prueba la calidad y el cumplimiento de requisitos (funciones, actividades, operaciones, rangos) que afectan la funcionalidad, confiabilidad, seguridad, estabilidad, administración y control.
   - Cumplimiento: Las Pruebas de Cumplimiento son procedimientos utilizados para comprobar cumplimiento de procedimientos de control en la organización.
   - Sustantivas: Las Pruebas Sustantivas son los procedimientos para evaluar la integridad de las transacciones individuales, los datos u otra información.

b. **Inspección**. Examina y evalúa el funcionamiento, la eficiencia y la eficacia sistemas, operación y proceso datos, Gestión Administrativa, actividades, estructura organizativa y otros componentes. Este método se usa para verificar componentes y/o participantes del proceso informativo así como para determinar el cumplimiento de requisitos.

c. **Confirmación**. Examen de hechos y certificación de datos, oportunidad, confiabilidad, veracidad, autenticar, validar la información en una base objetivo.

d. **Comparación**. Información de datos y procesos de la misma organización frente a otras similares.

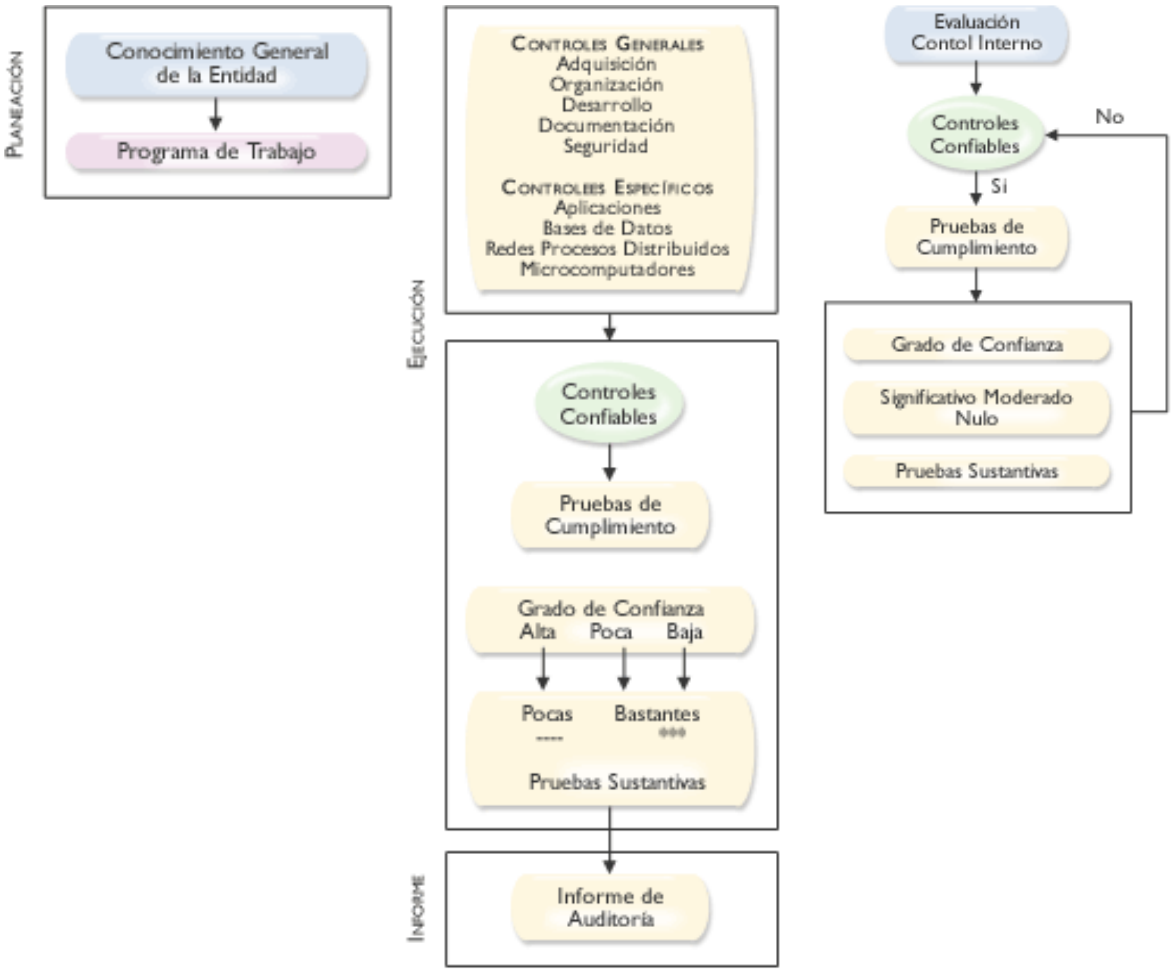
e. **Revisión documental**. Actividad fundamental consistente en la revisión de evidencia a nivel de documentación, del adecuado registro de datos y el cumplimiento de reglas.

Es el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos[134] [135].

[134] HERNANDEZ, Enrique. Auditoría en Informática. 2ª edición. Ciudad de México: Editorial

5.3.2. Audite. La Contraloría General de la República, en Colombia, en ejercicio de sus funciones legales y constitucionales, estableció una norma general de auditoría con énfasis fiscal con su respectivo proceso auditor. Hasta la versión 4.0 era una norma específica en cuanto a sus actividades y desde el año 2012 se convirtió en una norma general de manera similar a las normas internacionales, especialmente la ISO 19011.

Figura 20. Proceso de auditoría (Audite)



Fuente: Contraloría General de la Nación

Continental, 2000.

[135] PIATTINI, Mario G.– EMILIO DEL PESO. Auditoria Informática Un Enfoque Practico. 2ª edición. México: Alfa y Omega, 2001

Dado su enfoque fiscal, el AUDITE está orientado a auditar de manera general:

a. Adquisiciones: Procedimientos implementados por una entidad con el fin de hacer más efectiva, eficiente y económica la adquisición de recursos, incluidos los tecnológicos.

b. Organizacional: Políticas, normas, procedimientos orientados a la función de tecnología de información para asegurar que la entidad posea: estructura organizacional adecuada; planes informáticos alineados con los planes de la entidad; definición de políticas, procedimientos, funciones, y comités de sistemas que garanticen la dirección de los recursos informáticos como apoyo a la Entidad para el logro de los objetivos institucionales.

c. Desarrollo: Metodología para el desarrollo y mantenimiento de sistemas de información y de controles establecidos.

d. Documentación: Existencia de políticas sobre la documentación de las actividades desarrolladas en la dependencia de informática.

e. Seguridad: procedimientos, medidas y mecanismos de control que protegen los recursos informáticos (conservación del entorno y restricción y control de accesos lógicos a los sistemas de información y físicos a la infraestructura) de su uso no autorizado, modificación, daño o pérdida.

Y de manera específica:

a. Aplicaciones: Aplicaciones en producción en términos de automatización, funcionalidad y satisfacción de los usuarios, cantidad de recursos inmersos, grado de obsolescencia.

b. Bases de datos: Políticas, normas y procedimientos para la administración de las bases de datos, que garanticen la seguridad, la confiabilidad y la oportunidad de la información contenida en ellas.

c. Equipos de cómputo: Políticas, normas y procedimientos establecidos para garantizar la adecuada adquisición, utilización y administración de estos recursos.

6. CALIDAD DE LA INFORMACION

El concepto de calidad de información (CI) está ligado a la función informática, siendo pieza clave de la investigación en ingeniería de sistemas, sin que exista una única definición o patrón base para la cualificación del nivel de calidad de la información.

La calidad de la información puede definirse[136] como la suma de características referentes o relacionadas con la calidad de la información que satisfacen o aún exceden las necesidades de los consumidores de información[137] [138] considerando que solo información de alta calidad permite tomar decisiones razonables.

6.1. DIMENSIONES DE LA CALIDAD DE LA INFORMACION

Conforme a diversos estudios[139] [140] [141] [142] [143] [144] que confirman que la calidad de la información es un concepto multidimensional[145] y en especial el modelo AIMQ[146] donde participaron investigadores de College of Business Administration,

[136] RUŽEVIČIUS J., GEDMINAITĖ A.. peculiarities of the business information quality assessment. 2007
[137] ENGLISH L. Information Quality: Meeting Customer need, Information Impact Newsletter. 1996
[138] ENIAC. – Internet: http://www.thocp.net/hardware/eniac.htm
[139] BALLOU, D.P., PAZER, H.L. Modeling data and process quality in multi-input, multi-output information systems. Management Science 31, 2, (1985), 150–162.
[140] BALLOU, D.P., WANG, R.Y., Pazer, H. and Tayi, G.K. Modeling information manufacturing systems to determine information product quality. Management Science 44, 4 (1998), 462–484.
[141] HUANG, K. ,LEE, Y., WANG, R. Quality Information and Knowledge. Prentice Hall, Upper Saddle River: N.J. 1999.
[142] REDMAN, T.C., ed. Data Quality for the Information Age. Artech House: Boston, MA., 1996.
[143] WAND, Y., WANG, R.Y. Anchoring data quality dimensions in ontological foundations. Commun. ACM 39,11. 1996, 86–95.
[144] WANG, R.Y., STRONG, D.M. Beyond accuracy: what data quality means to data consumers. Journal of Management Information Systems 12, 4 (1996), 5–34.
[145] PIPINO, Leo L., LEE, Yang W., WANG, Richard Y.. Data Quality Assessment.
[146] YANG W. Leea, STRONGB, Diane M., KAHNC, Beverly K., WANG, Richard Y.. AIMQ: a methodology for information quality assessment. Elsevier Science B.V., 2002.

Northeastern University, Boston; Worcester Polytechnic Institute, Management Department, Worcester; Sawyer School of Management, Suffolk University, Suffolk; MIT, UC, Berkerley and Boston University, Boston; se tienen las siguientes dimensiones de calidad de la información ampliamente reconocidas por la industria y sientan las bases para la investigación en la ciencia de la calidad de la información y su posterior desarrollo[147] [148] que concuerdan con los enfoques comunes para identificar las dimensiones de calidad de la información[149] [150]

a. **Calidad intrínseca**: La calidad de la información por sí misma y la fuente de la cual proviene.

b. **Calidad contextual**: La calidad de la información debe ser considerada en el contexto en el cual se usa y por lo cual añade valor.

c. **Calidad en su representación**: La información debe estar representada de manera adecuada en el (los) mecanismo(s) de almacenamiento de forma que sea interpretable, fácil de entender, portable, fácil de manipular, y representada de manera concisa y consistente garantizando el significado y la integridad de la información.

d. **Calidad en su accesibilidad**: La información debe ser accesible de manera oportuna pero de manera segura (introduciendo el concepto de seguridad de la información) y sin obstáculos. Hace énfasis en el concepto de sistema.

---

[147] AL-HAKIM L.. Information Quality Deployment, Proceeding of Ninth International Conference on Information Quality, p.170-182. 2004 – Internet: http://www.iqconference.org/Documents/IQ%20Conference%202004/Papers/IQFunctionDeployment.pdf

[148] WANG, R.Y.. A product perspective on total data quality management, Communications of the ACM. 1998. Internet: http://mitiq.mit.edu/Publications.htm#1998

[149] PIERCE, E., KAHN, B., MELKAS, H. “A comparison of quality issues for data, information, and knowledge”, in Khosrow-Pour, M. (ed.), Emerging Trends and Challenges in Information Technology Management: Proceedings of the 2006 Information Resources Management Association Conference. 17th IRMA International Conference, Washington, 2006, pp. 21–24.

[150] MELKAS, Helinä, UOTILA, Tuomo. Quality of data, information and knowledge in technology foresight processes. Lappeenranta University of Technology, Lahti Unit, Finland.

El modelo AIMQ analiza la óptica académica y de la industria, como mecanismo que permita generar un inventario base de sub-dimensiones para las dimensiones enunciadas, considerando que:

En la vista académica, el primer enfoque (Zmud[151]) corresponde a una investigación pionera en calidad de la información generando sus propias sub-dimensiones en cada caso, el segundo representa los identificados por los autores de la metodología AIMQ de tipo pionera. Los siguientes tres estudios fueron derivados de los primeros, Jarke y Vassiliou[152] a partir de Wang-Strong[153], Delone y McLean[154] a partir de reportes de calidad de la información provenientes de nueve estudios en especial el de Bailey y Pearson sobre satisfacción del usuario[155], y en el caso de Godhue[156] que proviene de una búsqueda en la literatura existente para determinar las características clave para administradores de sistemas. En el caso de los estudios de Ballou y Pazer[157] se hace énfasis en dimensiones de tipo intrínseco medibles de forma directa, mientras que Wand y Wang[158] toma un enfoque ontológico para definir las dimensiones de estudio.

[151] ZMUD, R., Concepts, theories and techniques: an empirical investigation of the dimensionality of the concept of information, Decision Sciences 9, 1978, pp. 187–195.
[152] JARKE, M., VASSILIOU, Y., Data warehouse quality: a review of the DWQ project, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 299–313.
[153] WANG, R.Y., STRONG, D.M., Beyond accuracy: what data quality means to data consumers, Journal of Management Information Systems, 1996, pp. 5-34.
[154] DELONE, W.H., MCLEAN, E.R., Information systems success: the quest for the dependent variable, Information systems research, 1992, pp. 60–95.
[155] BAILEY, J.E., PEARSON, S.W., Development of a tool for measuring and analyzing computer user satisfaction, Management Science 29 (5), 1983, pp. 530–545.
[156] GOODHUE, D.L., Understanding user evaluations of information systems, Management Science 41, 1995, pp. 1827–1844.
[157] BALLOU, D.P., PAZER, H.L., Modeling data and process quality in multi-input, multi-output information systems, Management Science. 1985, pp. 150–162.
[158] WAND, Y., WANG, R.Y., Anchoring data quality dimensions in ontological foundations, Communications of the ACM 39, 1996, pp. 86–95.

6.1.1. Vista académica de información de la calidad.

Tabla 11. Revisión académica de la calidad de la información

	Calidad intrínseca	**Calidad contextual**	**Calidad representacional**	**Calidad accesabilidad**
Zmud	Exactitud (accuracy) Real (factual)	Cantidad (quantity) Confiable (reliable) Oportuno (timely)	Organización (arrangement) Legible (readable) Razonable (reasonable)	
Wang y Strong	Exactitud (accuracy) Credibilidad (Believability) Reputación (reputation) Objetividad (Objectivity)	Valor añadido (value added) Relevancia (relevance) Completo (completeness) Temporal (timeliness) Apropiado (appropriate amount)	Inteligibilidad (understanbility) Interpretabilidad (interpretability) Conciso (concise) Consistente (concistent representation)	Accesabilidad (accesability) Facilidad (ease of operation) Seguridad (security)
Jarke y Vassiliou	Exactitud (accuracy) Credibilidad (Believability) Credibilidad (credibility) Consistencia (consistency) Completitud (completeness)	Relevancia (relevance) Uso (usage) Temporal (timeliness) Actualización (currency source) Actualización de los datos (datawarehouse currency) No volatilidad (non volatility)	Interpretabilidad (interpretability) Sintaxis (syntax) Control de versiones (version control) Semántica (semantics) Sinónimos (aliases) Origen (origin)	Accesabilidad (accesability) Disponibilidad del sistema (system availability) Disponibilidad transacción (transaction availability) Privilegios (privileges)

Delone y McLean	Exactitud (accuracy) Precisión (precision) Confiabilidad (reliability) No desviación (freedom from bias)	Importancia (importance) Relevancia (relevance) Utilidad (usefulness) Informatividad (informativeness) Contenido (content) Suficiencia (sufficiency) Completo (completeness) Actualización (currency) Temporal (timeliness)	Inteligibilidad (understanbility) Legibilidad (readability) Claridad (clarity) Formato (format) Apariencia (appearance) Conciso (conciseness) Único (uniqueness) Comparable (comparability)	Usable (usableness) Cuantitativo (quantitativeness) Conveniencia del acceso (convenience of access)
Ballou y Pazer	Exactitud (accuracy) Consistencia (consistency)	Completo (completeness) Temporal (timeliness)		
Goodhue	Exactitud (accuracy) Confiabilidad (reliability)	Actualización (currency) Profundidad (level of detail)	Compatible (compatibility) Significante (meaning) Presentación (presentation) No confuso (lack of confusion)	Accesabilidad (accesability) Casos de uso (case of use) Localización (locatability)
Wand y Wang	Correcto (correctness) No ambiguo (unambiguous)	Completo (completeness)	Significante (meaningfulness)	

6.1.2. Vista de la industria de información de la calidad.

Tabla 11. Revisión industrial de la calidad de la información

	Calidad intrínseca	Calidad contextual	Calidad representacional	Calidad accesabilidad
DoD[159]	Exactitud (accuracy) Completo (completeness) Consistencia (consistency) Validez (validity)	Temporal (timeliness)	Único (uniqueness)	
MITRE[160]	Exactitud (accuracy) Credibilidad (Believability) Reputación (reputation) Objetividad (Objectivity)	Valor añadido (value added) Relevancia (relevance) Completo (completeness) Temporal (timeliness) Apropiado (appropriate amount)	Inteligibilidad (understanbility) Interpretabilidad (interpretability) Conciso (concise representation) Representación consistente (consistent representation)	Accesabilidad (accesability) Facilidad (ease of operation) Seguridad (security)

[159] CYKANA, P., PAUL, A., STERN, M., DoD guidelines on data quality management, Proceedings of the Conference on Information Quality, Cambridge, MA, 1996, pp. 154–171.

[160] MEYEN, D.M., WILLSHIRE, M.J., A data quality engineering framework, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 95–116.

Unitech[161]	Exactitud (accuracy) Consistencia (consistency) Confabilidad (reliability)	Completo (completeness) Temporal (timeliness)		
Diamond Technology Partners[162]	Exactitud (accuracy)			
IRI [163]	Exactitud (accuracy)	Temporal (timeliness)		Confiability (reliability)
HSBC[164]	Correcto (correctness)	Completo (completeness) Actualización (currency)	Consistencia (consistency)	Fácil obtener (obtainability) Flexibilidad (flexibility) Robustez (robustness)
AT&T and Redman[165]	Exactitud (accuracy) Consistencia (consistency)	Completo (completeness) Relevancia (relevance) Comprensividad	Claridad de definición (clarity of definición) Precisión de dominios	

[161] MANDKE, V.V., NAYAR, M.K., Information integrity–a structure for its definition, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 314–338.
[162] MATSUMURA, A, SHOURABOURA, N., Competing with Quality Information, Proceedings of the Conference on Information Quality, Cambridge, MA, 1996, pp. 72–86.
[163] KOVAC, R., LEE, Y.W., PIPINO, L.L., Total Data Quality Management: the case of IRI, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 63–79.
[164] GARDYN, E., A Data Quality Handbook For A Data Warehouse, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 267–290.
[165] REDMAN, T.C., Data Quality: Management and Technology, Bantam Books, New York, NY, 1992

		(comprehensiveness) Esencial (essentialness) Granuralidad de atributos (attribute granularity) Actualización (currency) Ciclo (time cycle)	(precision of domains) Naturalidad (naturalness) Homogeneidad (homogeneity) Identidad (identifiability) Mínima redundancia (minimun redundancy) Consistencia semántica (semantic consistency) Consistencia estructural (structural consistency) Representación apropiada (appropriate representation) Interpretabilidad (interpretability) Portabilidad (portabiity) Precisión del formato (format precisión) Flexibilidad del formato (format flexibility) Representación valores nulos	

			(represent null values) Almacenamiento eficiente (efficient use of storage) Consistencia en representación (representation consistency) Características del metadato (metadata characteristics)	

En cuanto a la vista de la industria, encabeza el listado lo propuesto por el Departamento de Defensa de los Estados Unidos (DoD) incluyendo su ciclo de vida para la información que incluye las fases de definir, medir, analizar y mejorar tal como lo recomienda el programa de gestión total de calidad del dato del MIT (Total Data Quality Management[166] – TDQM) que tiene como objetivo entregar productos de información de alta calidad a los consumidores de información[167].

La organización Mitre[168] ha realizado estudios sobre el impacto de las dimensiones en los usuarios de información encontrando que el 35% de los usuarios están interesados en la dimensión de usabilidad, 27% en calidad intrínseca, 24% en calidad de índole contextual, y 14% en calidad debida a la representación donde el 43% de los problemas surgen de la operación de los sistemas de información.

En el caso de Information Resources Inc. (IRI) han propuesto el modelo TRAQ (Temporalidad + Confiabilidad + Exactitud = Calidad) por sus siglas en inglés (Timeliness + Reliability + Accuracy = Quality) mientras que Unitech plantea el concepto denominado Integridad de la información a través de tres atributos intrínsecos (exactitud, consistencia y confiabilidad) y Diamond Technology partners sugiere evaluar la calidad de información a partir de su exactitud y accesibilidad para el caso de datawarehousing.

Finalmente, basado en su trabajo en AT&T, Redman provee una lista de atributos de calidad de la información desde una óptica representacional.

En el año 2007 los resultados del modelo AIMQ (en organizaciones de USA) de la investigación de Wang-Strong (1996) fueron contrastados por Ruževičius y

[166] http://web.mit.edu/tdqm/
[167] WANG. A product perspective on Total Data Quality Management. Comunications of the ACM. February 1998, Vol 41 No. 2.
[168] www.mitre.org

Gedminaitė (en organizaciones empresariales localizadas en Europa del norte) teniendo el siguiente resultado, donde se resaltan los aspectos disímiles entre los dos estudios (símbolo ≠):

Tabla 13. Comparación de estudios en calidad de la información

Wang y Strong (1996)		**Ruževičius y Gedminaitė (2007)**
Exactitud		Exactitud
Objetividad		Objetividad
Credibilidad		Credibilidad
Reputación	≠	Adaptabilidad a necesidades profesionales
Acceso		Acceso
Seguridad	≠	Actualización
Relevancia		Relevancia
Valor añadido		Valor añadido
Temporalidad		Temporalidad
Completo		Completo
Cantidad de datos	≠	Confidencialidad
Interpretabilidad	≠	Facilidad de manejo
Fácil de entender		Fácil de entender
Representación concisa		Representación concisa
Representación consistente		Representación consistente

Según lo anterior (investigación y estudios) se tiene el siguiente grupo de dimensiones:

Tabla 14. Inventario de dimensiones en calidad de la información

DIMENSION	**SUBDIMENSIONES**
Calidad intrínseca	Completitud (completeness) - **Confiabilidad** (reliability) - **Consistencia** (consistency) * **Credibilidad** (Believability) * **Exactitud** (accuracy) No ambiguo (unambiguous) No desviación (freedom from bias) * **Objetividad** (Objectivity) - **Precisión** (precision) Real (factual) * **Reputación** (reputation) Validez (validity)
Calidad contextual	- **Actualización** (currency) Actualización de la fuente (source currency) * **Cantidad** (quantity) - **Coherente** * **Completo** (completeness) Comprensividad (comprehensiveness) Confiable (reliable) Contenido (content) - **Correcto** (correctness) Esencial (essentialness) Granuralidad (attribute granularity) Importancia (importance) Informativo (informativeness) Profundidad (level of detail) * **Relevancia** (relevance) Suficiencia (sufficiency) * **Temporalidad** (timeliness) Uso (usage) Utilidad (usefulness) * **Valor añadido** (value added)

Calidad de acceso	* **Accesabilidad** (accesability) Casos de uso (case of use) + **Confidencialidad** Conveniencia del acceso (convenience of access) Cuantitativo (quantitativeness) - **Disponibilidad** del dato Disponibilidad del sistema (system availability) Disponibilidad transacción (transaction availability) Facilidad (ease of operation) Localización (locatability) - **Oportuno** (timely) Privilegios (privileges) * **Seguridad** (security) Usable (usableness)
Calidad representacion	Apariencia (appearance) Características del metadato (metadata characteristics) - **Claridad** (clarity)[169] Claridad de definición (clarity of definición) Comparable (comparability) Compatible (compatibility) * **Conciso** (concise representation) * **Consistente** (concistent representation) Consistencia estructural (structural consistency) Consistencia en representación (representation consistency) Consistencia semántica (semantic consistency) Control de versiones (version control) Eficiencia de almacenamiento (efficient use of storage) Formato (format) Homogeneidad (homogeneity) Identidad (identifiability) * **Inteligibilidad** (understanbility) * **Interpretabilidad** (interpretability) Flexibilidad del formato (format flexibility)

[169] Estatuto general de contratación colombiano - Ley 80 de 1993. Art 25 numeral 3.

	Legible (readable) Naturalidad (naturalness) No confuso (lack of confusion) No volatilidad (non volatility) Organización (arrangement) Origen (origin) Portabilidad (portabiity) Precisión de dominios (precision of domains) Precisión del formato (format precisión) Presentación (presentation) Razonable (reasonable) Redundancia mínima (minimun redundancy) Representación apropiada (appropriate representation) Representación consistente (consistent representation) Representación valores nulos (represent null values) Semántica (semantics) Significante (meaningfulness) Sinónimos (aliases) Sintaxis (syntax) Único (uniqueness)

En el recuadro se han resaltado con asterisco los resultados del estudio de Wang y Strong, con el signo suma la conclusión de Ruževičius y Gedminaitė. Además, y con guión aquellas dimensiones necesarias y exigidas en el estado colombiano:

- En cuanto a la contratación estatal[170]: el numeral 3 del artículo 25 de la ley 80 de 1993 (estatuto general de contratación reformado por la Ley 1150 de 2007) establece que, tanto las entidades como los servidores públicos, deben responder "*cuando hubieren abierto licitaciones sin haber elaborado*

[170] BLANCO RESTREPO, Jose Vicente. La responsabilidad del Estado por la calidad de la información suministrada en las licitaciones públicas. Febrero de 2011. Internet: http://contratacionestatal.blogspot.com/2011/02/la-responsabilidad-del-estado-por-la.html

previamente los correspondientes pliegos de condiciones, diseños, estudios, planos y evaluaciones que fueren necesarios, o cuando los pliegos de condiciones hayan sido elaborados en forma incompleta, ambigua o confusa que conduzcan a interpretaciones o decisiones de carácter subjetivo por parte de aquellos". Se incluyen entonces los antónimos de incompleto (completo), ambiguo (exacto y preciso) y confuso (claro)

- Sobre información financiera[171], la circular 052 de 2007, dentro del numeral 2 "Definiciones y criterios de seguridad y calidad", tiene como criterios de calidad:
  a) Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
  b) Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos (eficiencia).
  c) Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones. Por lo anterior, se adicionan los criterios de oportunidad (dentro de la dimensión de acceso),

- En cuanto a la seguridad de la información (de tipo financiera), la circular 052 de 2007, dentro del numeral 2 "Definiciones y criterios de seguridad y calidad", se plantean como criterios de seguridad de la información:
  a) Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.
  b) Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción (ciclo de vida del documento).
  c) Disponibilidad: La información debe estar en el momento y el formato que se requiera ahora y en el futuro, al igual que recursos necesarios para su uso.
- En cuanto a la seguridad de la información (de tipo financiera), la circular 052 de 2007, dentro del numeral 2 "Definiciones y criterios de seguridad y calidad",

[171] Superintendencia financiera de Colombia – Circular externa 052 de 2007. Octubre de 2007. Internet: http://www.netsecuritysuite.com/pdf/Norma-052.pdf

se plantean como criterios de calidad de la información:

6.2. MECANISMOS DE CONTROL DE CALIDAD DE LA INFORMACIÓN

De lo anterior se obtiene el esquema definitivo de subdimensiones al resaltar las necesarias por el contexto normativo colombiano, especialmente en el ámbito público, descartar las no seleccionadas por los estudios anteriores y la selección aquí realizada, consolidar subdimensiones según sus definiciones y conceptos y revisar su pertinencia en cada dimensión, para lograr la siguiente clasificación[172]:

Tabla 15. Criterios de análisis de calidad de la información

DIMENSION	SUBDIMENSION	DEFINICION
Calidad intrínseca	**Confiabilidad** (Reliability) <cuantitativa>	Consistencia de un conjunto de datos o mecanismo de medición[173]. La confiabilidad se puede determinar: a. Coeficiente de correlación de producto momento de Pearson[174] (r) donde la calificación e interpretación del coeficiente está unida al contexto y propósito de los datos[175] b. Significación de la correlación mediante la Ley de Student[176] para determinar que la correlación no es producto del azar[177] [178]

[172] ANGARITA CASTELLANOS, Juan Carlos. Information Quality Assessment for Compliance and Governance. UIS. 5 International Conference on theory & practice of electronic governance. Tallin, Estonia. ACM Press 2011

[173] MEEKER, William Q., ESCOBAR, Luis A.. Statistical Methods for Reliability Data. Hoboken, New Jersey: Wiley, 1998. ISBN 0471143286

[174] RODGERS, J. L., NICEWANDER, W. A.. Thirteen ways to look at the correlation coefficient. The American Statistician, 42(1):59–66, February 1988.

[175] COHEN, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.)

[176] http://personal.us.es/vararey/adatos2/correlacion.pdf

[177] RAHMAN, N.A, A Course in Theoretical Statistics; Charles Griffin and Company, 1968

[178] FERNÁNDEZ, Pita, PÉRTEGA, S. Relación entre variables cuantitativas. Unidad de

	Exactitud (accuracy) (trueness) <cuantitativa>	Proximidad de concordancia entre el resultado de una medición (o promedio) y el valor real de lo medido[179] [180] [181] como garantía de integridad de los datos[182]. El valor real[183] es un valor consistente con una variable particular y es el valor que sería obtenido de una medición perfecta. En aquellos contextos donde no es posible obtener una medición perfecta se usa un valor por convención (mejor valor estimado). La exactitud se expresa mediante la magnitud media de error relativo, incluye el error aleatorio y el sistemático[184], y es inversamente proporcional al sesgo de los resultados[185].
	Precisión (precision) <cuantitativa>	Cercanía de resultados entre mediciones[186] hechas a objetos (o sujetos) presumiblemente idénticos bajo condiciones técnicas presumiblemente iguales que deben entregar los mismos resultados[187]. Su medición depende de la distribución del error aleatorio sin el valor real o esperado, se expresa en términos de imprecisión y se calcula como la desviación estándar de los resultados, donde a mayor desviación estándar frente a la media aritmética es menor la precisión.

Epidemiología Clínica y Bioestadística. Complexo Hospitalario Universitario de Coruña (España). 1997; http://www.fisterra.com/mbe/investiga/var_cuantitativas/var_cuantitativas.asp

[179] ISO 3534-1:1993, Numeral 3.11

[180] ISO/IEC TR 14143-3:2003 Information technology -- Software measurement

[181] WALTER, W. Hauck, KOCH, William, ABERNETHY, Darrell, USP. Making Sense of Trueness, Precision, Accuracy, and Uncertainty. Pharmacopeial Forum. Vol. 34(3) [May 2008], pp 838-842

[182] ISO/IEC 27001:2005, Numeral 3.8

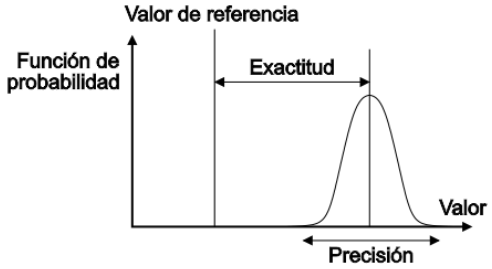
[183] ISO Vocabulary of basic and general terms in metrology (1993)

[184] ISO 5725-1:1994, Numeral 3.6. Accuracy (trueness and precission) of measurement methods and results - part 1 - General principles and definitions. 1994

[185] ROTHMAN, K.J. et al. (2008) Modern epidemiology. Lippincott Williams & Wilkins pp.134-137.

[186] ISO 5725-1:1994, Numeral 0.2 y 3.12. Accuracy (trueness and precission) of measurement methods and results - part 1 - General principles and definitions. 1994

[187] ISO 2. 21748 Guidance for the Use of Repeatability, Reproducibility, and Trueness Estimates in Measurement Uncertainty Estimation. Geneva, Switzerland: ISO; 2004.

		Figura 21. Precisión vs Exactitud 
	Credibilidad (believability) <cualitativa>	Calidad de ser creíble o de confianza[188] a través de la confianza en el dato (trustworthiness) y la experticia (expertise) [189] de la fuente. La confianza en el dato involucra la no desviación y objetividad del dato[190]; mientras que la experticia incluye el grado de conocimiento, experiencia y competencia en el tema de estudio, conformando cierta autoridad temática, entendida ésta como la medida del grado de confianza de la fuente[191] por su grado de legitimidad, calidad y competencia[192] La medición de la credibilidad[193] [194] se puede por: - **Credibilidad experimental**, evaluativa, ligada al dato, donde la ocurrencia de error (de valor o formato), omisión o desviación no explicadas, reduce la credibilidad del dato.

[188] PACmeter - Popularity, Authority, Credibility Online: How To Measure Them? http://www.masternewmedia.org/2004/08/11/pacmeter_popularity_authority_credibility.htm
[189] SELF, C. Credibility. An integrated approach to communication theory and research, Salves Eds, NJ, 1996
[190] TSENG, Shawn & FOGG, B.J.. Credibility and Computing Technology. Communications of the ACM, vol. 42, issue 5 (May 1999), pp. 39-44.
[191] Montgomery. http://www.montgomerycollege.edu/library/libtp/instructions/findingarticles/glossary.htm
[192] Real Academia de la Lengua. www.rae.es
[193] TSENG, Shawn & FOGG, B.J. The Elements of Computer Credibility. Proceedings of ACM CHI 99 Conference on Human Factors in Computing Systems, v.1, pp. 80-87. New York: ACM Press.
[194] RIEH, S. Y. (2002) Judgment of information quality and cognitive authority in the web. Journal of the American Society for Information Science and Technology, 53, 145-161.

		- **Credibilidad por reputación**, predictiva, de la mano con la experticia o nivel de autoridad de la fuente, surge a partir de la participación de personas conocedoras del tema según sus competencias y experiencia, así como la experiencia, tradición e institucionalidad propia de la organización que emite la información. Para cuantificar lo anterior, es factible por indicadores (elementos ponderados) valorando la credibilidad experimental y la reputación mediante criterios específicos según el contexto y el tipo de información bajo análisis[195].
	Validez (validity) <mixto>	Evaluación sobre la medición que informa sobre si sus resultados son significativos y útiles, y el proceso aplicado es adecuado[196] [197] [198] donde el dato obtenido tiene carácter de firme, subsistente y que vale o debe valer legalmente.[199] - **Validez del contenido o lógica (cualitativa)**, Determina si los datos son reflejo de lo que se intenta medir, si cubre el dominio de interés, si se basa en un tamaño de muestra adecuado y si verifica la adecuada implementación del método y condiciones de medición.

[195] HILLIGOSS, B. & RIEH, S. Y.. Developing a unifying framework of credibility assessment: Concept, heuristics, and interaction in context. 44(4), 2008. 1467-1484.
[196] HURST, Cliff. Measurement, Reliability, and Validity: Part Four in the continuing series, Getting Quality Right. July/August 2008. http://www.connectionsmagazine.com/articles/8/061.html
[197] Research methods knowledge base. http://www.socialresearchmethods.net/kb/measval.php
[198] PACKER, Martin. Experimental and Statistical Research Methods. Duquesne University. 2004. http://www.mathcs.duq.edu/~packer/Courses/Psy624/test.html
[199] Real Academia Española. http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=accesibilidad

		- **Validez de criterio (cuantitativa)**, Evalúa si el criterio usado permite correlacionar la medición con otras mediciones [200] [201]. Validez predictiva: Mide la capacidad predictiva sobre lo que en teoría debe ser capaz de predecir. Validez concurrente: Establece la capacidad de distinguir grupos entre los datos que de forma teórica debería ser capaz de distinguir. Validez convergente:[202] Examina la similitud de la implementación del método frente a otras mediciones que usan el mismo método. Validez de discriminación: Explora el grado de diferencia de implementación frente a otras mediciones que buscan obtener datos similares. La medición de la validez de criterio se da por el coeficiente de correlación (Pearson) aplicado sobre los diversos conjuntos de datos y revisar el comportamiento planteado. - **Validez del proceso (cuantitativa)**, dada por los mecanismos técnicos (documentados) para la obtención, proceso y publicación de datos garantizando repetitividad[203] y reproducibilidad. La evidencia procedimental (en su definición y registro) concede validez al dato obtenido.[204]

[200] Research methods knowledge base. The Multitrait-Multimethod Matrix. http://www.socialresearchmethods.net/kb/mtmmmat.php
[201] CRONBACH, L., MEEHL, P.. Construct validity in psychological tests, Psychological Bulletin, 1955. 52, 4, 281-302
[202] Research methods knowledge base. Convergent & Discriminant Validity. http://www.socialresearchmethods.net/kb/convdisc.php
[203] Instituto Nacional de Tecnología Industrial. Argentina.
[204] SENAR, J.C.. La Medición de la Repetibilidad y el Error de Medida. Museu de Zoologia, Ap.

		Repetitividad (r)[205] Precisión en condiciones de repetitividad, o sea mediciones realizadas con el mismo método sobre la misma característica por el mismo operador usando los mismos instrumentos Reproducibilidad (R) Precisión en condiciones de reproducibilidad, es decir mediciones hechas con igual método sobre la misma característica por diferentes operadores u organizaciones y usando diferentes instrumentos (variación de evaluador) [206] Ambos usan coeficiente de variación media[207] [208]
	Autenticidad (authenticity) <cualitativa>	Propiedad que asegura que la identidad de un sujeto o recurso es aquel que dice ser,[209] y aplica a usuarios, sistemas, procesos e información.
Calidad contextual	**Actualización** (currency) (timeliness) <cualitativa>	Medida de que tan actualizada (o a la fecha) está una medición[210]. No implica modificar datos. - **Continuidad** (línea de tiempo). Permite evaluar la actualización de datos en una periodicidad especificada por variable, donde el indicador reporta el número de períodos con datos. - **Estructural**. Establece que tan frecuentemente cambia la estructura de datos.

Correus Barcelona. 1999. http://www.bcn.es/museuciencies_fitxers/imatges/FitxerContingut1201.pdf

[205] ISO 5725-1:1994, Numeral 3.13 y 3.14. Accuracy (trueness and precission) of measurement methods and results - part 1 - General principles and definitions. 1994

[206] ISO 5725-1:1994, Numeral 3.17 y 3.18. Accuracy (trueness and precission) of measurement methods and results - part 1 - General principles and definitions. 1994

[207] Universidad de Málaga - Fundación Universitaria Andaluza Inca Garcilaso. Grupo de investigación eumednet. http://www.eumed.net/libros/2007a/239/5d.htm

[208] O'CONNOR, Daniel P.. Measurement in Health & Physical Education – Validity. University of Houston.

[209] ISO/IEC 13335-1:2004

[210] Montgomery college.
http://grants.hhp.coe.uh.edu/doconnor/PEP6305/Topic%20012%20Validity.htm
http://www.montgomerycollege.edu/library/libtp/instructions/findingarticles/glossary.htm

	Completo (completeness) <cuantitativa>	Capacidad de presentar datos para cada medida relevante en cada período de tiempo[211] [212] [213] [214] como garantía de integridad de los datos. - **Completitud de datos**. Para una medición periódica, compara la cantidad de valores no nulos (*v*) frente al total de valores (*n*) del mismo conjunto en un determinado período de tiempo. - **Completitud del sistema**. Para un sistema con un flujo constante de datos, la completitud está dada por la cantidad de valores no nulos (*v*) frente al número de sensores (n) y la duración (d) de la medición. - **Completitud de consulta**. Para un sistema con un flujo constante de datos, la completitud está dada por los datos disponibles (completitud del sistema) amplificado por la rata de consulta del sistema frente a la rata de consulta solicitada. La completitud debe incluir información[215] de autoridad, metadatos y notas a los datos[216]

[211] BISWAS, Jit, NAUMANN, Felix, QIU, Qiang. Assessing the Completeness of Sensor Data. Institute for Infocomm Research (I2R), Singapore, Humboldt-Universit¨at zu Berlin, Germany.
[212] DUTTA, M. The impact of internet information completeness: The moderating role of Web use motivation. University of Minnesota. 2001
[213] DUTTA-BERGMAN, M. health communication on the web: The role of web use motivation and informaton completeness Communication monographs, 70, 264-274. 2003
[214] DUTTA-BERGMAN. The impact of completeness and web use motivation on the credibility of e-health information. International Communication Association. 2004. pp 253-269
[215] TOULMIN, S. The uses of argument. Cambridge, UK. Cambridge University Press. 1958
[216] KORPAN, C. A., BISANZ, G. L., BISANZ, J. y HENDERSON, J. Assessing literacy in science: Evaluation of scientific news briefs. Science education, 81, 515-532. 1997

	Relevancia (relevance) <cuantitativa>	Un documento recuperado se considera relevante cuando su contenido posee alguna significación o importancia con motivo de la pregunta realizada por el usuario, su necesidad de información[217] [218] - **Precisión** (relevancia).Fracción de documentos recuperados que son relevantes a la necesidad de los usuarios[219] [220] - **Sensibilidad**. Fracción de documentos que son recuperados y son relevantes a la consulta y que son exitosamente recuperados. - **Especificidad**. Proporción de documentos no relevantes que son recuperados.
Calidad de acceso	**Accesibilidad** (accessibility) <cuantitativa>	Grado de acceso exitoso a uno o más recursos[221] de información[222] [223]
	Confidencialidad (confidenciality)	Corresponde al deber de mantener el secreto y por ende respetar la privacidad de las personas[224] [225] al

[217] COOPER, W.S. 'On selecting a Measure of Retrieval Effectiveness'. Journal of the American Society for Information Science, v. 24, March-April 1973. p.87-92

[218] FRANTS , V.I. et al. Automated information retrieval : theory and methods. San Diego [etc.] : Academic Press, cop.1997. XIV, 365 p.

[219] TURPIN, Andrew; SCHOLER, Falk. "User performance versus precision measures for simple search tasks". Proceedings of the 29th Annual international ACM SIGIR Conference on Research and Development in information Retrieval (Seattle, Washington, USA, August 06-11, 2006) (New York, NY: ACM): 11–18

[220] MAKHOUL, John; KUBALA, Francis; SCHWARTZ, Richard; WEISCHEDEL, Ralph: Performance measures for information extraction. In: Proceedings of DARPA Broadcast News Workshop, Herndon, VA, February 1999

[221] ISO/IEC 2382-1:1993 Information technology--Vocabulary--Part 1: Fundamental terms.

[222] ISO/IEC 18019:2004 Software and system engineering - Guidelines for the design and preparation of user documentation for application software

[223] ISO/IEC 25062:2006 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability test reports. 4.10

[224] MANN, J. M.; GOUSKINS, S.; GRODIN, M. A.; ANNAS, G. J., eds. (1999). Health and Human Rights: A Reader. New York and London: Routledge.

[225] United Nations (UN) Universal Declaration of Human Rights (1948) Art 12

	<cualitativa>	asegurar que la información solo sea accesible a aquellas personas, o sistemas, autorizadas para su acceso[226] [227] [228] y que existan las restricciones y autorizaciones debidas para el control de acceso y divulgación incluyendo los mecanismos para la protección de la privacidad e información personal [229] [230] [231] [232] [233] de forma que la información no sea disponible o publicado a individuos, entidades o procesos no autorizados[234] La medición de la confidencialidad exige adoptar e implementar modelos técnicos de gestión sobre el riesgo informático o de seguridad de la información donde se planteen mediciones de tipo predictivo, preventivo y correctivo.
	Disponibilidad (availability) <cuantitativa>	La disponibilidad incluye asegurar que los datos o servicios de comunicación e información estén listos para usarse cuando sea requerido[235] [236] en general bajo demanda por entidades autorizadas[237] - **Disponibilidad de contenido** (c). Cantidad de información entregada al usuario[238].

[226] ISO/IEC 17799, Jan 4, 2009
[227] ISO/IEC 7498-2
[228] ISO/IEC 13335-1:2004 Numeral 2.6
[229] SP 800-53
[230] FIPS 200
[231] FIPS 199
[232] 44 U.S.C., Sec. 3542
[233] FIPS 140-2
[234] ISO/IEC 27001:2005
[235] University of Oulo. Glossary of Vulnerability Testing Terminology. https://www.ee.oulu.fi/research/ouspg/Glossary
[236] ISO/IEC 7498-2
[237] ISO/IEC 27001:2005, Numeral 3.2
[238] MATULEVIČIUS, Raimundas, KAMSEU, Flora, HABRA, Naji. Measuring Open Source Documentation Availability. PReCISE, Computer Science Faculty, University of Namur, Belgium. Pp8, 2010

		- **Disponibilidad de información** (d). (nivel de detalle). Mide la cantidad de nivel de detalle 0 No hay unidades de información 1 Nivel de detalle bajo (en resumen) 2 Nivel de detalle promedio 3 Alto nivel de detalle Donde la disponibilidad está dada por la suma de contenido ponderada por el nivel de detalle frente al número de unidades de información: - **Disponibilidad de sistema** (Ds). Tiempo en el cual la infraestructura de TI está activa (Ta) frente al tiempo total[239].
	Oportuno (timely) <cuantitativa>	Publicación de información dentro del marco de tiempo pactado con los usuarios de la información de forma que se asegura su pronta disponibilidad, de forma tácita o explícita, incluyendo la posible vigencia y expiración del dato en un tiempo establecido[240] Su medición puede operar en dos marcos de tiempo: - **Publicación oportuna**. Agilidad de publicación de datos (t_d) frente al tiempo pactado (t_a). - **Publicación de información vigente**. Muestra si el dato es publicado dentro de su ventana de tiempo en la cual es aún vigente (t_v). - **Aprovechamiento**. Ilustra la relevancia del dato en la ventana de tiempo de su vigencia.

[239] Federal Standard 1037C (MIL-STD-188) http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm
[240] UNDERWOOD, George M., MAGLIO, Paul P., BARRETT, Rob. User-centered push for timely information delivery. IBM Almaden Research Center. http://www.almaden.ibm.com/cs/wbi/papers/www7/user-centered-push.html

	Seguridad (security) <cualitativa>	Protección de la información de forma que personas o sistemas no autorizados no puedan leerla o modificarla, y que no se le niegue acceso a las personas o sistemas autorizadas[241]. La seguridad es un concepto derivado que exige asegurar la confidencialidad, la integridad de los datos apoyada en la completitud, exactitud y precisión así como su disponibilidad, la autenticidad y confiabilidad de forma integral.
Calidad presentación	**Coherente** (Coherent) <cualitativa>	Propiedad de un conjunto de datos que mejora la confianza en la información bajo el concepto Cæterīs pāribus "permanece el resto constante" [242] [243] [244] de forma que se puede esperar un conjunto equivalente de proposiciones en el conjunto de datos y sus definiciones, mientras se mantiene la conexión, relación y unión de sus elementos entre sí de forma lógica y estructurada[245]. La coherencia suele darse por la presencia de una estructura macro del dato (metadato) que define, relaciona y organiza las variables y por ende los datos, y el nivel consistencia de la información que garantiza la uniformidad del dato. Por lo anterior, puede plantearse que la existencia del metadato aumentará el valor de coherencia del dato.

[241] ISO/IEC JTC1/SC7:12207
[242] BOVENS, Luc, HATMANN, Stephan. Solving the riddle of coherence. Mind, Vol 112-448. Bovens and Hartmann. Octubre 2003
[243] Information Coherence Authority for Defence (ICAD) – Ministry of Defence – United Kingdom. http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/ICAD/
[244] Stephan Hartmann and Luc Bovens. A Probabilistic Theory of the Coherence of an Information Set. http://www.gap-im-netz.de/gap4Konf/Proceedings4/pdf/6%20Ek05%20Hartmann.pdf
[245] Real Academia Española. http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=coherencia

	Consistente (concistent) (comparability) <cualitativa>	Grado de uniformidad, estandarización y libertad de contradicción entre los documentos o partes de un sistema o componente[246] [247]. La consistencia de la información[248] se da a través de estructuras de datos uniformes, documentadas y acompañadas de metadatos, permite funciones de: - Comparación entre varios conjuntos de datos. - Armonización entre conjuntos de datos con estructuras de datos disímiles, de diferente nivel o profundidad de detalle. - Complementación al incrementar la completitud de los datos entre varios grupos de datos. - Claridad al estar plenamente documentado el metadato se puede conocer el dominio de datos representado, su significancia y operadores que le son aplicables. - Homogeneidad al estandarizar la estructura de datos y por ende los mecanismos de acceso al mismo recurso de información.
	Inteligibilidad (understanbility) <cualitativa>	Un documento es entendible si está organizado de forma que los usuarios que tengan interés en su información pueden fácilmente acceder y entender sus datos y relaciones lógicas existentes. Para medirla, se puede diseñar un instrumento donde se evalúe la estructura y relaciones lógicas entre sus partes según el tipo de documento, los datos contenidos y los usuarios interesados[249].

[246] IEEE-STD-610
[247] SEI:SW-CMM
[248] MOTTOLA, R.M., SYTSMA, Sid. The Basics of Experimental Design - A Quick and Non-Technical Guide. 2009
[249] MATULEVIČIUS, Raimundas, KAMSEU, Flora, HABRA, Naji. Measuring Open Source Documentation Availability. PReCISE, Computer Science Faculty, University of Namur, Belgium.

Notas: En el caso de la confiabilidad ésta se encuentra asociada y hace referencia a la fuente de la cual proviene el dato, por lo cual se elimina consolidándola como fuente.

6.3. MEDICION DE LA CALIDAD DE LA INFORMACION

6.3.1. Estandarización de la medición. El concepto de medición requiere tener patrones tanto para su realización como para su definición, lo cual se logra a través de un vocabulario común[250] entendido como un diccionario terminológico que contiene designaciones y definiciones para uno o más campos de aplicación específica.

En 1993, la organización internacional para la normalización (ISO) expidió la primera versión del vocabulario internacional de términos básicos y generales en metrología (VIM) liderado por la ISO[251] de la mano con la norma ISO 5725-1:1994[252] sobre la exactitud (veracidad y precisión) de los métodos de medición y los resultados obtenidos.

En el año 1997 se crea el Joint Committee for Guides in Metrology Bureau (JCGM)[253] o Comité commun pour les guides en métrologie, integrado por las entidades líderes de medición a nivel internacional: International des Poids et Mesures (BIPM), International Electrotechnical Commission (IEC), International Federation of Clinical Chemistry and Laboratory Medicine (IFCC), International Laboratory Accreditation Cooperation (ILAC[254]), International Organization for

---

Pp7, 2010
[250] ISO 1087-1: 2000 numeral 3.7.2
[251] ISO. International Vocabulary of Basic and General Terms in Metrology, 1993.
[252] ISO 5725-1:1994 Accuracy (trueness and precision) of measurement methods and results
[253] http://www.bipm.org/utils/en/pdf/JCGM_charter.pdf
[254] http://www.ilac.org/library_documents.html

Standardization (ISO[255]), International Union for Pure and Applied Chemistry (IUPAC), International Union for Pure and Applied Physics (IUPAP), International Organization of Legal Metrology (IOLM), el cual tiene como responsabilidad establecer las normas base para el desarrollo de la actividad de metrología incluyendo la guía para el control de incertidumbre y error[256] [257].

En el año 2008, el JCGM produce el vocabulario internacional de metrología (JCGM 200:2008[258] 3 edición) en sus términos básicos, generales y relacionados, equivalente a la guía ISO 99-12:2007[259] publicada por la ISO, el cual es tomado como base de referencia, junto con la norma ISO 15939:2007[260], como vocabulario común de esta investigación.

6.3.2. Estándares y/o marcos técnicos disponibles.

6.3.2.1. ISO/IEC 15939

a. Vocabulario. La norma técnica ISO/IEC 15939[261] (en su actual versión 2007) establece un modelo de medición de información donde resalta el siguiente conjunto de definiciones:

[255] http://www.iso.ch
[256] Evaluation of measurement data – Guide to the expression of uncertainty in measurement [JCGM 100:2008]; Evaluation of measurement data – An introduction to the "Guide to the expression of uncertainty in measurement" [JCGM 104:2009], Evaluation of measurement data – Supplement 1 to the "Guide to the expression of uncertainty in measurement" – Propagation of distributions using a Monte Carlo method [JCGM 101:2008]
[257] http://www.bipm.org/en/publications/guides/gum.html
[258] JCGM 200:2008. International vocabulary of metrology — Basic and general concepts and associated terms (VIM)
[259] ISO/IEC Guide 99-12:2007, International Vocabulary of Metrology — Basic and General Concepts and Associated Terms
[260] ISO/IEC 15939:2007, Systems and software engineering - Measurement process.
[261] ISO/IEC 15939

Atributo (Numeral 2.2): Propiedad o característica de una entidad que puede distinguirse de forma cualitativa y/o cuantitativa usando medios humanos o automatizados.

Entidad (Numeral 2.9): Objeto que es caracterizado por la medida de sus atributos.

Medición (Numeral 2.17): Desarrollo de un conjunto de operaciones que tienen como objeto determinar un valor (cuantitativo) o representación categórica (cualitativo) de uno o varios atributos, teniendo un propósito establecido.

Indicador (Numeral 2.10): medida que proporciona una estimación o evaluación de atributos a partir de un modelo, con respecto a ciertas necesidades de información.

Almacén de datos (Numeral 2.6): Colección organizada y persistente de datos que permite su recuperación.

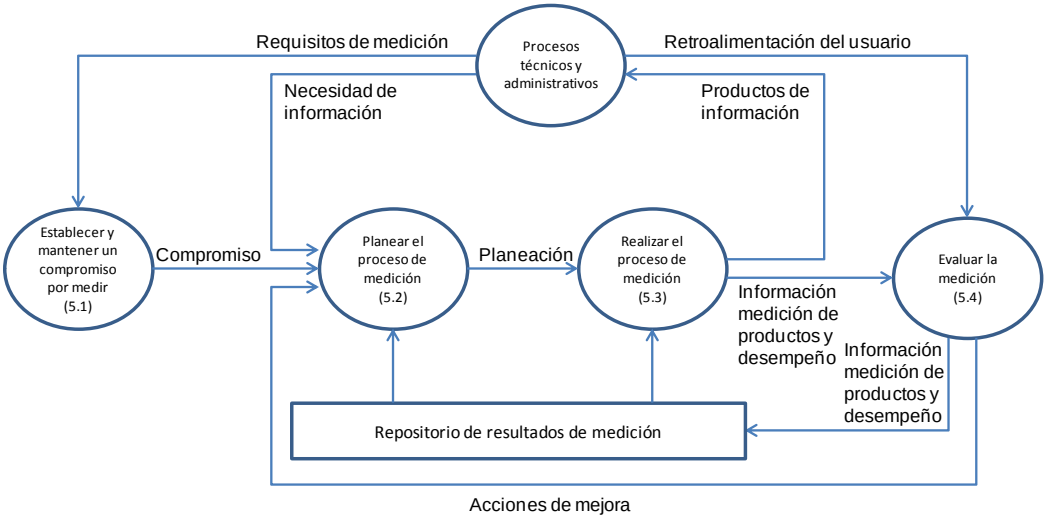
Proceso (Numeral 2.32 + ISO 9000:2008): Conjunto de actividades interrelacionadas o que interactúan las cuales transforman entradas en salidas.

Partes interesadas (stakeholder) (Numeral 2.37): Individuo u organización que teniendo derechos, comparte, reclama o manifiesta interés en un sistema o está en posesión de características que satisface sus expectativas o necesidades. En el contexto de gestión de la información, incluye a todos los individuos u organizaciones que patrocinan las mediciones, proveen datos, son usuarios de las mediciones, o de alguna otra manera participa en el proceso de medición.

Usuario (Numeral 2.41): Individuo o grupo beneficiario de un sistema en su utilización.

b. Proceso.

Figura 22. Proceso de medición según la norma ISO 15939



Fuente: ISO 15939

El proceso de medición planteado por la norma ISO 15939 está igualmente inscrito en el ciclo PHVA, donde la planeación está planteada en el numeral 5.2, el hacer en el numeral 5.3, y la verificación y actuación en el numeral 5.4. Este ciclo igualmente emana de la alta dirección, según el numeral 5.1, con el compromiso de la organización en la medición. Sin embargo, es común observar que se realicen mediciones sin que medie norma técnica en la realización de tal proceso.

7. EL PROBLEMA DEL CUMPLIMIENTO

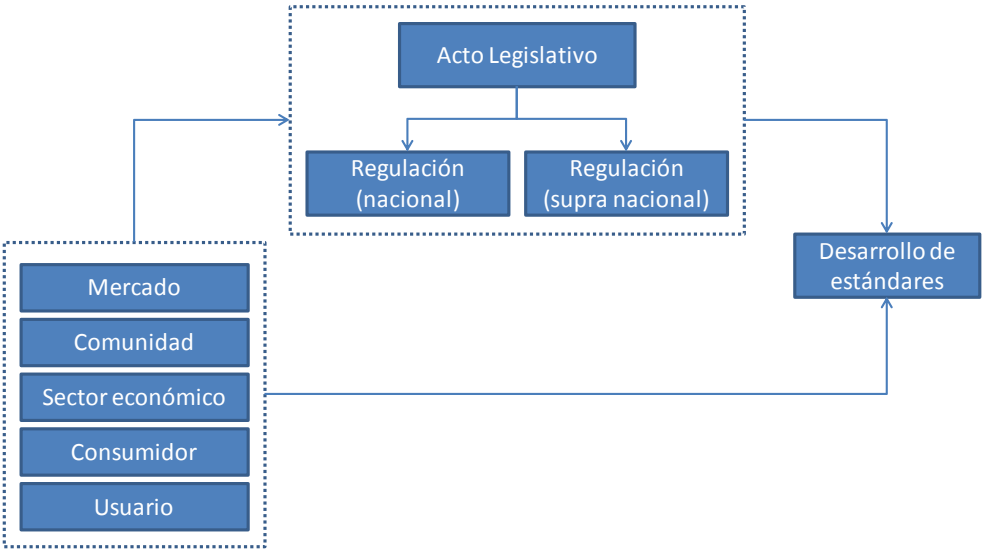
El proceso de estandarización sucede en varios escenarios. Por una parte, en el ejercicio de creación de actos legislativos y/o regulaciones, puede suceder que en el cuerpo de la norma estén insertas algunas cláusulas de estandarización en el campo de aplicación de la norma. Por otro lado, los estándares, o familias de normas técnicas, pueden ser emitidos de manera independiente a la norma jurídica, bien sea para complementarla o reglamentarla, o solo dentro del mimo espacio sin que exista relación explícita entre las normas jurídicas y las técnicas.

En la práctica, existen diversas autoridades produciendo y de igual manera consumiendo o usando reglas, o solicitándolas de no existir. Dichas autoridades producen normas al nivel técnico (para autoridades de normalización técnica) o público (de normalización jurídico) del orden legislativo, ejecutivo, judicial e incluso de control, bajo diferentes enfoques, representando una obligación de índole legal e incluso sanciones.

De igual manera, las normas legales y regulaciones, en el caso de acuerdos comunitarios, y las normas técnicas, pueden tener un alcance nacional o internacional.

Esta situación crea un contexto donde concurren y compiten diversas autoridades con guías, normas y directrices que pueden solaparse o general conflictos en el mismo tema.

Figura 23. Marco general de normas técnicas

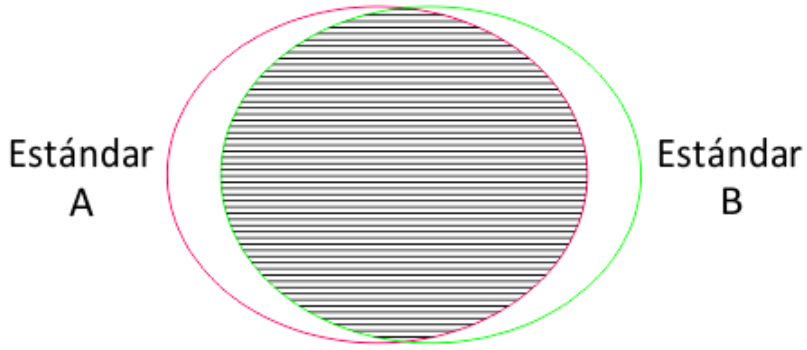


7.1. INTERSECCION ENTRE ESTÁNDARES

Es altamente posible y común que un objeto, sujeto o método específico, sea considerado por varias y diversas autoridades con sus respectivos y diferentes enfoques, lo cual tiene como resultado un grupo de estándares en conflicto al considerar que los requerimientos, especificaciones, metodologías y exigencias o recomendaciones, no concuerdan total o parcialmente entre ellos.

7.1.1. Estándar equivalente a nivel total. Este caso ideal plantea el caso en el cual dos o más estándares normalizan de manera concurrente el mismo aspecto a través de un conjunto similar de cláusulas y que a su vez poseen especificaciones que equivalen en su totalidad o en la mayor parte de la norma.

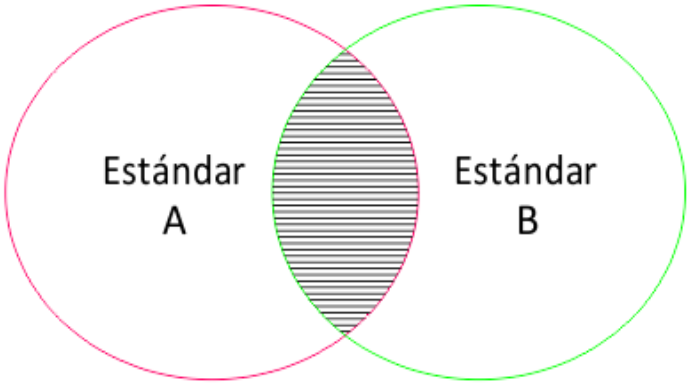
Figura 24. Intersección entre estándares similares



7.1.2. Estándar equivalente parcialmente. Este escenario, más probable que el anterior, plantea el caso en el cual dos o más estándares, aplicados al mismo objeto, sujeto o área de conocimiento, exponen diferencias especialmente en cuanto al alcance y por ende el conjunto de cláusulas que tratan el mismo tema, algunas de ellas concurrentes y otras con un enfoque a aspectos diferentes.

Usualmente las discrepancias expresadas se presentan en el conjunto de cláusulas, las especificaciones, rangos de validez, controles e incluso los métodos de implementación o de medición. Esta clase de conflicto surge debido a los diferentes enfoques y contexto legal y socio económico que poseen las autoridades que le producen. Esta situación es altamente conflictiva en auditorías.

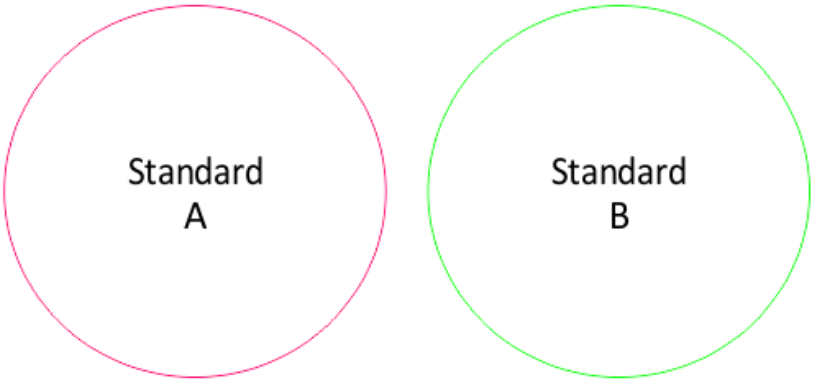
Figura 25. Intersección entre estándares parcialmente similares



7.1.3. Estándares no equivalentes. Este caso muestra como dos estándares aplicados al mismo objeto, sujeto o área de conocimiento, poseen cláusulas disímiles que manejan aspectos diferentes para obtener normas independientes entre sí, con una posible ventaja relativa a la posible integración entre ellas al no tener cláusulas en conflicto.

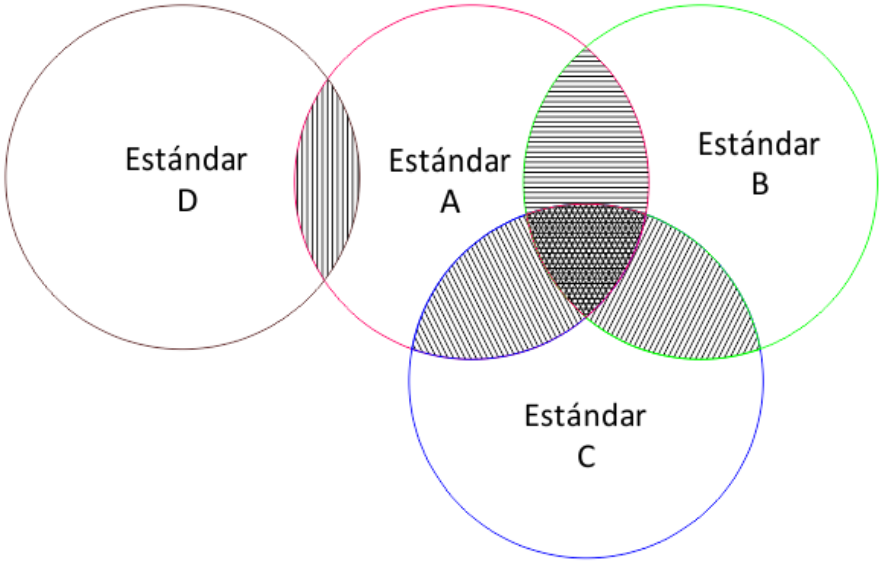
La diferencia entre normas pude conllevar a diferentes especificaciones, controles o métodos de uso, aplicación o medición. Esta situación surge de diferentes enfoques o puntos de vista o necesidades del mercado, consumidores o usuario.

Figura 26. Estándares no equivalentes



7.1.4. Escenario de múltiples estándares. En el mundo real, el escenario más probable y común, es que un objeto, sujeto, método, tecnología o en términos generales un área de conocimiento, posea varios estándares concurrentes, con diferentes enfoques, cláusulas y elementos así como diversos grados de interacción entre ellos.

Figura 27. Caso real de intersección entre estándares



En el caso mostrado, los estándares A y D tienen algunos elementos en común mientras que el estándar D no tiene cláusulas en común con los estándares B y C.

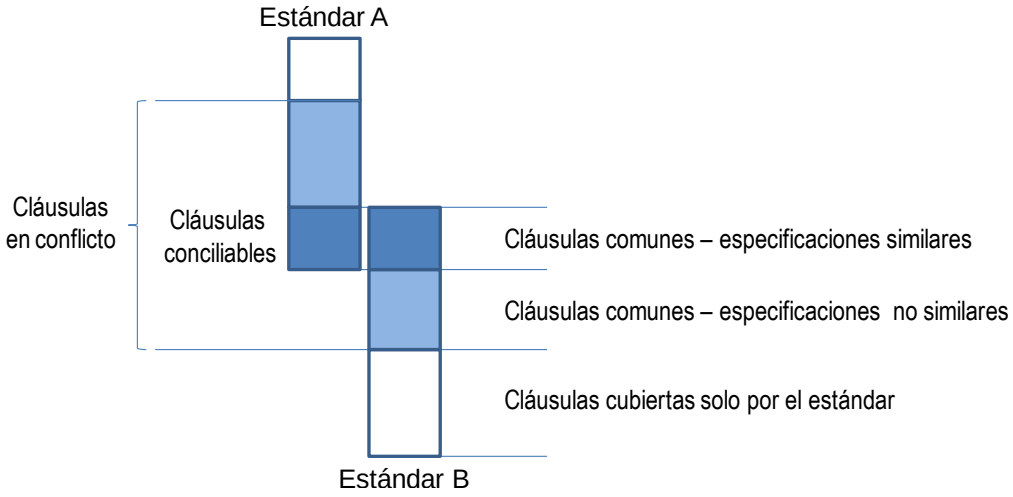
En la práctica, puede existir un conjunto aún más amplio de normas que estén ejerciendo fuerza normativa sobre el mismo campo, de forma que la intersección entre estándares es aún más compleja en la práctica, mostrando aspectos no cubiertos y posibles problemas de colisión entre estándares.

7.2. INCONSISTENCIA ENTRE CLÁUSULAS

Una intersección entre estándares puede producir:

- Cláusulas en común con especificaciones similares, fácilmente reconciliables en un mismo documento.
- Cláusulas en común con diferentes especificaciones, requisitos, metodologías y/o rangos de validez.
- Cláusulas que no son comunes, cubiertas solo por uno de los estándares.

Figura 28. Esquema de inconsistencias entre cláusulas

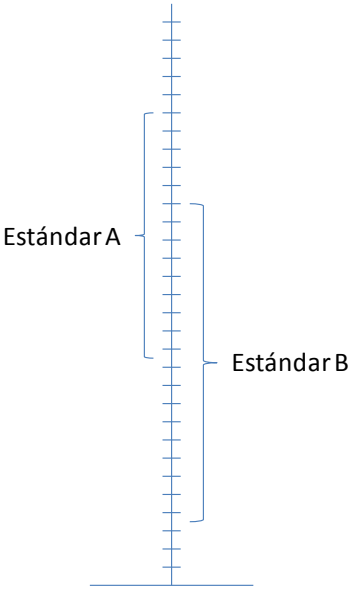


La inconsistencia entre estándares impide la total conformidad aún cuando un estándar esté plenamente adoptado, considerando que algunas normas (como la familia ISO) exige total cumplimiento con reglas legales y técnicas aplicables a la organización o proceso.

7.2.1. Inconsistencia parcial. En este caso, dos o más estándares poseen especificaciones, para un mismo aspecto, con valores o rangos de operación o validez similar o cercana, así como requisitos, metodologías y mecanismos de uso, control y/o medición.

Este tipo de inconsistencia demanda un trabajo adicional para lograr conformidad partiendo de un estándar específico para avanzar hacia los demás.

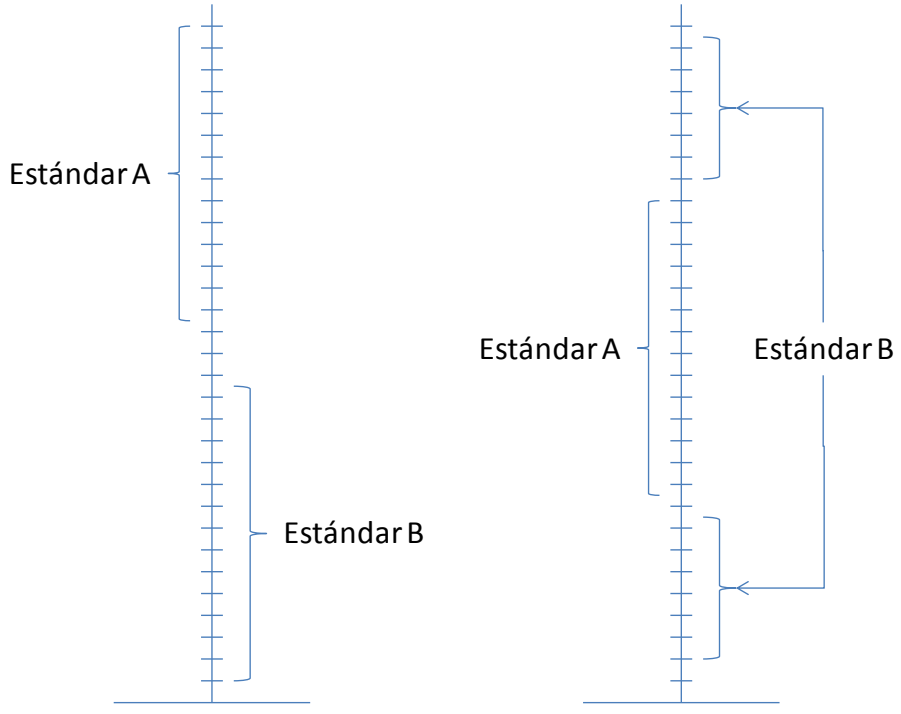
Figura 29. Estándares parcialmente equivalentes



Sin embargo, pueden existir restricciones o prohibiciones sobre usar especificaciones u operar fuera de un determinado rango de validez. En este caso, la conformidad total no es factible pues dar cumplimiento a un estándar automáticamente incumple los demás.

7.2.2. Inconsistencia total. En el peor escenario, dos o más estándares pueden tener cláusulas con especificaciones sobre un mismo aspecto, los cuales tienen valores o rangos de uso, operación o validez, completamente diferentes con los demás estándares alternativos. Este tipo de consisetncia puede ampliarse a los espacios metodológicos, de requisitos, de uso, control o de medición.

Figura 30. Estándares con requisitos no equivalentes o contradictorios



Este caso es un verdadero reto, lograr la conformidad con una norma técnica producirá una automática no conformidad contra los estándares alternativos.

Este caso es una situación común en organizaciones que tratan con mercados diversos, en diferentes ámbitos, bajo diversas autoridades legales y normativas, las cuales regulan la misma área según sus propios aspectos conceptuales, de contexto legal y socio económico así como tecnológico, además de los antecedentes técnicos, lo cual provee diferentes elementos de decisión que soportan sus especificaciones[262].

[262] NAMIRI, K., STOJANOVIC, N., “Towards a formal framework for business process compliance,” in Proceedings of the Multikonferenz Wirtschaftsinformatik, February 2008.

8. REVISION ARQUITECTONICA DE METODOLOGIAS EXISTENTES

8.1. ORIENTADAS AL CUMPLIMIENTO

8.1.1. Compliance driven Models, Languages and Architectures for Services. El proyecto COMPAS[263], fue concebido para asegurar la gestión dinámica del cumplimiento de servicios informáticos a las actuales regulaciones y los requisitos formales pactados para el servicio. El proyecto finalizó en enero de 2011.

Figura 31. Ciclo del proyecto COMPAS

Fuente:COMPAS

De manera análoga a los sistemas de gestión, COMPAS parte del ciclo PHVA enfrentándolo a siete etapas incluyendo la fase de diseño como la de ejecución, aplicable a todo tipo de emprendimiento tecnológico. Un aspecto interesante es la rotación que hace que la planeación del segundo ciclo inicie al final del primero, esto es, recogiendo las experiencias y resultados de la primera iteración.

[263] EUROPEAN COMISSION. SEVENTH FRAMEWORK PROGRAM. COMPAS Project. Vienna: http://www.compas-ict.eu/, 2010

Aspectos del cumplimiento. COMPAS establece los siguientes aspectos[264]:

a. **Descubrimiento marco normativo aplicable.** Busca encontrar normas de importancia para la organización y sus consecuencias. Para descubrir cuales normas existen y mantenerse al tanto de cambios y/o nuevas reglamentaciones se debe mantener un inventario de autoridades normativas, un directorio de controles normativos[265] con un registro de normas y su interpretación respecto de la organización, al igual que el registro de patrones de cumplimiento[266] para anticipar las infracciones asociadas.

b. **Especificaciones y requisitos aplicables**. Este aspecto se encarga de modelar los requisitos asociados al cumplimiento tanto en los procesos de negocios como en los temas externos. Diversos enfoques son aplicables para desarrollar este aspecto, uno de ellos es desarrollar objetivos de control dentro de la estructura de procesos de negocios[267], otro es aislar los procesos de negocio de los retos de cumplimiento para luego complementar dichos procesos con fases adicionales de formalización[268].

c. **Reporte del cumplimiento**. La medición y reporte del estado de cumplimiento de los procesos de negocio permite detectar infracciones de cumplimiento cuando éstas ya sucedieron (retrospectiva - correctiva) o cuando pueden suceder (detectiva/preventiva). Aquí es clave la disponibilidad de registros relacionados al cumplimiento[269].

---

[264] TILBURG UNIVERSITY. State-of-the-art in the field of compliance languages. 2008

[265] SADIQ, G., GOVERNATORI, "Modeling control objectives for business process compliance" Proceedings of the 5th International Conference on Business Process Management, 2007

[266] GHOSE, A., KOLIADIS, G., "Auditing business process compliance," in Proceedings of the International Conference on Service-Oriented Computing, 2007

[267] SADIQ, G., GOVERNATORI, NAIMIRI, K., "Modeling control objectives for business process compliance," in Proceedings of the 5th International Conference on Business Process Management, September 2007,

[268] LIU, Y., MULLER, S., XU, K., "A static compliance-checking framework for business process models," IBM Systems Journal, vol. 46, no. 2, pp. 335–362, 2007.

[269] VAN DER AALST, W., VAN DONGEN, B. F., HERBST, J., MARUSTER, L., SCHIMM, G.,

d. **Mejora continua de cumplimiento**. El constante refinamiento y ajuste de los procesos de negocios respecto al cumplimiento se basa en la evaluación continua para remediar las diferencias entre requisitos y el cumplimiento actual. En este punto es importante maximizar la consistencia entre procesos de negocio y los requisitos de cumplimiento [270] así como entre requisitos, e igualmente todo el universo de requisitos[271] incluyendo los de origen contractual.

   Otro aspecto importante es la trazabilidad entre el cumplimiento y los puntos mediante los cuales el o los procesos de negocio desarrollan tal obligatoriedad[272] que contribuye a la mejora del cumplimiento. Ahora, es factible que en las organizaciones algunos elementos exigidos por las normas son delegados a diversos participantes dentro de la jerarquía organizacional de forma que hay un responsable por uno o varios de esos elementos requeridos[273]. El modelo de delegación puede reforzar la trazabilidad.

e. **Gestión del riesgo**. Hace énfasis en los riesgos asociados con el cumplimiento, en especial en aquellas condiciones donde los requisitos no pueden ser logrados. Sobre el riesgo, COSO plantea que existen cambios asociados a factores externos (fuera de control de la organización), internos (de la organización) o asociados al cambio sobre cómo se responde y se maneja el cambio en el contexto interno o externo.

WEIJTERS, A. J. M. M, "Workflow mining: a survey of issues and approaches," Data and Knowledge Engineering, vol. 47, no. 2, pp. 237–267, 2003.

[270] GHOSE, A., KOLIADIS, G., "Auditing business process compliance," in Proceedings of the International Conference on Service-Oriented Computing, 2007

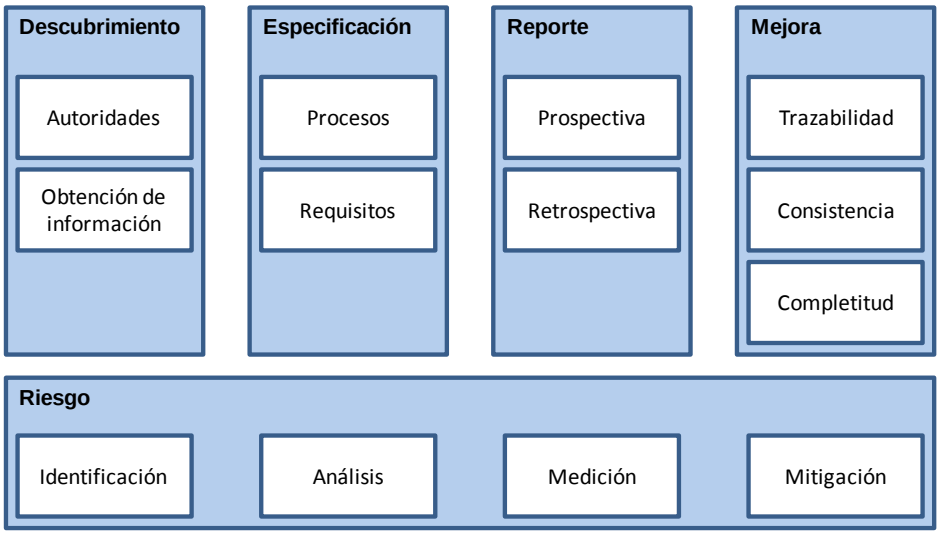
[271] GOEDERTIER, S., VANTHIENEN, J., "Designing compliant business processes with obligations and permissions," in Proceedings of the BPM 2006 Workshop, 2006

[272] GHANAVATI, S., AMYOT, D., PEYTON, L., "A requirements management framework for privacy compliance," in Proceedings of the Workshop on Requirements Engineering, 2007.

[273] BREAUX, T., ANTON, A., SPAFFORD, E., "A distributed requirements management framework for legal compliance and accountability", North Carolina State University Computer Science, Tech. Rep. 14, 2006.

En las organizaciones, algunos riesgos residen en sus procesos de negocio y deben obtener tratamiento considerando que a veces las normas plantean una obligatoriedad pero fallan al no indicar cómo lograr cumplimiento. Esto exige diseñar e implementar controles internos en los procesos de negocio[274]. Es importante tener en cuenta que los riesgos son dinámicos[275] y por ende el sistema de gestión del riesgo debe ser dinámico, responsivo y preventivo.

Figura 32. Aspectos del cumplimiento según COMPAS



Fuente: COMPAS

8.1.2. Métodos académicos.

a. Dekker y Hartog, proponen un método para el control de cumplimiento basado en auditoria aplicado a la salud[276]. En este caso, el método plantea mecanismos de control de disponibilidad y confidencialidad de información. De igual forma propone un esquema de políticas y acciones que producen registros auditables.

[274] NAMIRI, K., STOJANOVIC, N., "Towards a formal framework for business process compliance," in Proceedings of the Multikonferenz Wirtschaftsinformatik, February 2008.
[275] ZUR MUEHLEN, M., ROSEMANN, M., "Integrating risks in business process models," in Proceedings of the 16th Australasian Conference on Information Systems, Sydney, November-December 2005.
[276] DEKKER, M., HARTOG, J.. Audit-based Compliance Control (AC2) for EHR Systems. En: CTIT Technical Report. Enschede, NL: Universiteit Twente, 2007.

b. Cedersquit, Corin y otros, formularon un método para el control del cumplimiento basado en auditoría[277]. Este método establece una alineación entre políticas y acciones en la organización, en dos sentidos: Cual política debe ser satisfecha para satisfacer o justificar una acción, y que política se deduce de la realización de una acción, con el claro entendido que la política asume un rol de norma en la organización y los actores que las realizan asumen una responsabilidad por tal acción, o su omisión.

c. Gartner[278], plantea un proceso práctico de ocho pasos para la auditoria y gestión del cumplimiento en identificación y acceso.
   - Mejora de los procesos de autenticación.
   - Segregación de funciones – Gap Analysis (Análisis de diferencia entre lo normativo y lo implementado)
   - Control de acceso basado en roles.
   - Gestión continua de la matriz de roles.
   - Reforzamiento de la segregación de funciones.
   - Gestión de control de identidad y acceso.
   - Revisión de la gestión.
   - Gestión continua de procesos.

d. Sobre modelamiento del cumplimiento normativo, Grigoris Antoniou, David Billington, Guido Governatori y Michael J. Maher[279], abordan el cumplimiento como problema a ser modelado para su análisis. Esta propuesta está orientada a facilitar el análisis de las normas (marco normativo y técnico) que enfrenta una organización.

---

[277] CEDERQUIST, J., CORIN, R., y otros, Audit-based Compliance Control. En: International Journal of Information Security, 2007. Pag 133-151.

[278] GARTNER. Use This Eight-Step Process for Identity and Access Management Audit and Compliance. Gartner Research. 2005

[279] ANTONIOU, G., BILLINGTON, y otros. ON MODELING AND ANALYSIS OF REGULATIONS. Proceedings of the Australian Conference Information Systems, pages 20-29, Sidney, 1999

e. De manera similar, Guido Boella, Guido Governatori, Antonino Rotolo, and Leendert van der Torre, plantean enfoques para el estudio de la complejidad de los sistemas legales, su interpretación y cumplimiento[280] y mecanismos para el entendimiento lógico de la interpretación legal[281], en especial:

- Jerarquía de regulaciones. Las normas tienen jerarquías y las autoridades de donde provienen o por quienes fueron creadas igualmente, es conveniente tener presente la jerarquía al momento de establecer la obligatoriedad.
- Conocimiento ontológico. Las normas se dan en un ambiente definido y los términos son comunes al sector socio económico al cual está determinada cierta norma.

f. Sobre el incumplimiento normativo, Guido Governatori and Antonino Rotolo, plantean un método de razonamiento del incumplimiento obligado, es decir dictado por otras normas que contradicen la primera[282], un algoritmo para el cumplimiento en procesos de negocio[283] y un modelo conceptual en la misma área[284], los cuales básicamente enlazan las tareas de un proceso frente a las obligaciones que los crean o se derivan.

---

[280] BOELLA, G., GOVERNATORI, y otros. LEX MINUS DIXIT QUAM VOLUIT, LEX MAGIS DIXIT QUAM VOLUIT: A FORMAL STUDY ON LEGAL COMPLIANCE AND INTERPRETATION. AI APPROACHES TO THE COMPLEXITY OF LEGAL SYSTEMS. LNAI. Springer. Berlin, 2010.

[281] BOELLA, G., GOVERNATORI, y otros. A LOGICAL UNDERSTANDING OF LEGAL INTERPRETATION. IN PROCEEDINGS AAAI, 2010.

[282] GOVERNATORI, G. ROTOLO, A.. LOGIC OF VIOLATIONS: A GENTZEN SYSTEM FOR REASONING WITH CONTRARY-TO-DUTY OBLIGATIONS. Australasian Journal of Logic 4: 193-215, 2006.

[283] GOVERNATORI, G. ROTOLO, A.. AN ALGORITHM FOR BUSINESS PROCESS COMPLIANCE. Legal Knowledge and Information Systems (Jurix 2008), Frontieres in Artificial Intelligence and Applications 189, pages 186-191. IOS Press, 2008.

[284] GOVERNATORI, G. ROTOLO, A.. A CONCEPTUALLY RICH MODEL OF BUSINESS PROCESS COMPLIANCE. In Sebastian Link and Aditya Ghose, editors, 7th Asia-Pacific Conference on Conceptual Modelling (APCCM 2010), CRPIT. ACS, 2010.

8.2. ORIENTADAS A LA MADUREZ Y CAPACIDAD

8.2.1. Software Process Improvement and Capability Determination (SPICE – ISO 15504). La norma ISO 15504 SPICE es una norma abierta e internacional para evaluar y mejorar la capacidad y madurez de los procesos[285], la cual guarda compatibilidad con el modelo CMM (los equipos de trabajo son similares), y puede ser utilizada para garantizar la madurez del proceso de cumplimiento.

Figura 33. Niveles de SPICE – ISO 15504

Fuente: ISO 15504

Se debe observar que el nivel 3 exige contar con procesos adaptados a estándares, pilar del cumplimiento, mientras que el nivel 5 demanda la mejora continua de los procesos, aspecto clave que permite incrementar de forma continua el grado de cercanía entre las normas que aplican en una organización y su adopción e implementación.

[285] http://www.iso15504.es/index.php/la-norma-iso-15504-spice.html

Tabla 16. Desarrollo de niveles en el ISO 15504

NIVEL	SUBNIVELES
BASICO Objetivos de procesos	Desempeño de procesos
GESTIONADO Gestión de procesos y productos	Gestión del desempeño Gestión del trabajo
ESTABLECIDO Procesos adaptados a estándares	Definición de procesos Implementación de procesos
PREDECIBLE Gestión cualitativa	Medición de procesos Control de procesos
OPTIMIZANDO Mejora continua de los procesos	Innovación en procesos Optimización de procesos

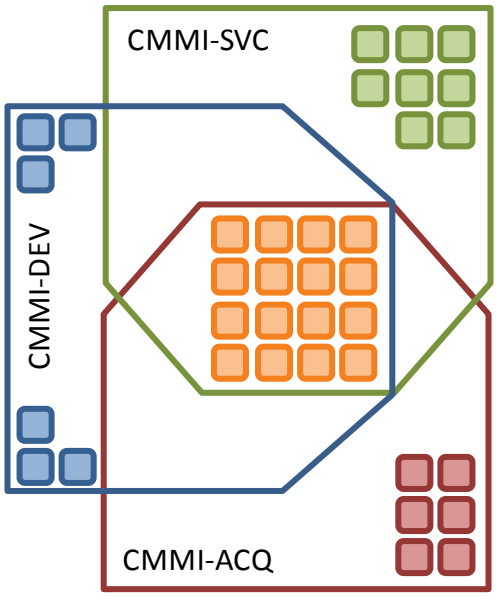
8.2.2. Capability Maturity Model® Integration (CMMI). El modelo CMMI[286] desarrollado por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon, plantea un esquema orientado a la madurez que reúne a ISO 15504 e ISO 20000, y es aplicable a la industria en general, no solamente la de software.

En efecto, el mismo instituto[287], hace un análisis sobre la aplicación del CMMI enfocado a servicios resaltando que la economía colombiana está basada en un 64% en la prestación de servicios: Financieros (18.1%), Gobierno (17.5%), Comercio (13.4%), Transporte y Comunicaciones (7%), Construcción y trabajos públicos (5%) y servicios públicos (2.7%)

[286] http://www.sei.cmu.edu/cmmi/solutions/index.cfm
[287] CARNEGIE MELLON UNIVERSITY – SOFTWARE ENGINEERING INSTITUTE. CMMI Services 1.3 presentation, 2011.

8.2.2.1. Esquema de procesos. CMMI está estructurado en un modelo que atiende los aspectos relacionados con servicios, adquisiciones y desarrollo:

Figura 34. Integración del CMMI



Procesos comunes

1. Causal Analysis and Resolution (CAR). El proceso de análisis y solución de causas, está orientado a detectar las causas del resultado de cierto proceso o trabajo y propone tomar acciones efectivas para asegurar los buenos resultados y prevenir los resultados erróneos o inadecuados. Este proceso corresponde a organizaciones de alta madurez.
2. Configuration Management (CM). La gestión de la configuración controla los cambios a los a los procesos y trabajos cruciales de la organización.
3. Decision Analysis and Resolution (DAR). El proceso de análisis y solución para toma de decisiones formaliza la toma de decisiones en aspectos críticos de la organización.
4. Integrated Project Management (IPM). La gestión integral del trabajo busca maximizar resultados de procesos y equipos de trabajo en tareas complejas.

5. Measurement and Analysis (MA). El proceso de medición y análisis hace énfasis en la medición y análisis como mecanismo de control de procesos.
6. Organizational Process Definition (OPD). La definición de procesos en la organización establece la estandarización de procesos y su divulgación en la organización.
7. Organizational Process Focus (OPF). El enfoque a procesos de la organización hace énfasis en controlar las fortalezas y debilidades de los procesos de negocio, de forma que se pueda planear que mejorar y facilitar la implementación de tales mejoras.
8. Organizational Performance Management (OPM). El proceso gestión del desempeño organizacional se enfoca en la gestión de mejoras e innovaciones usando una base estadística a partir del desempeño de procesos. Este proceso corresponde a organizaciones de alta madurez.
9. Organizational Process Performance (OPP). El proceso de desempeño de procesos de negocio, está enfocado a mantener registros e informar sobre el desempeño de los procesos y como éste afecta la calidad del servicio. Este proceso corresponde a organizaciones de alta madurez.
10. Organizational Training (OT). El proceso de entrenamiento de la organización busca hacer énfasis en el desarrollo de las destrezas y conocimiento de las personas de forma que se asegure la prestación de servicios de elevada calidad.
11. Work Monitoring and Control (WMC). El control y monitoreo de los trabajos buscan proporcionar seguridad razonable sobre logro de resultados y control de desviaciones frente a lo planeado.
12. Work Planning (WP). La planeación del trabajo se orienta a planear costos, esfuerzos, programas de trabajo, recursos, entendiendo quienes participarán en los procesos, mientras hace gestión del riesgo y los recursos involucrados.
13. Process and Product Quality Assurance (PPQA). El proceso de aseguramiento de la calidad de productos y procesos, busca asegurar que la organización haga lo que dicho en la política, normas técnicas y procedimientos.

14. Quantitative Work Management (QWM). La gestión cuantitativa del trabajo se encarga de gestionar el trabajo bajo consideraciones cuantitativas y de control de desempeño. Este proceso corresponde a organizaciones de alta madurez.
15. Requirements Management (REQM). La gestión de requisitos mantiene transparencia con los grupos de interés sobre los productos y servicios que la organización provee y refuerza los ajustes necesarios para detectar inconsistencias y evitar mal información.
16. Risk Management (RSKM). La gestión del riesgo está orientada a asegurar el éxito de la entidad (el logro de los objetivos corporativos) al anticipar problemas y su manejo antes que éstos ocurran.

Procesos especializados en servicios

1. Capacity and Availability Management (CAM). El proceso de gestión de la capacidad y disponibilidad busca asegurar que la organización posea la cantidad suficiente y adecuada de recursos necesarios para proveer servicios de manera oportuna a un costo adecuado.
2. Incident Resolution and Prevention (IRP). El proceso de solución y prevención de incidentes maneja aquellos aspectos que han tenido problemas y previene que tales situaciones sucedan (de forma detectiva, preventica o correctiva).
3. Supplier Agreement Management (SAM). La gestión de acuerdos con proveedores busca asegurar la máxima disponibilidad y calidad por parte de los proveedores.
4. Service Continuity (SCON). El proceso de continuidad del servicio permite estar listo para recuperarse de un desastre y volver a la mayor brevedad a la operación.
5. Service Delivery (SD). El proceso de entrega de servicios, establece acuerdos de servicio, considerando las solicitudes, los procesos y la prestación del servicio.

6. Service System Development (SSD). El proceso de desarrollo del sistema de servicio se asegura que la organización cuente con lo necesario para prestar servicios, incluyendo el recurso humano, procesos, consumibles y equipos.
7. Service System Transition (SST). El proceso de gestión de la transición en el sistema de prestación del servicio, busca que los procesos estén en su lugar, mantener los sistemas existentes o retirando los obsoletos, mientras minimiza el impacto negativo en la prestación del servicio.
8. Strategic Service Management (STSM). La gestión de servicios estratégicos, decide que servicios está la organización provee, asegura que sean acordes con estándares aplicables, comunicando y divulgando los aspectos respectivos.

Procesos especializados para adquisiciones

1. Acquisition Requirements Development (ARD). El desarrollo de requisitos tiene como objetivo obtener los requisitos de un producto o servicio, desarrollarlos y analizarlos para trasladarlos a acuerdos y contratos.
2. Solicitation and Supplier Agreement Development (SSAD). El desarrollo de acuerdos entre solicitud y proveedor tiene como propósito preparar el paquete de requisitos, seleccionar proveedores, para luego establecer y mantener un acuerdo formal con el proveedor.
3. Agreement Management (AM). La gestión de los acuerdos busca asegurar que el proveedor y el comprador se comportan conforme al acuerdo suscrito entre ellos.
4. Acquisition Technical Management (ATM). La gestión técnica de adquisiciones busca evaluar las soluciones técnicas propuestas por los proveedores y gestionar interfaces seleccionadas de dichas soluciones.
5. Acquisition Verification (AVER). La verificación de la adquisición busca asegurar que los productos o servicios seleccionados cumplen los requisitos especificados.

6. Acquisition Validation (AVAL). La validación de la adquisición tiene como objeto el demostrar que un producto o servicio adquirido cumple con sus objetivos una vez ha sido ubicado en su ambiente especificado.

Procesos especializados en desarrollo

1. Product Integration (PI). El proceso de integración de productos se encarga de poner juntos los componentes necesarios y adecuados de forma que el producto tenga el comportamiento y las características esperadas.
2. Requirements Development (RD). El desarrollo de requisitos se encarga de entender las necesidades de los grupos de interés, registrando y comunicando tales aspectos al equipo de desarrollo de productos y servicios.
3. Supplier Agreement Management (SAM). La gestión de acuerdos con proveedores busca asegurar la máxima disponibilidad y calidad por parte de los proveedores.
4. Technical Solution (TS). El proceso de soluciones técnicas usa procesos de forma efectiva para desarrollar soluciones que cumplan con las necesidades de los clientes.
5. Validation (VAL). Este proceso busca asegurar que las soluciones satisfagan las necesidades de los usuarios en el ambiente de servicios.
6. Verification (VER). Este proceso se encarga de verificar que la solución satisfaga los requisitos pactados.

8.2.2.2. Madurez y capacidad. CMMI distingue entre madurez y capacidad, y establece diferentes escalas para su calificación[288].

Capacidad. Refiere al logro de mejora en los procesos de la organización, de

[288] CARNEGIE MELLON UNIVERSITY – SOFTWARE ENGINEERING INSTITUTE. CMMI for Acquisition 1.3, 2011.

manera individual. En el caso de la capacidad, el CMMI usa un esquema de representación de etapas de forma continua entendiendo que la organización toma sus procesos y los gestiona y mejora de manera continua, extendiendo el logro alcanzado en un proceso hacia los demás procesos de la organización.

0. Incompleto. Proceso que no se realiza o se lleva a cabo de manera incompleta. No se satisfacen las metas del área a la cual pertenece el proceso.
1. Realizado. Procesos que se realizan para lograr un producto esperado, satisfaciendo las metas del área a la cual pertenece el proceso.
2. Gestionado. Los procesos gestionados son realizados conforme a políticas, planeación y control, empleando destrezas con los recursos suficientes para obtener productos controlados, revisados y evaluados para asegurar adherencia a la descripción técnica del producto.
3. Definido. Un proceso definido es un proceso gestionado que se ajusta a los estándares que la organización ha elegido o debe aplicar, está plenamente documentado, de forma rigurosa, y desde luego contribuye a la organización como un activo productivo.

Conforme a lo anterior, un nivel tres de capacidad establece un alto nivel de compromiso frente al tema de cumplimiento normativo.

Madurez. Refiere al logro de mejora en procesos de la organización, de forma simultánea a través de diversas áreas o procesos. En cuanto a la madurez, el CMMI plantea un esquema de representación por etapas, de forma que la organización tenga procesos seleccionados que son gestionados conforme a un determinado nivel de madurez.

1. Inicial. En este nivel, los procesos se hacen de forma intuitiva y tienden a ser caóticos, no hay un ambiente organizacional estable para soportar los procesos.

Usualmente los procesos en este nivel tienen un alto nivel de errores, fallas y excesos de costos o consumo de tiempo, además de posibles abandonos.

2. Gestionado. En este caso, el enfoque a proyectos fija la base en la organización para la mejor adquisición de recursos. En este nivel los procesos son gestionados según una planeación que es acorde con las políticas de la organización.

   En este nivel, se adquieren recursos adecuados, asigna responsabilidades, controla, revisa y evalúa los productos obtenidos además de gestionar la configuración en la organización.
3. Definido. En ese nivel, se fortalece el enfoque a proyectos de forma integrada en los procesos de negocio y se verifica el cumplimiento de requisitos. Los procesos en este nivel están bien definidos y documentados a nivel de proceso, procedimientos, método y estándares aplicables, estando ajustados a las normas que le sean aplicables, para lograr consistencia a lo largo de la organización.
4. Gestionado cuantitativamente. La organización establece objetivos cuantitativos para el control de la calidad y el desempeño de procesos, mide y analiza tal información en términos estadísticos, y emplea dicha información en la gestión de los procesos. Los objetivos surgen a partir de las necesidades y requisitos de los grupos de interés. En este nivel, se obtiene la capacidad de predecir el comportamiento de los procesos.
5. Realizando optimizaciones. En el máximo nivel la organización realiza mejora continua a sus procesos, objetivos y necesidades de desempeño sobre una base cuantitativa de información, y analiza las desviaciones estadísticas del servicio o producto entregado frente a los compromisos asumidos.

Conforme a lo anterior, un nivel cinco de madurez establece un alto nivel de compromiso frente al tema de cumplimiento normativo.

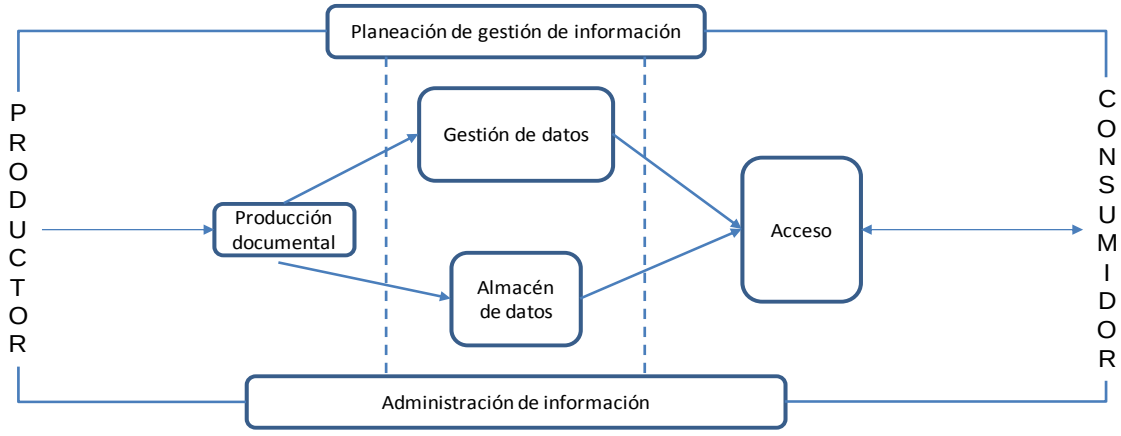
Tabla 17. Comparación de niveles de capacidad y madurez en el CMMI

NIVEL	CAPACIDAD	MADUREZ
Nivel 0	Incompleto	
Nivel 1	Realizado	Inicial
Nivel 2	Gestionado	Gestionado
Nivel 3	Definido	Definido
Nivel 4		Gestionado cuantitativamente
Nivel 5		Realizando optimizaciones

9. EL MAPA TECNICO

9.1. EL PROCESO DE GESTION DE LA INFORMACION

Figura 35. El proceso de gestión de la información



El proceso típico de gestión de la información, con énfasis en las instituciones públicas, integra una planeación documental que incluye el programa de gestión documental, las tablas de retención documental (que estructuran la información en series y sub-series y a su vez dicta el tiempo de retención en el archivo), la política de gestión de documentos en la organización[289], al igual que la necesidad de contar en información para diversos sistemas de gestión como los de calidad[290] y control interno[291], entre otros.

La fase de ejecución (el hacer) consiste principalmente en tres aspectos: la producción de documentos (entendida ésta como la que se produce al interior de la organización como también la que se recibe de fuentes externas, el trámite documental (Recorrido del documento desde su producción o recepción, hasta el

[289] Ley 594 de 2000
[290] Ley 872 de 2003
[291] Ley 87 de 1993

cumplimiento de su función administrativa) en ejercicio de los procesos de negocio y las actividades de consulta bajo normas de oportunidad, disponibilidad y seguridad.

En cuanto a la verificación, ésta suele suceder en ocasionales auditorías que realizan las oficinas de control interno u órganos externos y la actuación a través de planes de acción o mejoramiento. Sin embargo, es usual que estas dos últimas actividades sean poco frecuentes.

Las anteriores fases, se reúnen en el concepto de gestión documental, entendida como el conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación[292] [293].

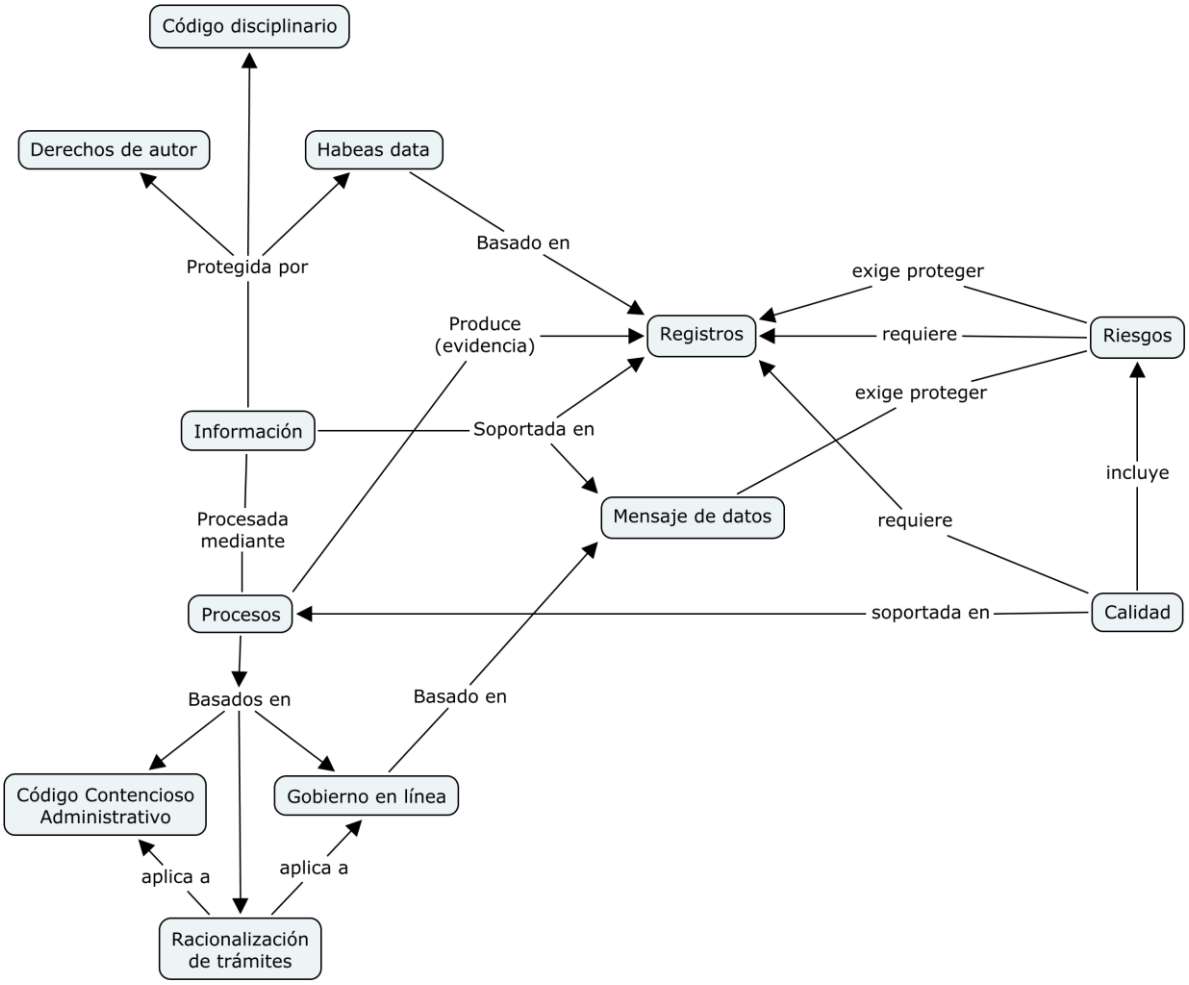
De igual manera, la norma de calidad para el sector público colombiano añade en su numeral 4.2 la obligatoriedad de procedimientos documentados y registros producidos por la entidad.

De igual manera, el manual de implementación del MECI[294], plantea que la información es un bien de interés para las organizaciones, por cuanto es insumo y producto en la ejecución de procesos, garantiza la transparencia en la actuación pública y rendición de cuentas e igualmente aporta a la evaluación y mejora de los procesos.

[292] Ley 594 de 2000, Art. 3
[293] Norma NTCGP 1000:2009, numeral 3.29
[294] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA, Manual de implementación del MECI, 2008.

9.2. RELACION CONCEPTUAL

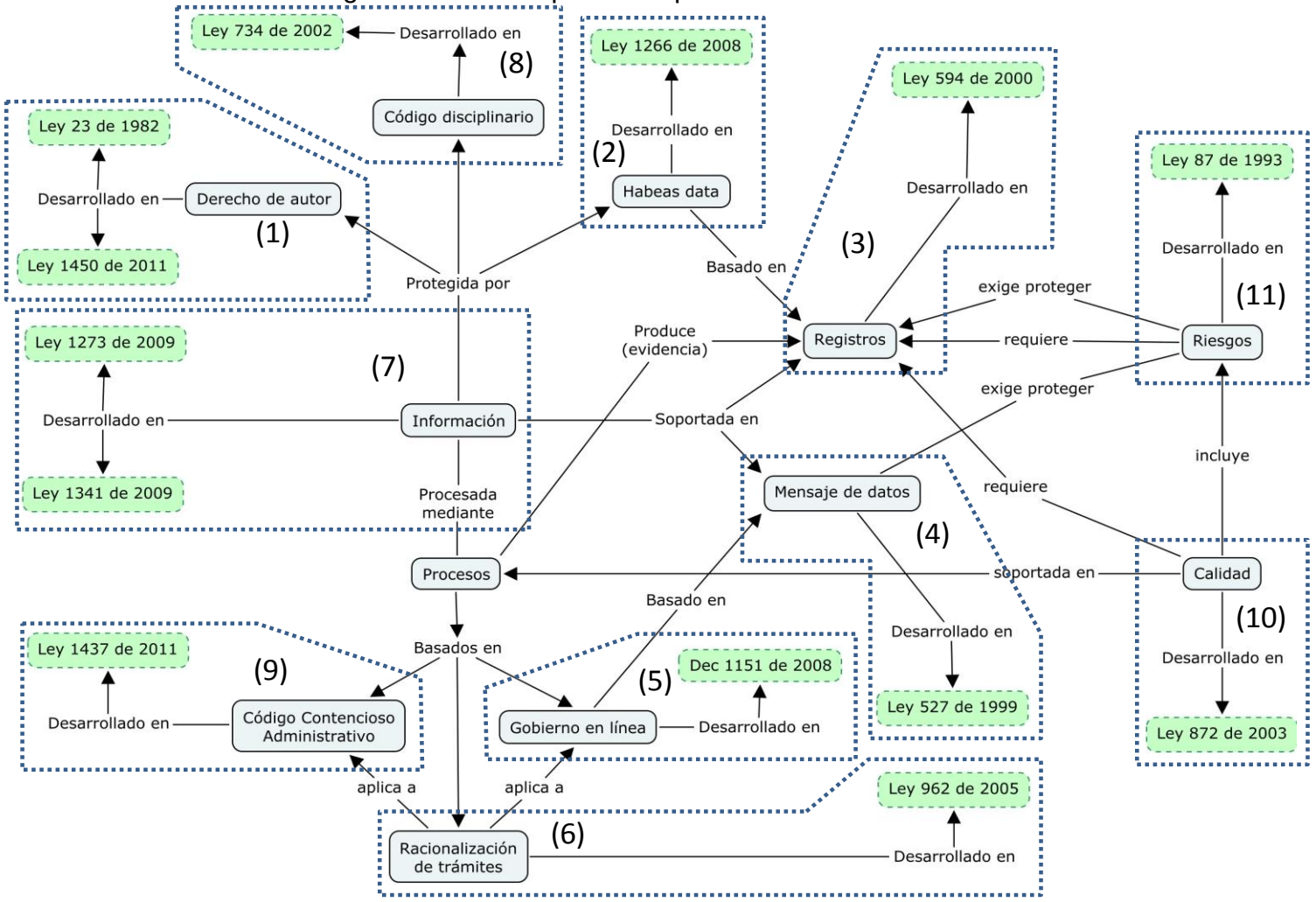
Figura 36. Despliegue del concepto de información



Considerando lo expuesto en la teoría de la información y las comunicaciones, se tiene que la información reposa como registros almacenados sobre diversos tipos de soportes (analógicos o digitales) o se transmite a manera de mensajes de datos, en ambos casos producidas o tramitadas por procesos organizacionales que para la administración pública obran dentro de las funciones estipuladas legalmente. La información posee igualmente la protección sobre su contenido bien sea en lo personal o por derecho de autor, y es la base legal para los sistemas de gestión de la calidad y de gestión del riesgo.

9.3. NORMATIVIDAD LEGAL ASOCIADA

Figura 37. Relación de normas legales asociadas por concepto informático.



El mapa conceptual mostrado, resalta en verde las normas legales asociadas para cada concepto (contexto jurídico colombiano), de donde surge el mapa de requisitos legales por norma, resaltando solo aquellos involucrados directamente con gestión de información:

Derecho de autor. La Ley 23 de 1982 sienta la base de protección de las obras literarias, científicas y artísticas, donde el software se considera como una obra literaria. Esta norma fue modificada mediante la Ley 1450 de 2011 que establece el manejo que sobre el derecho de autor debe darse en el caso de los contratos de prestación de servicios.

Habeas data. Sobre el derecho de las personas de conocer, actualizar y rectificar datos que sobre ellas tengan los bancos de datos, y los aspectos relacionados con recolección, tratamiento y circulación de datos personales, así como el derecho a la información, la Ley 1266 de 2008 reglamenta estos aspectos para bancos de datos privados o públicos.

Registros documentales. La Ley General de Archivo, Ley 594 de 2000, establece la obligatoriedad de la conformación del archivo de manera independiente a su soporte, sea físico o virtual, de la gestión documental, de la validez de diversos soportes documentales, de la clasificación e inventario documental así como los controles aplicables a la consulta y acceso a la información. Establece el manejo de la información en forma de documento.

Mensajes de datos. La Ley 527 de 1999 reconoce a la información cuando está en la forma de un mensaje de datos y le otorga validez jurídica y técnica.

Gobierno en línea. El Decreto 1151 de 2008 plantea la universalización de trámites en las organizaciones públicas mediante el uso de plataformas informáticas en Internet, haciendo uso extensivo del concepto de mensajes de

datos y documentos de forma digital.

Racionalización de trámites. El gobierno colombiano en su intención de adoptar técnicas modernas de gestión, ha propuesto la simplificación de trámites iniciando con la Ley 962 de 2005, tanto en la solicitud de información como en la entrega de la misma, incluyendo los trámites al interior de las organizaciones públicas.

Información. El reconocimiento de la información como bien, hace que sea susceptible de ser objeto del delito. Para este fin expidió la Ley 1273 de 2009 que versa sobre los delitos informáticos. De igual manera, el concepto de tecnologías de la información y las comunicaciones ha sido reglamentado como de necesaria intervención nacional a través de la Ley 1341 de 2009, conocida como Ley de TICs.

Código disciplinario. La Ley 734 de 2002 establece deberes que los servidores públicos deben atender en materia de gestión de documentos e información.

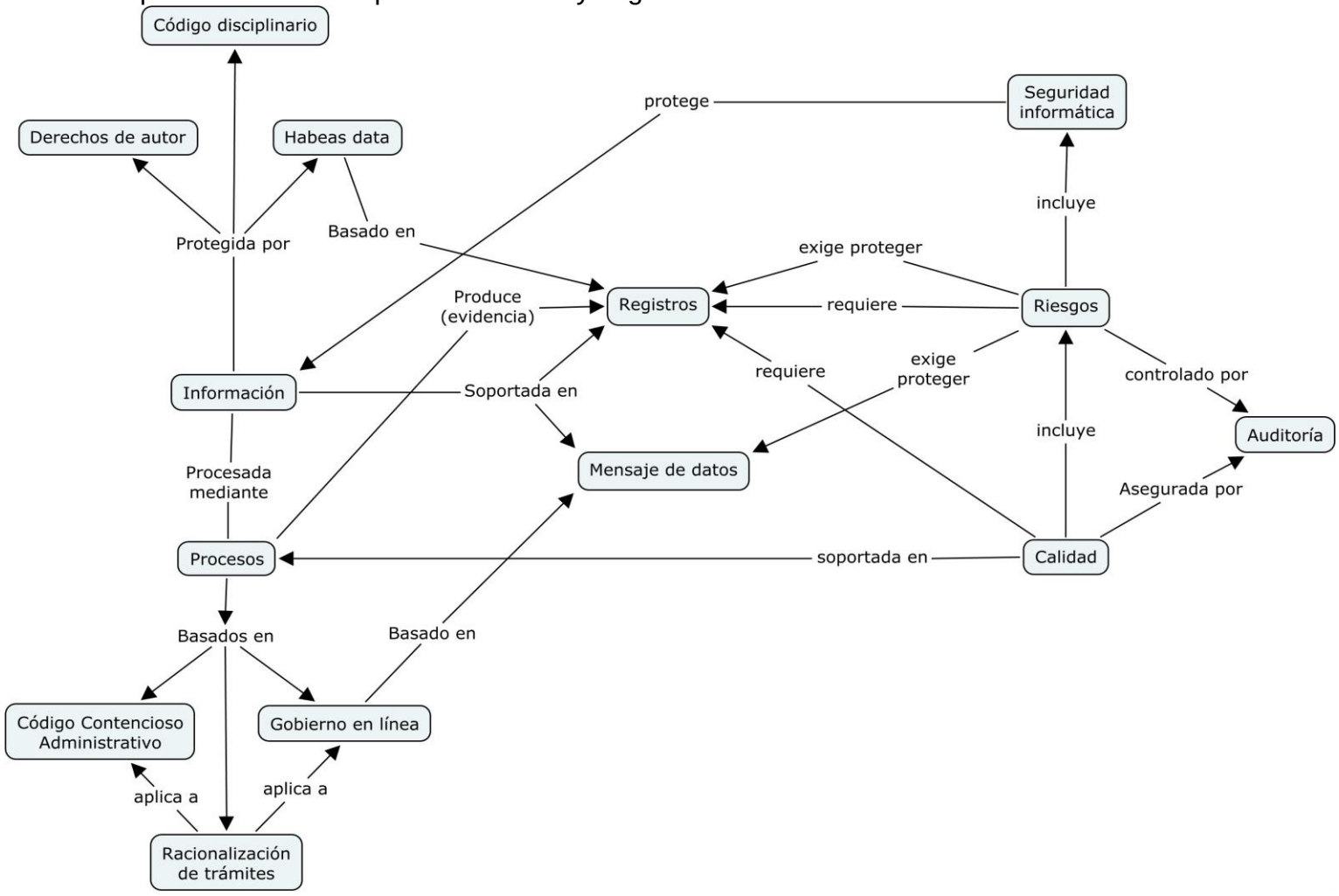
Código contencioso administrativo. La Ley 1437 de 2011 establece una guía jurídica frente al desarrollo de actuaciones administrativas incluyendo las iniciadas por terceros tal como el derecho de petición, entre otros, que incluyen gestión de información.

Gestión de la calidad. La Ley 872 de 2003 creó el sistema de gestión de la calidad para el sector público, el cual tiene dentro de la norma técnica (numeral 4) la obligatoriedad de contar con documentos incluyendo registros de evidencia operativa.

Control interno. El control interno tiene dentro de sus componentes el de la información y los sistemas de información que la gestionan, tal como fue creado por la Ley 87 de 1993.

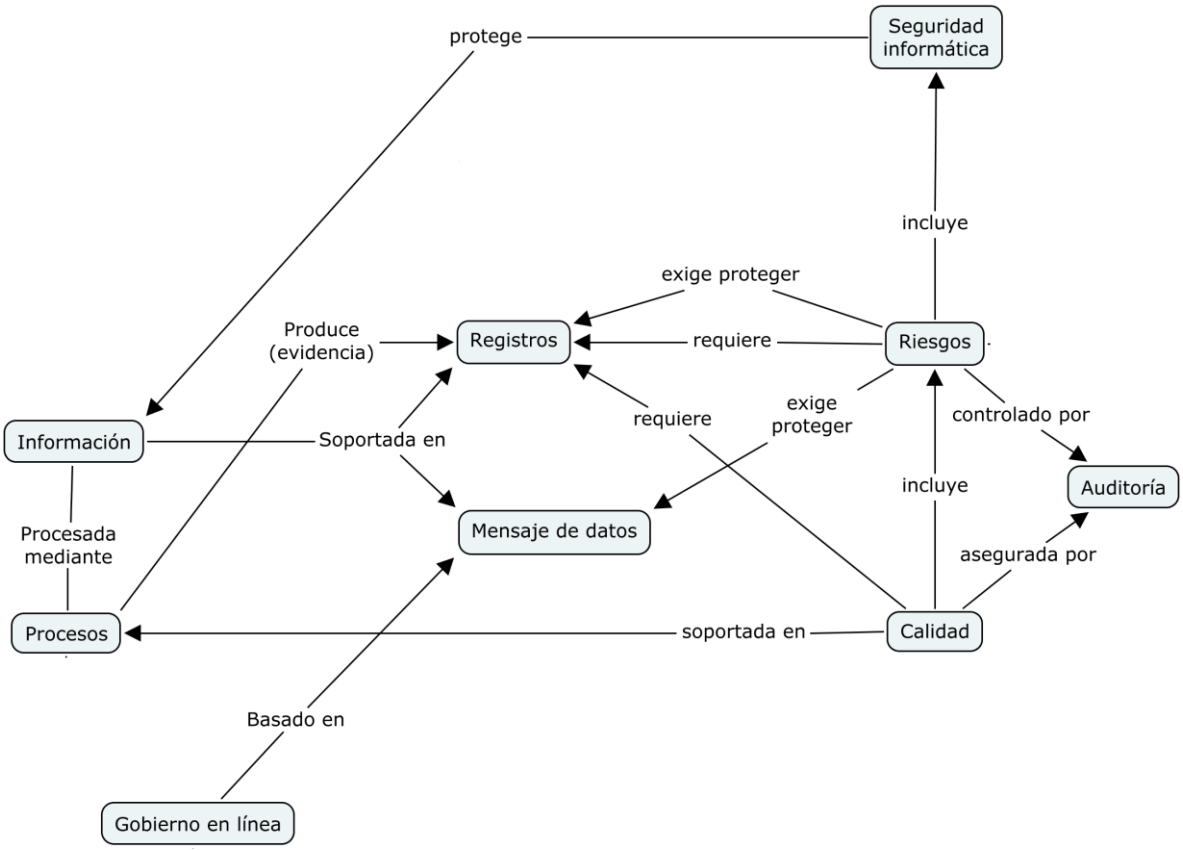
9.4. DESPLIEGUE TÉCNICO

Figura 38. Incorporación del concepto de auditoría y seguridad informática



Por lo anterior, para poder determinar el cumplimiento, se hace necesario incorporar los elementos de auditoría y de gestión necesarios (y mandatorios) como el de calidad, riesgo y control interno así como el de seguridad informática.

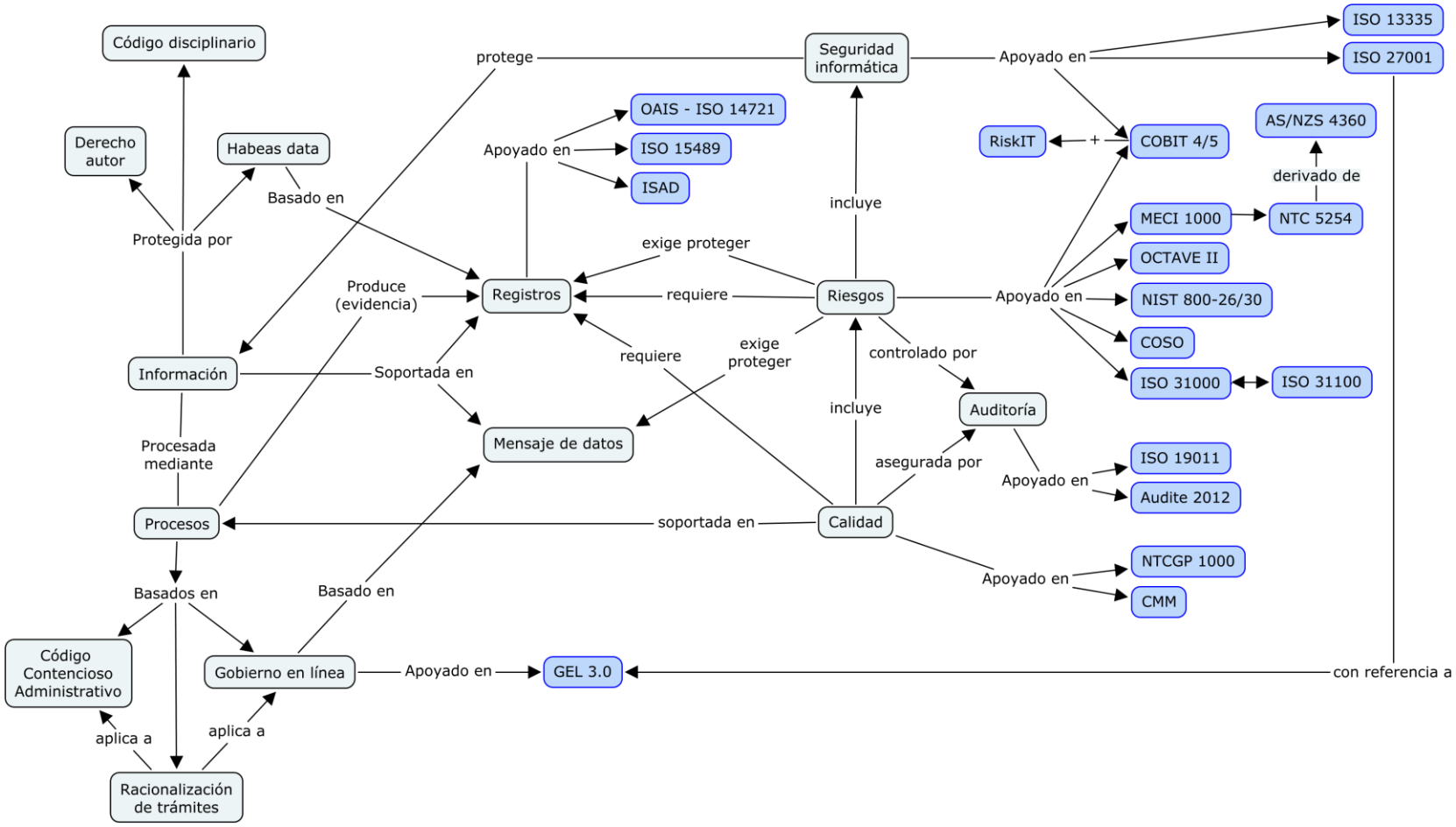
Figura 39. Incorporación del concepto de auditoría y seguridad informática



Frente a estos elementos, se ubican normas ampliamente conocidas en el mercado las cuales fueron previamente analizadas en este documento. Para cada norma se estudiaron los aspectos clave de forma que se pudieran recoger las consideraciones más importantes que resaltan por su impacto en una metodología de cumplimiento o aquellos que son concordantes en varias de ellas. Las normas técnicas asociadas a cada concepto (en el contexto técnico nacional e internacional) de uso más frecuente en la industria son marcadas en azul en la siguiente sección.

9.5. NORMATIVIDAD TECNICA ASOCIADA

Figura 40. Normas técnicas por concepto



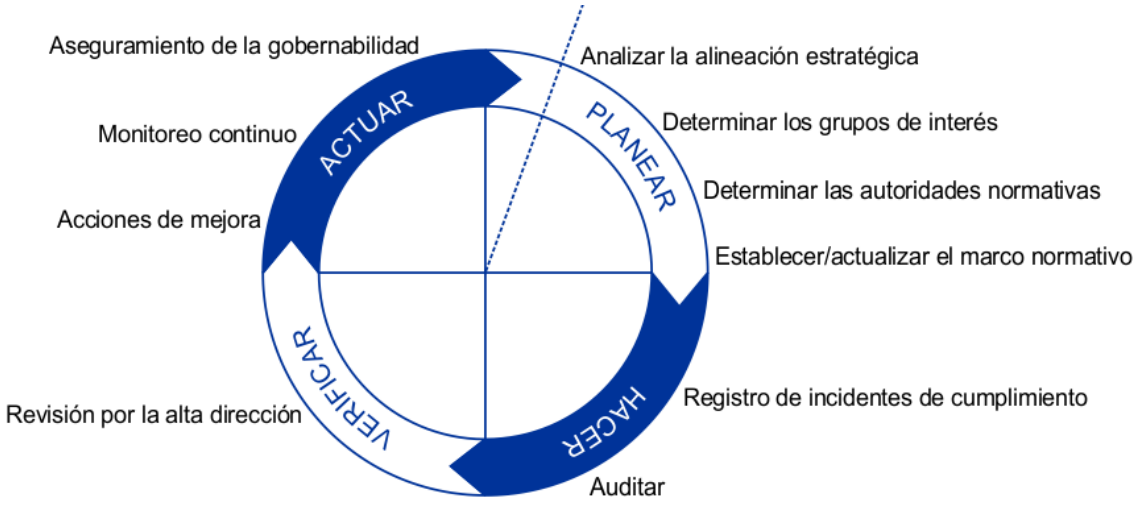
10. EVALUACION DEL CUMPLIMIENTO Y EL RIESGO

10.1. METODOLOGÍA PROPUESTA

La metodología propuesta en esta investigación armoniza los requisitos y planteamientos de diversas normas, mostradas y analizadas en este documento, y fuertemente basada en el ciclo de mejora continua y en auditoría.

10.1.1. El ciclo de mejora continua. Los sistemas de gestión están basados en el ciclo PHVA, o ciclo Deming, tal como se evidencia en la revisión normativa.

Figura 41. Ciclo de mejora continua para la propuesta metodológica



Sobre dicho ciclo, es conveniente plantear las siguientes actividades por fase:

1. **Planear**:
   a. La planeación de la gestión del cumplimiento surge del direccionamiento estratégico de la organización en cuyo debe converger los objetivos de TI

(Tecnologías de la Información y las Comunicaciones) como primer elemento de verificación del cumplimiento.

b. Entendidos los objetivos de la organización, la organización debe tener conciencia sobre los grupos de interés y la incidencia de éstos en el marco de aspectos obligados para la organización.
c. Algunos de estos grupos de interés se comportan como autoridades que producen normas jurídicas o técnicas mientras que otros demandan su cumplimiento.
d. Finalmente, debe conocerse el universo normativo que será armonizado en una única base para poder medir, controlar y verificar el cumplimiento.

2. **Hacer**: Dado que la metodología busca mejorar cumplimiento, existen dos momentos en los cuales este aspecto es atendido:
   a. Registro de incidentes de cumplimiento, por detección de situaciones de no cumplimiento o en el evento de acciones de control.
   b. Auditoría al estado actual del cumplimiento en la organización.

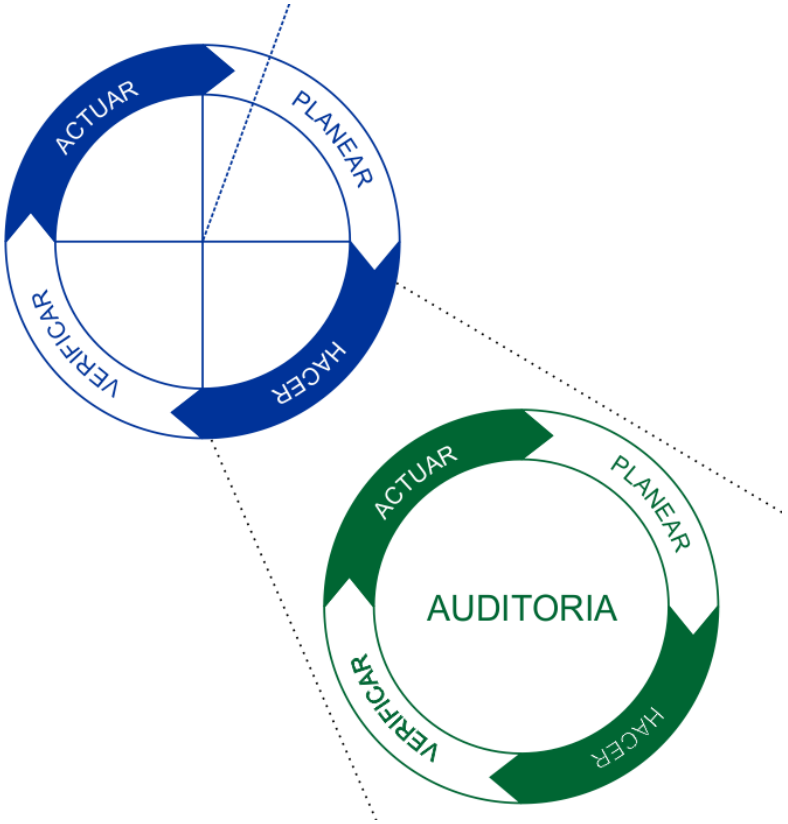
3. **Verificar**: De manera similar a diversos sistemas de gestión, la verificación se realiza mediante la revisión por parte de la alta dirección, posiblemente en manos del oficial de cumplimiento o de control interno del organismo auditado.

4. **Actuar**: Al ser un proceso basado en un ciclo de mejora continua, y entendiendo que el cumplimiento es una acción continua e iterativa orientada a la mejora continua mientras se garantiza que la organización cuenta con la madurez institucional suficiente para mantener el status alcanzado, se plantean varias actividades:
   a. Acciones de mejora. Las acciones de mejora preventivas, detectivas y correctivas (cuando ya ha sucedido el no cumplimiento) atacan directamente la causa y efecto del posible no cumplimiento. Una posible acción es la mejora del proceso de gestión de cumplimiento en sí mismo.

b. Monitoreo continuo. Una acción especial es mantener el monitoreo continuo y alerta temprana en la organización de forma que se reduzca la exposición al riesgo del no cumplimiento.
c. Aseguramiento de la gobernabilidad. La gobernabilidad tiene implícito cumplimiento. Permite enlazar objetivos, políticas, procesos y marco normativo.

10.1.2. El ciclo de mejora continua integrado. Al ser la presente metodología basada en auditoría como la herramienta principal para medir el cumplimiento, y siendo la auditoría un proceso que igualmente requiere de la mejora continua, es conveniente alinear ambos ciclos en un proceso interrelacionado.

Figura 42. El doble ciclo de mejora continua



El formalismo asociado al proceso auditor está en manos de la norma de auditoría de sistemas de gestión ISO 19011:2011 al considerar que el proceso de gestión de cumplimiento se ubica dentro de los de gestión. La auditoría deberá atender la verificación de requisitos frente a registros y el sistema de gestión del riesgo.

10.1.3. Equivalencia metodológica. La presente metodología reúne mejores prácticas de la industria, especialmente TI, y en especial las normas técnicas, metodologías y marcos normativos expuestos en este documento. Para entender la relación entre las cláusulas de la norma y reforzar la aplicación de la misma por parte del usuario de esta metodología, se suministra un paralelo entre las cláusulas de la norma y las normas que se relacionan directamente. Este paralelo le podrá servir al usuario de la norma para que profundice y aproveche los aspectos metodológicos específicos de la norma relacionada.

Tabla 18. Comparación de la metodología propuesta con normas técnicas

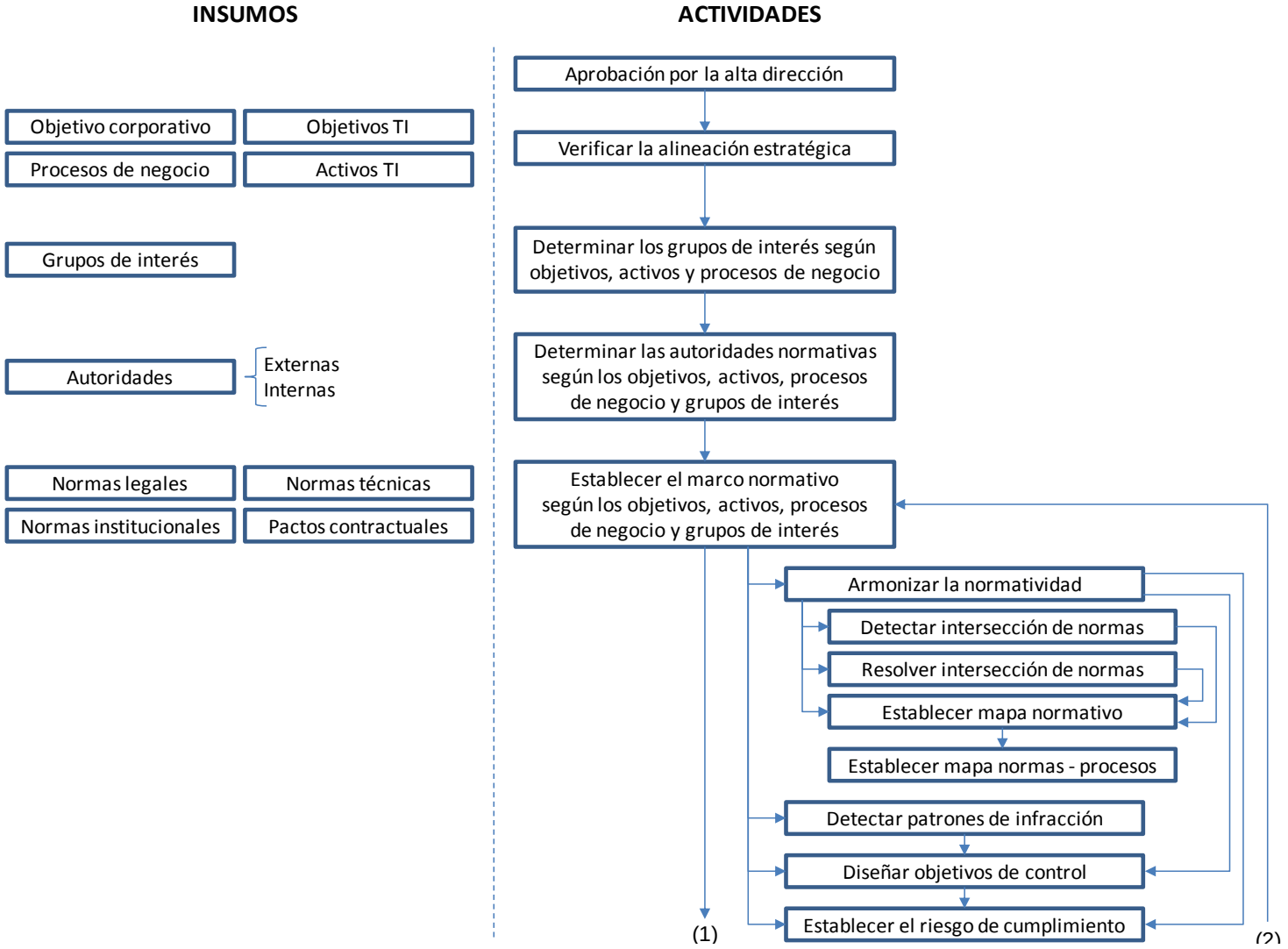
METODOLOGIA PROPUESTA	NORMAS RELACIONADAS
Planeación	
Aprobación por la alta dirección	COSO II
Verificar la alineación estratégica	COSO II
Objetivo corporativo	COSO II, COBIT
Objetivos TI	COSO II, COBIT
Procesos de negocio	COMPAS, CMMI
Activos TI	ISO 27001, ISO 31000,OCTAVE, MECI
Determinar los grupos de interés	ASNZ 4360:2004, ISO 31000, ISO 27001, COBIT

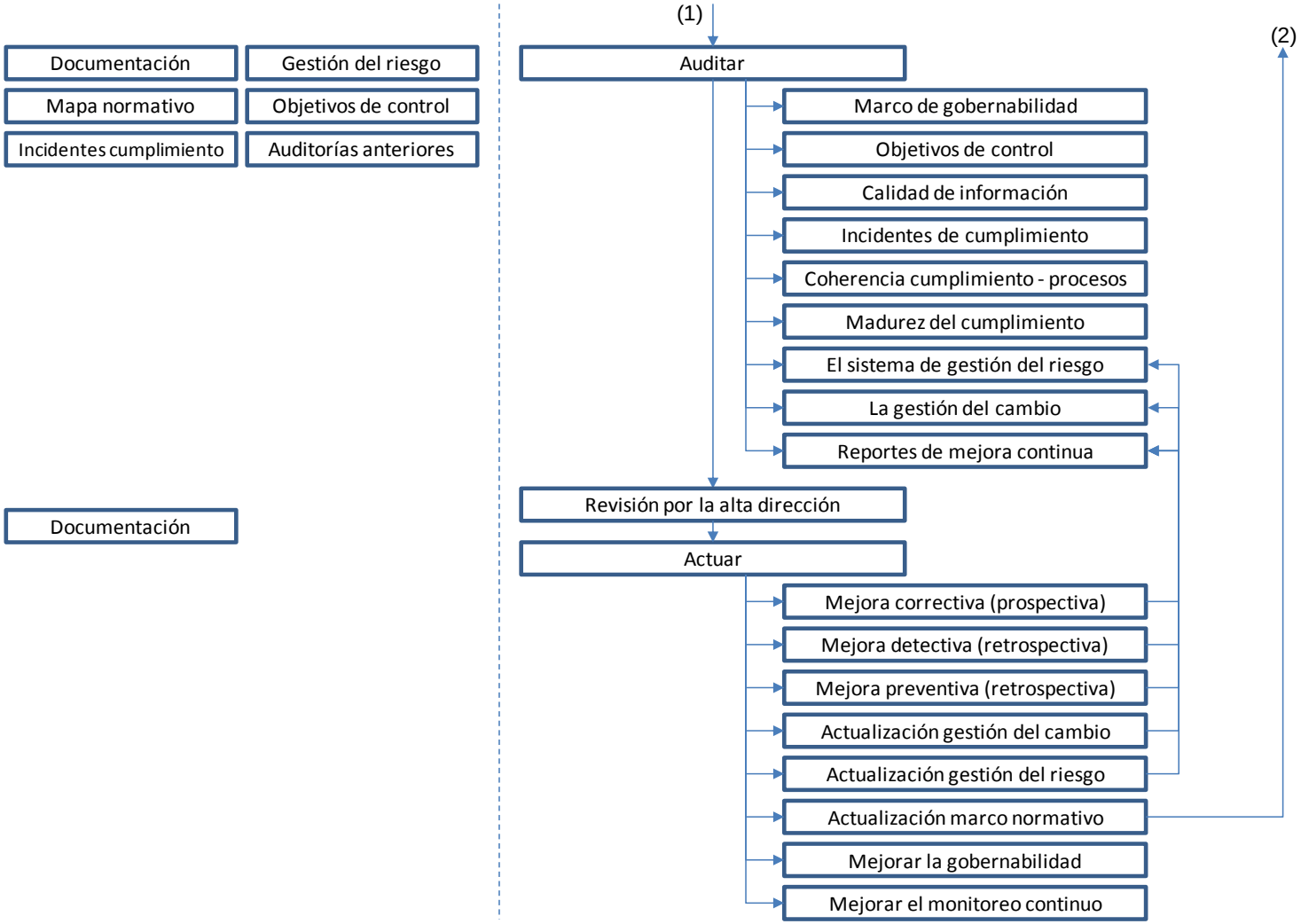
Determinar las autoridades normativas		COMPAS
Establecer el marco normativo		COBIT
	Armonizar la normatividad	ISO 27001, COBIT, COMPAS
	Detectar intersección de normas	-
	Resolver intersección de normas	-
	Establecer mapa normativo	ISO 27001, COMPAS
	Establecer mapa normas - procesos	ISO 27001, COMPAS, CMMI
	Detectar patrones de infracción	COSO II, OCTAVE
	Diseñar objetivos de control	COSO II, COBIT
	Establecer el riesgo de cumplimiento	COMPAS
Hacer		
Auditar		MECI, ISO 19011, AUDITE
	Marco de gobernabilidad	COBIT
	Objetivos de control	COSO II, COBIT
	Calidad de información	COBIT, AIMQ, DQMIM, ISO 15939
	Incidentes de cumplimiento	COSO II
	Coherencia cumplimiento - procesos	COMPAS
	Madurez del cumplimiento	CMMI SPICE - ISO 15504
	El sistema de gestión del riesgo	COSO II, MECI, ISO 27001, ISO 31000, COMPAS
	La gestión del cambio	CMMI
	Reportes de mejora continua	COMPAS, CMMI
Revisión		COSO
Accion		

Acciones de mejora		COMPAS
	Mejora correctiva (prospectiva)	ISO 9001, ISO 31000
	Mejora detectiva (retrospectiva)	COMPAS
	Mejora preventiva (retrospectiva)	ISO 9001, ISO 31000
Actualizacion		-
	Actualización gestión del cambio	CMMI
	Actualización sistema de gestión del riesgo	ISO 27001, ISO 31000, COSO II, MECI, COMPAS
	Actualización marco normativo	COBIT, COMPAS
Reforzar		CMMI
	Monitoreo continuo	COSO II, COBIT
	Gobernabilidad	COBIT

Aplicando el ciclo de mejora continua, y los componentes planteados en la estructura anterior, se tiene el siguiente flujo-grama de la metodología, del cual se desprende la formulación textual de la misma con los deberes por parte del usuario (implementador o auditor) de la metodología.

Figura 43. Metodología propuesta




INSUMOS
ACTIVIDADES
(1)
(2)
Documentación
Gestión del riesgo
Mapa normativo
Objetivos de control
Incidentes cumplimiento
Auditorías anteriores
Auditar
Marco de gobernabilidad
Objetivos de control
Calidad de información
Incidentes de cumplimiento
Coherencia cumplimiento - procesos
Madurez del cumplimiento
El sistema de gestión del riesgo
La gestión del cambio
Reportes de mejora continua
Revisión por la alta dirección
Documentación
Actuar
Mejora correctiva (prospectiva)
Mejora detectiva (retrospectiva)
Mejora preventiva (retrospectiva)
Actualización gestión del cambio
Actualización gestión del riesgo
Actualización marco normativo
Mejorar la gobernabilidad
Mejorar el monitoreo continuo

10.2. METODOLOGIA COMO NORMA TÉCNICA

El esquema metodológico expuesto en la anterior gráfica, se desarrolla específicamente como norma técnica compuesta por cláusulas auditables y verificables.

0. INTRODUCCION

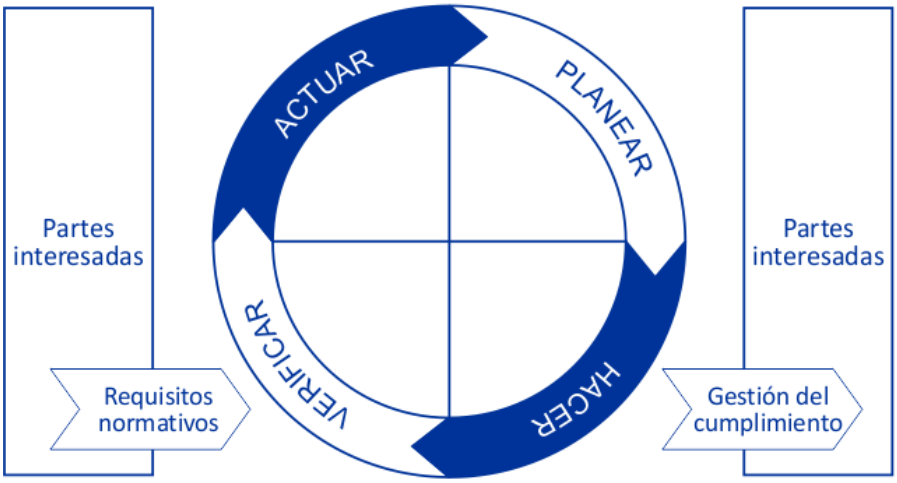
0.1. **General**.

a. Esta metodología ha sido establecida para proveer un marco metodológico para la evaluación del cumplimiento y el riesgo asociado a la gestión de la información.
b. La adopción de una metodología técnica para la evaluación del cumplimiento es una decisión estratégica para la organización.
c. La evaluación del cumplimiento está influenciada por los objetivos, necesidades, políticas, requisitos, procesos y en general el contexto social y legal en el cual se desempeña la organización, factores que se esperan cambien con el tiempo.

0.2. **Enfoque basado en procesos**.

a. La evaluación del cumplimiento se entenderá a lo largo de este documento como el sistema de evaluación del cumplimiento, el cual es transversal a la organización y sus procesos de negocio.
b. El sistema de evaluación del cumplimiento requiere del monitoreo continuo basado en mediciones objetivas para proporcionar seguridad razonable frente a requisitos normativos aplicables a una organización en un marco de mejora continua.
c. Esta metodología adopta un enfoque basado en procesos bajo el modelo PHVA (Planear, Hacer, Verificar, Actuar)

Figura 44. Ciclo de mejora continua de la norma técnica propuesta



1. ALCANCE

1.1. **General**.

a. La presente metodología está orientada a la evaluación del cumplimiento asociado a las Tecnologías de la Información y Comunicaciones (TI) en organizaciones del sector público.

b. Esta metodología establece los pasos recomendados para realizar la evaluación del cumplimiento en el contexto de la organización y sus riesgos.

1.2. **Definiciones**. En su orden, se entenderá como vocabulario común aceptado para esta metodología lo establecido en la guía ISO Guide 73, ISO 31000:2009, ISO 27001:2005, ISO 9000:2005, CMMI, COBIT 5, OCTAVE.

2. EL SISTEMA DE EVALUACIÓN DEL CUMPLIMIENTO

2.1. Establecer el sistema de evaluación del cumplimiento. La organización deberá:

a. Definir el alcance y límites del sistema de evaluación del cumplimiento en términos de objetivos del negocio, los procesos de negocio y el contexto

socio-económico y normativo en los ámbitos jurídico y técnico para los procesos de TI.

b. Revisar la política de cumplimiento organizacional.
c. Analizar los objetivos de cumplimiento de la organización frente a los objetivos corporativos y los de TI, los cuales deben estar previamente alineados.
d. Identificar los procesos de negocio que consuman, procesen, produzca, soporten o gestionen información de forma independiente al soporte documental.
e. Identificar los activos de TI que participan en los procesos de negocio.
f. Identificar los grupos de interés frente a la organización en términos de objetivos del negocio, los procesos de negocio, activos de TI y el contexto socio-económico y normativo en los ámbitos jurídico y técnico para los procesos de TI.
g. Establecer el marco normativo en términos jurídicos, técnicos o contractuales.
    1. Identificar las autoridades normativas con competencia o jurisdicción sobre la organización, sus procesos, productos y/o servicios, en términos de TI.
    2. Identificar las normas emitidas por las autoridades normativas identificadas y que sean aplicables o exigibles a la organización.
    3. Detectar y resolver la intersección de normas, esto es, cuando cláusulas de dos o más normas tratan el mismo aspecto.
    4. Identificar las relaciones entre normas y procesos de negocio, de forma que se pueda conocer quien, qué, dónde y cómo se atiende un requisito normativo.
h. Definir el sistema de gestión del riesgo de la organización en términos de TI
    1. Identificar una metodología de evaluación del riesgo aplicable al sistema de evaluación del cumplimiento frente a los procesos de negocio, activos de TI y el contexto socioeconómico y normativo para procesos de TI.

2. Revisar el criterio institucional para la aceptación de riesgo de no cumplimiento.
3. Analizar los aspectos normativos, así como el cambio normativo y el contexto como potenciales amenazas.
4. Identificar las vulnerabilidades que impidan o favorezcan el no cumplimiento.
5. Revisar la eficacia y eficiencia de los controles existentes en desarrollo de los objetivos de control.
6. Evaluar la eficacia y eficiencia del tratamiento del riesgo.

i. Analizar los objetivos de control en términos de gestión de cumplimiento en TI.
j. Formular el plan de puesta en marcha del sistema de evaluación del cumplimiento.
k. Obtener aprobación para operar el sistema de evaluación de cumplimiento.

2.2. Implementar el sistema de evaluación del cumplimiento. La organización deberá:

a. Implementar el plan de evaluación del cumplimiento.
b. Gestionar la disponibilidad de recursos para la evaluación del cumplimiento.
c. Realizar revisiones independientes y objetivas mediante auditoría sobre:
    1. Los procesos y controles establecidos para el aseguramiento del cumplimiento.
    2. Los procesos y controles adoptados para la detección temprana de cambios en el contexto normativo.
    3. El registro de incidentes de cumplimiento por detección de situaciones de no cumplimiento o eventos de acciones de control.
    4. El sistema de gestión del riesgo.
    5. Los objetivos de control y de sus controles, incluyendo su definición, operación, control, efectividad y mejora continua.
    6. Madurez del cumplimiento.
    7. Calidad de la información.

2.3. Revisar el sistema de evaluación del cumplimiento. La alta dirección deberá:

a. Revisar los informes de revisión independiente y objetiva, incluyendo la auditoría, discutir los hallazgos y explicar o soportar, para fijar el informe final aceptado.
b. Revisar el registro de patrones de infracción normativa que permita facilitar la detección de posibles situaciones de no cumplimiento.
c. Revisar el registro de incidentes de cumplimiento, por circulares informativas, detección de situaciones de no cumplimiento o eventos de acciones de control.

2.4. Mejorar el sistema de evaluación del cumplimiento. La organización deberá:

a. Diseñar acciones de mejora con su respectivo cronograma de implementación.
    1. Mejora correctiva, orientada a atender incidentes de cumplimiento.
    2. Mejora detectiva, enfocada a detectar situaciones de no cumplimiento por cambios en el contexto normativo.
    3. Mejora preventiva, para prevenir la ocurrencia de eventos de no cumplimiento.
b. Gestionar la disponibilidad de recursos para la implementación de tales acciones.
c. Implementar, controlar y evaluar las acciones de mejora formuladas.
d. Comunicar las acciones y mejoras realizadas y la madurez del cumplimiento en TI en la organización al nivel directivo.
e. Mantener actualizados:
    1. Los procesos y controles dedicados a la gestión del cambio.
    2. Los controles que dentro de los procesos de negocio aseguran el cumplimiento.
    3. El sistema de gestión del riesgo.
    4. El marco normativo.

f. Reforzar mediante la asignación de recursos y la aplicación de procesos:
    1. El monitoreo continuo.
    2. La gobernabilidad orientada a TI.
g. Evaluar el proceso de evaluación del cumplimiento.

3. REQUISITOS DOCUMENTALES

3.1. **General**. El sistema de evaluación del cumplimiento debe incluir:

a. Definición de alcance y límites del sistema evaluación del cumplimiento.
b. El marco normativo en términos jurídicos, técnicos o contractuales.
c. El plan de puesta en marcha del sistema de evaluación del cumplimiento.
d. La aprobación para operar el sistema de evaluación de cumplimiento.
e. Los resultados de la revisión independiente y objetiva mediante auditoría del punto 2.2.c
f. Los resultados de la revisión independiente y objetiva sobre monitoreo.
g. La revisión por parte de la alta dirección.
h. El documento de diseño de acciones de mejora con su respectivo cronograma de implementación.
i. El resultado de la implementación, control y evaluación de acciones de mejora.
j. Evidencias de las comunicaciones en virtud del cumplimiento.
k. La asignación de recursos para realizar la evaluación del cumplimiento.
l. La asignación de recursos para la implementación de las acciones de mejora.
m. La evaluación del proceso de evaluación del cumplimiento.
n. Los registros de los numerales 2.1.b, 2.1.c, 2.1.d, 2.1.e, 2.1.f, 2.1.h.2, 2.1.h.6, 2.1.h.7, 2.1.h.8, 2.1.i, 2.1.k.

3.2. **Control de documentos**.

a. Los documentos que integran el sistema de evaluación del cumplimiento deben estar protegidos y controlados.

b. Los documentos deben estar aprobados antes de su uso.
c. Asegurarse que solo se usen documentos autorizados y actualizados.
d. Los documentos deben permanecer legibles y fáciles de usar.

3.3. **Control de registros**.

a. Los registros que se producen o hacen parte del sistema de evaluación del cumplimiento deben permanecer protegidos y controlados.
b. Los registros deben permanecer legibles y fáciles de usar.

4. LA ALTA DIRECCION

4.1. **Compromiso de la alta dirección**. La alta dirección debe proveer evidencia de su compromiso con el cumplimiento en la organización mediante:

a. La definición de una política de cumplimiento organizacional
b. La definición de objetivos de cumplimiento de la organización frente a los objetivos corporativos y los de TI, los cuales deben estar previamente alineados
c. La definición, documentación, implementación y control de procesos de negocio que consuman, procesen, produzca, soporten o gestionen información de forma independiente al soporte documental
d. El inventario de activos de TI que participan en los procesos de negocio
e. La definición y mantenimiento del marco normativo en términos jurídicos, técnicos o contractuales
f. La creación, puesta en marcha y revisión periódica del sistema de gestión del riesgo en términos de TI y los aspectos relacionados con el cumplimiento
g. La definición e implementación de objetivos de control en términos de gestión de cumplimiento en TI
h. La aprobación para operar el sistema de evaluación de cumplimiento

i. La revisión de los informes de revisión independiente y objetiva
j. La revisión del registro de patrones de infracción normativa
k. La revisión del registro de incidentes de cumplimiento
l. El diseño de acciones de mejora con su cronograma de implementación
m. La comunicación de las acciones y mejoras realizadas y la madurez del cumplimiento en TI en la organización

4.2. **Gestión de recursos**. La alta dirección debe:

a. Gestionar la disponibilidad de recursos para la evaluación del cumplimiento
b. Gestionar la disponibilidad de recursos para la implementación de las acciones de mejora.

5. LA MEJORA CONTINUA

La organización debe mejorar de manera continua su gestión del cumplimiento en términos de T y realizar de forma continua evaluaciones periódicas e independientes de su cumplimiento.

Para este fin deberá dictar acciones correctivas, preventivas y detectivas en respuesta a la revisión que realice la alta dirección conforme a la cláusula 2.4.a de esta norma.

11. PRUEBA PILOTO

11.1. SELECCIÓN DE LA ENTIDAD

Para la prueba piloto de la metodología se escogió al Departamento de Santander, sobre el cual, dado su tamaño y complejidad, el análisis se realizará en una de sus funciones informáticas denominada el Sistema Maestro de Información.

Alcance:	Sistema maestro de información
	Componente GEOPORTAL
Límites:	Sistema de información SMI - GEOPORTAL
Fecha:	Diciembre 12 al 14 de 2011
Auditor:	Ing. Juan Carlos Angarita C.
Perfil auditor:	Especialista en auditoría de sistemas
	Especialista en Sistemas de Información Geográfica
	Especialista en Desarrollo de Software para Dispositivos Móviles
	Candidato a magíster en ingeniería de sistemas e informática
	Auditor líder certificado IRCA en ISO 27001:2005 (SGS)

11.2. RELACION NORMATIVA

El anexo A muestra la relación de normas y las cláusulas específicas que exhiben relación con el sistema auditado, al cual se le aplica la metodología de estudio. Las normas que se relacionan y que se usaron para este estudio son de índole nacional a nivel de actos legislativo de primer nivel (leyes).

11.3. DESARROLLO METODOLÓGICO

Para facilitar el entendimiento del desarrollo de la metodología propuesta, se presenta un paralelo entre cada una de las cláusulas y la forma como fue llevado a cabo en la entidad objeto de análisis.

Tabla 19. Desarrollo metodológico

CLÁUSULA DE LA NORMA	RESUMEN DEL DESARROLLO
2.1. Establecer el sistema de evaluación del cumplimiento. La organización deberá: a. Definir el alcance y límites del sistema de evaluación del cumplimiento en términos de objetivos del negocio, los procesos de negocio y el contexto socio-económico y normativo en los ámbitos jurídico y técnico para los procesos de TI.	Entidad: Departamento de Santander Área: Secretaría de Planeación Contexto: Entidad pública territorial de orden departamental. Le son aplicables las normas jurídicas técnicas diseñadas para el sector público colombiano. Alcance: Sistema maestro de información Componente GEOPORTAL Límites: Sistema de información SMI GEOPORTAL
b. Revisar la política de cumplimiento organizacional.	No se identificó la presencia de una política formalmente establecida al respecto.
c. Analizar los objetivos de cumplimiento de la organización frente a los objetivos corporativos y los de TI, los cuales deben estar previamente alineados.	No se identificaron objetivos corporativos. Sin embargo existe el plan de desarrollo departamental que cuenta con programas (que se comportan como objetivos) y metas al respecto. No se evidenció existencia de objetivos del área de TI formalmente establecidos. No se evidenció existencia de objetivos de cumplimiento general o en TI.

d. Identificar los procesos de negocio que consuman, procesen, produzca, soporten o gestionen información de forma independiente al soporte documental.	Procesos de negocio
e. Identificar los activos de TI que participan en los procesos de negocio.	Hardware: Servidor HP ML150G5 Software: Motor SIG (ESRI) MS SQL Server 2008 Datos: Cartografía base
f. Identificar los grupos de interés frente a la organización en términos de objetivos del negocio, los procesos de negocio, activos de TI y el contexto socio-económico y normativo en los ámbitos jurídico y técnico para los procesos de TI.	Ciudadanos colombianos Habitantes del Departamento de Santander. Organismos de control. Servidores públicos del Departamento de Santander. Contratistas y proveedores, Departamento de Santander.
g. Establecer el marco normativo en términos jurídicos, técnicos o contractuales. 1. Identificar las autoridades normativas con competencia o jurisdicción sobre la organización, sus procesos, productos y/o servicios, en términos de TI.	Congreso de la república Presidencia de la república Archivo general de la nación Departamento Administrativo de la Función Pública Departamento de Planeación Nacional Dirección Nacional de Derechos de Autor Ministerio de Telecomunicaciones y Tecnologías de la información Asamblea Departamental Organismos de control - Contraloría - Procuraduría
2. Identificar las normas emitidas por las autoridades normativas identificadas y que sean aplicables o exigibles a la organización.	Ver anexo A

h. Definir el sistema de gestión del riesgo de la organización en términos de TI 1. Identificar la metodología de evaluación del riesgo aplicable al sistema de evaluación del cumplimiento frente a los procesos de negocio, activos de TI y el contexto económico y normativo para procesos de TI.	Para los propósitos del análisis propuesto se aplicó la metodología planteada por la norma NTC5254, considerando que la entidad tiene un sistema de gestión básico del riesgo con base en esta norma.
2. Revisar el criterio institucional para la aceptación de riesgo de no cumplimiento.	Si bien el ente tiene un sistema de gestión del riesgo, no ha definido criterios para la aceptación del riesgo de no cumplimiento.
3. Analizar los aspectos normativos y el contexto como elementos potenciales de amenazas.	El sistema auditado tiene como función recopilar información estadística y estudios de varios aspectos del Departamento. Estos aspectos funcionales implican la publicación de datos que podrían estar bajo jurisdicción de las normas pertinentes al habeas data o de derechos de autor, sin descartar los aspectos propios de la gestión documental con los respectivos deberes en materia disciplinaria. Al ser un sistema que divulga información, le aplica la norma de gobierno en línea y lo referente a mensajes de datos electrónicos Dichas normas (Anexo A) sufren de forma continua cambios en el ámbito colombiano, tal como sucedió con la derechos de autor a la cual el año pasado se le hicieron cambios en su cuerpo normativo. Las entidades públicas suelen estar atentas al cambio pero su respuesta es lenta y reactiva (posteriori) a la situación.

4. Identificar las vulnerabilidades que impidan o favorezcan el no cumplimiento.	No hay vigilancia normativa (cambios en el entorno normativo) que permitan anticipar sucesos. Lenta respuesta al cambio. No incorporación de aspectos normativos (legales y técnicos) a los procesos de contratación, especialmente adquisición de elementos de TI Falta de entrenamiento en aspectos legales y técnico a los servidores que realizan la función de interventoría o supervisión en contratos.
5. Revisar la eficacia y eficiencia de los controles existentes en desarrollo de los objetivos de control.	No se evidencian controles formales. Los controles existentes son de índole personal realizados por los asesores jurídicos al momento de celebrar o liquidar contratos.
6. Evaluar la eficacia y eficiencia del tratamiento del riesgo.	Si bien la entidad cuenta con un sistema de gestión del riesgo, el riesgo asociado al no cumplimiento no tiene tratamiento.
i. Analizar los objetivos de control en términos de gestión de cumplimiento en TI.	Si bien la entidad cuenta con un sistema de gestión del riesgo, el riesgo asociado al no cumplimiento no tiene objetivos de control asociados al cumplimiento
k. Obtener aprobación para operar el sistema de evaluación de cumplimiento.	Se obtuvo aprobación por parte del grupo interventor del proyecto Geoportal. No se solicitó aprobación oficial dado que no existe contrato o convenio que soporte tal actividad de manera formal.
2.2. Implementar el sistema de evaluación del cumplimiento. La organización deberá: a. Implementar el plan de evaluación del cumplimiento.	El plan se implemento de manera informal dado que es un asunto académico y no existe contrato o convenio que soporte tal actividad de manera formal.

b. Gestionar la disponibilidad de recursos para la evaluación del cumplimiento.	Dado que la prueba piloto es académica, no se solicitaron recursos diferentes al auditor.
c. Realizar revisiones independientes y objetivas mediante auditoría sobre: 1. La coherencia entre los procesos de negocio y el mapa normativo.	Dado que la entidad cuenta con procesos documentados en el marco de un sistema de gestión de la calidad, existe coherencia entre procesos y requisitos. Sin embargo, no se proponen mecanismos de control y aseguramiento del cumplimiento.
2. Los procesos y controles establecidos para el aseguramiento del cumplimiento.	Los procesos no cuentan con controles definidos para aseguramiento y evaluación del cumplimiento.
3. Los procesos y controles adoptados para la detección temprana de cambios en el contexto normativo.	La entidad no cuenta con procesos y/o controles para la detección temprana de cambios en el contexto normativo, salvo boletines de noticias que requieren la interacción manual de funcionarios.
5. El registro de incidentes de cumplimiento, por circulares informativas, detección de situaciones de no cumplimiento o eventos de acciones de control.	La entidad no mantiene un registro de incidentes relativos al cumplimiento. El registro más cercano, conceptualmente, reposa en la oficina jurídica en referencia a acciones de cumplimiento o solicitud / sanciones por organismos de control.
6. El sistema de gestión del riesgo.	Si bien la entidad cuenta con un sistema de gestión del riesgo, el riesgo asociado al no cumplimiento no tiene tratamiento. No se pudo verificar el funcionamiento del sistema de gestión del riesgo. No se conocieron registros al respecto.
7. Los objetivos de control y de sus controles, incluyendo su definición, operación, control, efectividad y mejora continua.	Si bien la entidad cuenta con un sistema de gestión del riesgo, no se conoce sobre objetivos de control orientados hacia la gestión adecuada del cumplimiento.

8. Madurez del cumplimiento.	Si bien la entidad cuenta con procesos documentados en el marco de un sistema de gestión de la calidad, éstos tienen una baja orientación hacia proyectos, y mucho menos reforzado hacia el cumplimiento. Por ende, se puede establecer que el nivel de madurez es inicial.
9. Calidad de la información.	Se hizo una revisión exhaustiva de datos aplicada a la cartografía base del sistema de información SMI GeoPortal encontrando que la ausencia de requisitos claros en la consecución, tratamiento, almacenamiento y consulta de información llevó a obtener mapas con algunos problemas de precisión, distorsión y problemas con los atributos espaciales y alfanuméricos.

12. REVISIÓN METODOLÓGICA

12.1. SOBRE EL PROCESO

En cuanto al proceso, surgen las siguientes inquietudes:

a. Si bien no hubo necesidad de afectar la norma metodológica diseñada, practicándole cambios, sí parece importante establecer algunos objetivos de control generales al mejor estimo de la norma ISO 27001. Esto facilitaría a las organizaciones y auditores pudieran implementar y auditar fácilmente la evaluación del cumplimiento.

b. Las organizaciones deben implementar el concepto del cumplimiento a nivel de sus objetivos de negocio al igual que en sus procesos de negocio. Generalmente estos aspectos son tratados de forma general, como una expresión de adhesión a la norma sin que medie un mecanismo efectivo al respecto.

c. Una vez una entidad pública adopta la metodología de evaluación del cumplimiento, el ciclo de mejora continua debe estar estructurado con los procesos directivos, de control interno incluyendo el de auditoría, así como de compras y adquisiciones.

   Esto con el ánimo de asignarle recursos a la función de evaluación del cumplimiento, la de dictar la necesaria alineación institucional frente al cumplimiento de manera explícita, la de incorporar los aspectos normativos en los procesos contractuales así como el de mantener una continua evaluación para crecer al respecto.

d. La metodología de evaluación del cumplimiento puede proveer elementos importantes para desarrollar la obligatoriedad emanada de las autoridades legales y técnicas así como lo requerido en diversas normas técnicas. Un esfuerzo adicional interesante por parte de investigadores en el futuro sería el estudiar el caso de modelos específicos para los diversos aspectos de gestión de la información.

12.2. SOBRE LOS RESULTADOS

Sobre los resultados es importante resaltar:

e. Tal como se esperaba, si bien las entidades públicas y sus funcionarios si tienen conciencia sobre el concepto de obligatoriedad, muchas veces reforzado por actos de los entes de control, no existe un formalismo a nivel directivo y de procesos de negocio que permitan asumir un compromiso frente a la normatividad vigente y aplicable y controlar sus procesos como ejecutantes de dichas obligatoriedades.

f. La existencia de sistemas de gestión, llámese de calidad, gestión del riesgo y/o de control interno, igualmente obligatorios, y quienes en los cuerpos de sus normas está la exigencia de dar cumplimiento al marco normativo legal y técnico exigido a la organización, no necesariamente implica el aseguramiento del cumplimiento. En parte esto surge de la misma complejidad de normas legales y técnicas al igual que de la ausencia de mecanismos adecuados para establecer un marco normativo.

g. Los sistemas de gestión del riesgo no siempre consideran al riesgo inherente al no cumplimiento y mucho menos se le califica en cuanto a probabilidad o impacto, para darle el cumplimiento respectivo.

h. Es importante que los servidores públicos estén capacitados en aspectos relativos al cumplimiento, especialmente al momento de formular acciones de adquisición (bien sea desarrolladas por la entidad o con terceros) de forma que se tengan en cuenta lo referente al marco normativo.

i. La gestión del cambio, en el contexto normativo, es un proceso de necesario uso y adopción, por cuanto es el que se encarga de detectar y prevenir vulnerabilidades derivadas de nueva o modificadas normas que afectan la organización.

j. La no realización de la tarea de gestión, control y evaluación del cumplimiento, de manera formal, pueden llevar a que la entidad incurra en un posible daño fiscal, al no prevenir de forma adecuada sus adquisiciones y entregas de productos y servicios.

k. Es necesario reforzar el sistema de gestión del riesgo con objetivos de control y los respectivos controles, debidamente controlados y periódicamente auditados.

l. No se encontró una persona formalmente delegada “a cargo” del cumplimiento, que comúnmente se conoce como oficial de cumplimiento.

Estas conclusiones son las que comúnmente serían llevadas a un comité de revisión por parte de la alta gerencia, del cual surgen las acciones de mejora respectivas.

CONCLUSIONES

1. Existe una gran diversidad de normas de origen legal o técnico que rigen sobre la materia informática en sus diversos aspectos.

2. La intersección entre normas puede derivar en inconsistencias en cláusulas que estén desarrollando el mismo aspecto. Tal situación puede impedir alcanzar conformidad de manera simultánea con dos normas que traten el mismo aspecto.

3. La calidad de la información es mencionada a menudo en las normas que versan sobre información en sus diversas facetas, estableciendo un marco de cumplimiento al respecto. Por lo tanto, es necesario considerar el adoptar la calificación cualitativa de la calidad de la información para poder medir la mejora continua al respecto.

4. Existen diversas normas técnicas que bajo diversos enfoques aportan criterios para la evaluación del cumplimiento, algunos de ellos en una intersección conceptual.

5. La metodología propuesta incorpora un ciclo PHVA orientándola hacia un sistema de gestión para la evaluación del cumplimiento, siguiendo la estructura de seguridad de la información o del riesgo.

6. La metodología propuesta igualmente presenta en sus cláusulas la concurrencia de múltiples normas técnicas a partir de sus diversos aportes técnicos a la evaluación del cumplimiento.

7. La metodología propuesta fue aplicada en una organización pública donde se

pudo evidenciar que si bien se tiene conciencia sobre la obligatoriedad normativa en temas relacionados con tecnologías de la información, igualmente es cierto que no existe un direccionamiento estratégico organizacional para evaluar y controlar el cumplimiento.

8. Es común que las normas técnicas señalen la necesidad de dar cumplimiento total a las obligaciones de índole legal o técnica aplicables a la entidad. Sin embargo, al momento de implementar dichas normas o auditar su operación es difícil establecer el marco normativo para un adecuado ejercicio del sistema de gestión.

9. Es importante que las organizaciones del sector público cuenten con directrices y políticas orientadas al cumplimiento que les permitan reducir su vulnerabilidad legal y técnica frente al complejo entorno de obligatoriedad.

RECOMENDACIONES Y TRABAJOS POSTERIORES

1. Ampliar la metodología propuesta de evaluación de cumplimiento en Tecnologías de la Información y las Comunicaciones hacia una orientada a la gestión integral del cumplimiento en la misma área.

2. Profundizar el análisis de actos legislativos hacia los actos regulatorios e informativos que desarrolla el sector público.

3. Considerar el análisis de normas técnicas específicas en los diversos aspectos que hacen parte de las Tecnologías de la Información y las Comunicaciones.

4. Consolidar el presente estudio en un modelo académico a nivel universitario y con alcance nacional de forma que la institución pueda ejercer como autoridad normativa.

5. Investigar metodologías complementarias que permitan tratar el problema de la intersección y colisión de estándares y normas técnicas, especialmente ahora que el país enfrenta la globalización en tratados de libre comercio, como el de Estados Unidos, donde existe su propio conjunto de normas legales y técnicas.

6. Ampliar el modelo propuesto de evaluación de calidad de la información, reforzando su carácter cuantitativo y alineándolo con las normas técnicas aplicables.

7. Plantear la posibilidad de la cátedra de gestión del cumplimiento en Tecnologías de la Información y las Comunicaciones en la escuela de ingeniería de sistemas de forma que los próximos profesionales tengan en

cuenta en sus ejercicios de desarrollo de soluciones tecnológicas, bien sea a nivel de software, hardware o comunicaciones, lo referente al marco normativo legal y técnico aplicable.

BIBLIOGRAFIA

Acuerdo 027 de 2006 expedido por el Archivo General de la Nación (Colombia)

ALDEGANI, Gustavo. Seguridad Informática VIII. Buenos Aires: MP Ediciones. 1997.

AL-HAKIM L.. Information Quality Deployment, Proceeding of Ninth International Conference on Information Quality, p.170-182. 2004 – Internet: http://www.iqconference.org/Documents/IQ%20Conference%202004/Papers/IQFunctionDeployment.pdf

American Standard Code for Information Interchange o ANSI_X3.4-1968

ANGARITA CASTELLANOS, Juan Carlos. Diplomado de Gestión Documental. Solutions. Bucaramanga, 2007

ANGARITA CASTELLANOS, Juan Carlos. Information Quality Assessment for Compliance and Governance. UIS. 5 International Conference on theory & practice of electronic governance. Tallin, Estonia. ACM Press 2011

ANTONIOU, G., BILLINGTON. ON MODELING AND ANALYSIS OF REGULATIONS. Proceedings of the Australian Conference Information Systems, pag 20-29, Sidney, 1999

ARISTOTLE.. Retorica. Gredos. 1997

AUTOREGULADOR DEL MERCADO DE VALORES COLOMBIANO. Guía de control interno en la intermediación del mercado de valores. Bogotá. 2008

AZ/NZS 4360

BAILEY, J.E., PEARSON, S.W., Development of a tool for measuring and analyzing computer user satisfaction, Management Science 29 (5), 1983, pp. 530–545.

BALLOU, D.P., PAZER, H.L., Modeling data and process quality in multi-input, multi-output information systems, Management Science. 1985, pp. 150–162.

BALLOU, D.P., WANG, R.Y., PAZER, H., TAYI, G.K. Modeling information manufacturing systems to determine information product quality. Management Science. 1998, 462–484.

BERLO, D. K. (1996). El proceso de la comunicación. México, El Ateneo

BISWAS, Jit, NAUMANN, Felix, QIU, Qiang. Assessing the Completeness of Sensor Data. Institute for Infocomm Research (I2R), Singapore, Humboldt-Universit¨at zu Berlin, Germany.

BLANCO RESTREPO, Jose Vicente. La responsabilidad del Estado por la calidad de la información suministrada en las licitaciones públicas. Febrero de 2011. Internet: http://contratacionestatal.blogspot.com/2011/02/la-responsabilidad-del-estado-por-la.html

BOELLA, G., GOVERNATORI. A LOGICAL UNDERSTANDING OF LEGAL INTERPRETATION. IN PROCEEDINGS AAAI, 2010.

BOELLA, G., GOVERNATORI, y otros. LEX MINUS DIXIT QUAM VOLUIT, LEX MAGIS DIXIT QUAM VOLUIT: A FORMAL STUDY ON LEGAL COMPLIANCE AND INTERPRETATION. AI APPROACHES TO THE COMPLEXITY OF LEGAL SYSTEMS. LNAI. Springer. Berlin, 2010.

BOVENS, Luc, HATMANN, Stephan. Solving the riddle of coherence. Mind, Vol 112-448. Bovens and Hartmann. Octubre 2003

BREAUX, T., ANTON, A., SPAFFORD, E., “A distributed requirements management framework for legal compliance and accountability”, North Carolina State University Computer Science, Tech. Rep. 14, 2006.

BROWN, Duguid. La Vida Social de la Información, Harvard University Press, 2000

BSI. Product definitions. Londres: www.bsigroup.com/en/Standards-and-Publications/About-standards/Product-definitions/, 2010

CARNEGIE MELLON UNIVERSITY – SOFTWARE ENGINEERING INSTITUTE. CMMI for Acquisition 1.3, 2011.

CARNEGIE MELLON UNIVERSITY – SOFTWARE ENGINEERING INSTITUTE. CMMI Services 1.3 presentation, 2011.

CEDERQUIST, J., CORIN, R., y otros, Audit-based Compliance Control. En: International Journal of Information Security, 2007. Pag 133-151.

CERT. OCTAVE II METHOD. http://www.cert.org/octave/methodintro.html. 2001

CIGREF. Sécurité des systems d’information. Quelle politique globale de gestion des risques. Paris: www.cigref.com, 2002

Código de Procedimiento Civil (Colombia) Art. 251

CODINA, L. El libro digital y la WWW. Madrid: Tauro, 2000

COHEN, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.)

COOPER, W.S. 'On selecting a Measure of Retrieval Effectiveness'. Journal of the American Society for Information Science, v. 24, March-April 1973. p.87-92

CRONBACH, L., MEEHL, P. (1955). Construct validity in psychological tests, Psychological Bulletin, 52, 4, 281-302

CUÉLLAR, Guillermo Adolfo. Teoría General de la Auditoría y Revisoría Fiscal. Huila: Universidad del Cauca. 2003.

CYKANA, P., PAUL, A., STERN, M., DoD guidelines on data quality management, Proceedings of the Conference on Information Quality, Cambridge, 1996, pp. 154–171.

DARLINGTON, Angela, GROUT, Simon. HOW SAFE IS SAFE ENOUGH? The staple in actuarial society. 2001.

DE CASTRO Y BRAVO, F.: Derecho civil de España, t. I, Instituto de Estudios Políticos, Madrid, 1955.

DEKKER, M., HARTOG, J.. Audit-based Compliance Control (AC2) for EHR Systems. En: CTIT Technical Report. Enschede, NL: Universiteit Twente, 2007.

DELONE, W.H., MCLEAN, E.R., Information systems success: the quest for the dependent variable, Information systems research, 1992, pp. 60–95.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA, Manual de implementación del MECI, 2008.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Estructura del estado colombiano. Bogotá. 2006

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Modelo Estándar de Control Interno - MECI 1000:2005. Bogotá, 2005

Diccionario Robert

DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION – DCSSI. Typologie des normes et methods. Paris: DCSSI, 2002.

DUTTA, M. The impact of internet information completeness: The moderating role of Web use motivation. University of Minnesota. 2001

DUTTA-BERGMAN, M. health communication on the web: The role of web use motivation and informaton completeness Communication monographs, 70, 264-274. 2003

DUTTA-BERGMAN. Paper: The impact of completeness and web use motivation on the credibility of e-health information. International Communication Association. 2004. pp 253-269

El profesional de la información, v. 12, n. 4, julio-agosto 2003. Pag 305

ENGLISH L. Information Quality: Meeting Customer need, Information Impact Newsletter. 1996

ENIAC. – Internet: http://www.thocp.net/hardware/eniac.htm

ENISA. Agencia Europea Seguridad Informática. Heraklion: http://www.enisa.europa.eu/, 2010

e-SECURITE. Le choix des normes, outils et méthodes. París: http://www.e-securite.net , 2010

Estatuto general de contratación colombiano - Ley 80 de 1993. Art 25 numeral 3

EUROPEAN COMISSION. SEVENTH FRAMEWORK PROGRAM. COMPAS Project. Vienna: http://www.compas-ict.eu/, 2010

FEDERAL GEOGRAPHIC DATA COMMITTEE. Content Standard for Digital Geospatial Metadata. Federal Geographic Data Committee. Washington. 1998

Federal Standard 1037C (MIL-STD-188) http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm

FERNÁNDEZ, Pita, PÉRTEGA, S. Relación entre variables cuantitativas. Unidad de Epidemiología Clínica y Bioestadística. Complexo Hospitalario Universitario de Coruña (España). 1997; http://www.fisterra.com/mbe/investiga/var_cuantitativas/var_cuantitativas.asp

FERRER, Eulalio. Información y comunicación. México, Fondo de Cultura Económica. 1997

FIPS 140-2

FIPS 199

FIPS 200

FIRTMAN, Sebastian. Seguridad Informática, Manuales USERS: Las amenazas y vulnerabilidades más peligrosas al desnudo. Texas: M.P. Ediciones, 2005.

FRANTS , V.I. et al. Automated information retrieval : theory and methods. San Diego [etc.] : Academic Press, cop.1997. XIV, 365 p.

GALINDO, Jesús. Comunicación, ciencia e historia. Mcgraw hill. 2008

GARDYN, E., A Data Quality Handbook For A Data Warehouse, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 267–290.

GARTNER. Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms. Nueva York: Thomson Reuters, 2009

GARTNER. Use This Eight-Step Process for Identity and Access Management Audit and Compliance. Gartner Research. 2005

GHANAVATI, S., AMYOT, D., PEYTON, L., “A requirements management framework for privacy compliance,” in Proceedings of the Workshop on Requirements Engineering, 2007.

GHOSE, A., KOLIADIS, G., “Auditing business process compliance,” in Proceedings of the International Conference on Service-Oriented Computing, 2007
GOEDERTIER, S., VANTHIENEN, J., “Designing compliant business processes with obligations and permissions,” in Proceedings of the BPM 2006 Workshop, 2006

GOFFMAN, Erwin. The Presentation of Self in Everyday Life. New York, NY: Doubleday, 1959. 73

GOODHUE, D.L., Understanding user evaluations of information systems, Management Science 41, 1995, pp. 1827–1844.

GOVERNATORI, G. ROTOLO, A.. A CONCEPTUALLY RICH MODEL OF BUSINESS PROCESS COMPLIANCE. In Sebastian Link and Aditya Ghose, editors, 7th Asia-Pacific Conference on Conceptual Modelling (APCCM 2010), CRPIT. ACS, 2010

GOVERNATORI, G. ROTOLO, A.. AN ALGORITHM FOR BUSINESS PROCESS COMPLIANCE. Legal Knowledge and Information Systems (Jurix 2008), Frontieres in Artificial Intelligence and Applications 189, pages 186-191. IOS Press, 2008.

GOVERNATORI, G. ROTOLO, A.. LOGIC OF VIOLATIONS: A GENTZEN SYSTEM FOR REASONING WITH CONTRARY-TO-DUTY OBLIGATIONS. Australasian Journal of Logic 4: 193-215, 2006.

GRIFFIN, E. A., A first look at communication theory. 3rd edition, New York: McGraw-Hill, 1997

HARTLEY, Ralph. Transmission of Information. 1928

HERNANDEZ, Enrique. Auditoría en Informática. 2ª edición. Ciudad de México: Editorial Continental, 2000.

HILLIGOSS, B. & RIEH, S. Y.. Developing a unifying framework of credibility assessment: Concept, heuristics, and interaction in context. 44(4), 2008. 1467-1484.

HORTON, Forest W. "Information architectures: the information resources entity

(IRE) modeling approach". En: Aslib proceedings, 1989, nov-dic, v. 41, n. 11/12, pp. 313-318.

http://blogjus.wordpress.com/2007/04/01/conozcamos-nuestra-democracia/

http://derechoencolombia.net/index.php?title=Acto_legislativo_-definición-

http://etimologias.dechile.net

http://hermesoft.esap.edu.co/esap/hermesoft/portal/home_1/rec/arc_1623.pdf

http://personal.us.es/vararey/adatos2/correlacion.pdf

http://produccionmaslimpia-karenvictoria.blogspot.com/2009/08/diferencia-entre-ley-
decreto-resolucion.html

http://resolucionleyacuerdo.blogspot.com/2008/04/que-es-acuerdo.html
http://resolucionleyacuerdo.blogspot.com/2008/04/que-es-resolucin.html

http://web.mit.edu/tdqm/

http://www.bipm.org/en/publications/guides/gum.html

http://www.bipm.org/utils/en/pdf/JCGM_charter.pdf

http://www.cert.org/octave/ - Operationally Critical Threat, Asset Vulnerability Evaluation (OCTAVE)

http://www.dafp.gov.co/

http://www.dcc.uchile.cl/~rbaeza/inf/contexto.html

http://www.derechos.org/nizkor/ley/viena.html

http://www.enciclopedia-juridica.biz14.com/d/tratados/tratados.htm

http://www.eveliux.com/mx/historia-de-la-iso.php

http://www.icesi.edu.co/blogs_estudiantes/pmlefrenvalencia/2009/08/28/ley-norma-decreto-resolucion/

http://www.ilac.org/library_documents.html

http://www.isaca.org

http://www.iso.ch

http://www.iso.org/iso/catalogue_detail?csnumber=43170

http://www.iso15504.es/index.php/la-norma-iso-15504-spice.html

http://www.nist.gov/

http://www.productosdecolombia.com/main/guia/Acuerdos_Preferencias_Arancelarias.asp

http://www.sei.cmu.edu/cmmi/solutions/index.cfm

http://www.theiia.org/

http://www.unit.org.uy/proyecto_fomin-bid/index.php?O=4&S=1

http://www.wssn.net/WSSN/listings/links_regional.html

HUANG, K. ,LEE, Y., WANG, R. Quality Information and Knowledge. Prentice Hall, Upper Saddle River: N.J. 1999.

HURST, Cliff. Measurement, Reliability, and Validity: Part Four in the continuing series, Getting Quality Right. July/August 2008. http://www.connectionsmagazine.com/articles/8/061.html

ICONTEC. NTC 5254. Norma colombiana de gestión del riesgo. Bogotá: ICONTEC, 2004
IEEE-STD-610

Information Coherence Authority for Defence (ICAD) – Ministry of Defence – United Kingdom.
http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/ICAD/

Instituto Nacional de Tecnología Industrial. Argentina.

INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD – IAASB. Proyecto Clarity – Nuevas normas internacionales de auditoría. Nueva York: http://www.ifac.org/iaasb/ProjectHistory.php?ProjID=0024, 2010

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. Guide 73:2002, Risk managament Vocabulary. Ginebra: http://www.iso.org/, 2002

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 10196; ISO 12142; ISO 12037; ISO 18942, ISO 23081. Normas técnicas en gestión documental y archivística. Ginebra: http://www.iso.org/, 2010

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 14000. Norma de gestión ambiental. Ginebra: http://www.iso.org/, 2007

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 25999. Norma técnica en continuidad del negocio en gestión de información. Ginebra: http://www.iso.org/, 2008

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 2700x. Conjunto de normas en gestión de la seguridad de la información. Ginebra: http://www.iso.org/, 2007

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. ISO 31100:2009. Norma de gestión del riesgo. Ginebra: http://www.iso.org/, 2009

ISACA. IT Audit and Assurance Guidelines. Rolling Meadows, IL: http://www.isaca.org, 2009.
ISACA. IT Audit and Assurance Tools and Techniques. Rolling Meadows, IL: http://www.isaca.org, 2009.

ISO 1087-1: 2000 numeral 3.7.2

ISO 13335-1

ISO 15489-1:2001

ISO 19011:2011

ISO 19115

ISO 21748 Guidance for the Use of Repeatability, Reproducibility, and Trueness Estimates in Measurement Uncertainty Estimation. Geneva, Switzerland: ISO; 2004

ISO 3534-1:1993, Numeral 3.11

ISO 3534-2

ISO 5725-1:1994, Accuracy (trueness and precission) of measurement methods and results - part 1 - General principles and definitions. 1994

ISO 5725-1:1994, Accuracy (trueness and precission) of measurement methods and results - part 1 - General principles and definitions. 1994

ISO 8402

ISO Guide 51

ISO Guide 73

ISO Vocabulary of basic and general terms in metrology (1993)

ISO. International Vocabulary of Basic and General Terms in Metrology, 1993.

ISO. Introduccion a la normalización Geográfica: La familia ISO 19100

ISO/IEC 10646

ISO/IEC 13335-1:2004

ISO/IEC 15939:2007, Systems and software engineering - Measurement process.

ISO/IEC 17799, Jan 4, 2009

ISO/IEC 18019:2004 Software and system engineering - Guidelines for the design and preparation of user documentation for application software

ISO/IEC 2382-1:1993 Information technology--Vocabulary--Part 1: Fundamental terms.

ISO/IEC 25062:2006 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Common Industry Format (CIF) for usability test reports. 4.10

ISO/IEC 27001:2005

ISO/IEC 7498-2

ISO/IEC Guide 99-12:2007, International Vocabulary of Metrology — Basic and General Concepts and Associated Terms

ISO/IEC JTC1/SC7:12207

ISO/IEC TR 14143-3:2003 Information technology -- Software measurement

JARKE, M., VASSILIOU, Y., Data warehouse quality: a review of the DWQ project, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp.

299–313.

JCGM 200:2008. International vocabulary of metrology — Basic and general concepts and associated terms (VIM)

KORPAN, C. A., BISANZ, G. L., BISANZ, J. y HENDERSON, J. Assessing literacy in science: Evaluation of scientific news briefs. Science education, 81, 515-532. 1997

KOVAC, R., LEE, Y.W., PIPINO, L.L., Total Data Quality Management: the case of IRI, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 63–79.

LANHAM, Richard. Analyzing Prose' 2nd (2003): 7, 10

Ley 446 de 1998 (Colombia) Art. 11 sobre el principio de autenticidad

Ley 489 de 1998, art. 5

Ley 527 de 1999 (Colombia) sobre mensajes de datos electrónicos

Ley 594 de 2000, Ley General de Archivos (Colombia)

Ley 87 de 1993

Ley 872 de 2003

LITTLEJOHN, S. W.,Theories of human communication. 7th edition, Belmont, CA: Wadsworth, 2002

LIU, Y., MULLER, S., XU, K., “A static compliance-checking framework for business process models,” IBM Systems Journal, vol. 46, no. 2, pp. 335–362, 2007.

LÓPEZ YEPES, J. Teoría de la documentación. Pamplona: EUNSA, 1978

MAKHOUL, John; KUBALA, Francis; SCHWARTZ, Richard; WEISCHEDEL, Ralph: Performance measures for information extraction. In: Proceedings of DARPA Broadcast News Workshop, Herndon, VA, February 1999

MANDKE, V.V., NAYAR, M.K., Information integrity–a structure for its definition, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 314–338.
MANN, J. M.; GOUSKINS, S.; GRODIN, M. A.; ANNAS, G. J., eds. (1999). Health and Human Rights: A Reader. New York and London: Routledge.

MARTÍN VEGA, A. Fuentes de información general. Gijón: TREA. 1995.
Martínez Comenche

MATSUMURA, A, SHOURABOURA, N., Competing with Quality Information, Proceedings of the Conference on Information Quality, Cambridge, MA, 1996, pp. 72–86.

MATULEVIČIUS, Raimundas, KAMSEU, Flora, HABRA, Naji. Measuring Open Source Documentation Availability. PReCISE, Computer Science Faculty, University of Namur, Belgium. Pp7, 2010

MATULEVIČIUS, Raimundas, KAMSEU, Flora, HABRA, Naji. Measuring Open Source Documentation Availability. PReCISE, Computer Science Faculty, University of Namur, Belgium. Pp8, 2010

MEEKER, William Q., ESCOBAR, Luis A.. Statistical Methods for Reliability Data. Hoboken, New Jersey: Wiley, 1998. ISBN 0471143286

MELKAS, Helinä, UOTILA, Tuomo. Quality of data, information and knowledge in technology foresight processes. Lappeenranta University of Technology, Lahti Unit, Finland.

MEYEN, D.M., WILLSHIRE, M.J., A data quality engineering framework, Proceedings of the Conference on Information Quality, Cambridge, MA, 1997, pp. 95–116.

MILLER, K., Communication Theories: Perspectives, processes, and contexts. 2nd edition. New York: McGraw-Hill, 2005

http://grants.hhp.coe.uh.edu/doconnor/PEP6305/Topic%20012%20Validity.htm

http://www.montgomerycollege.edu/library/libtp/instructions/findingarticles/glossary.htm

MOTTOLA, R.M., SYTSMA, Sid. The Basics of Experimental Design - A Quick and Non-Technical Guide. 2009

NAMIRI, K., STOJANOVIC, N., “Towards a formal framework for business process compliance,” in Proceedings of the Multikonferenz Wirtschaftsinformatik, February 2008

NEGROPONTE, N. El mundo digital. Barcelona: Ediciones B., 1995

Norma ISO 9001:2008 numeral 0.2

Norma NTCGP 1000:2009, numeral 3.29

Norma UNE 50-113-92/1

NYQUIST, Harry. Certain Factors Affecting Telegraph Speed. 1924

O'CONNOR, Daniel P.. Measurement in Health & Physical Education – Validity. University of Houston.

OLIVAR ZÚÑIGA, Antonio (2006). Fundamentos teóricos de la comunicación

ONTOLOGY RESEARCH. 3rd International Workshop on Governance Risk and Compliance – Applications in Information Systems (GRCIS'10). Hammamet, Tunisia: http://ontology-research.com/2010/01/international-workshop-on-governance-risk-and-compliance-caise2010/, 2010

PACKER, Martin. Experimental and Statistical Research Methods. Duquesne University. 2004. http://www.mathcs.duq.edu/~packer/Courses/Psy624/test.html

PACmeter - Popularity, Authority, Credibility Online: How To Measure Them? http://www.masternewmedia.org/2004/08/11/pacmeter_popularity_authority_credibility.htm

PAGE, Stephen. Achieving 100% Compliance of Policies and Procedures. Los Angeles: Process Improvement Pub, 2007.

PIATTINI, Mario G.– EMILIO DEL PESO. Auditoria Informática Un Enfoque Practico. 2ª edición. México: Alfa y Omega, 2001

PIERCE, E., KAHN, B., MELKAS, H. "A comparison of quality issues for data, information, and knowledge", in Khosrow-Pour, M. (ed.), Emerging Trends and

Challenges in Information Technology Management: Proceedings of the 2006 Information Resources Management Association Conference. 17th IRMA International Conference, Washington, 2006, pp. 21–24.

PIPINO, Leo L., LEE, Yang W., WANG, Richard Y.. Data Quality Assessment.

RAHMAN, N.A, A Course in Theoretical Statistics; Charles Griffin and Company, 1968

Real Academia de la Lengua. www.rae.es

REDMAN, T.C., Data Quality: Management and Technology, Bantam Books, New York, NY, 1992

REDMAN, T.C., ed. Data Quality for the Information Age. Artech House: Boston, MA., 1996.

Research methods knowledge base. Convergent & Discriminant Validity. http://www.socialresearchmethods.net/kb/convdisc.php

Research methods knowledge base. http://www.socialresearchmethods.net/kb/measval.php

Research methods knowledge base. The Multitrait-Multimethod Matrix. http://www.socialresearchmethods.net/kb/mtmmmat.php

RIEH, S. Y. (2002) Judgment of information quality and cognitive authority in the web. Journal of the American Society for Information Science and Technology, 53, 145-161.

RiskIT

RODGERS, J. L., NICEWANDER, W. A.. Thirteen ways to look at the correlation coefficient. The American Statistician, 42(1):59–66, February 1988.

RODRÍGUEZ BRAVO, Blanca. REVISIÓN DE LAS CLASIFICACIONES DOCUMENTALES BASADAS EN EL SOPORTE. Área de Biblioteconomía y Documentación. Facultad de Filosofía y Letras. Universidad de León. correo-e: dphbrb@unileon.es. 17-1-2002.

ROTHMAN, K.J. et al. (2008) Modern epidemiology. Lippincott Williams & Wilkins pp.134-137.

RUŽEVIČIUS J., GEDMINAITĖ A.. peculiarities of the business information quality assessment. 2007

SADIQ, G., GOVERNATORI, NAIMIRI, K., “Modeling control objectives for business process compliance,” in Proceedings of the 5th International Conference on Business Process Management, September 2007,

SAGREDO FERNÁNDEZ, F. Documento y sistema virtual. En TRAMULLAS, J. (ed.), Tendencias de investigación en Documentación, Zaragoza: 1996, p. 9-17

SCHAMBER, L.. What is a document? Rethinking the concept in uneasy times. Journal of the American Society for Information Science, 1996, vol. 47, n. 9, p. 669-671

SCHRAMM, W.. How communication works. In W. Schramm (Ed.), The process and effects of mass communication. Urbana, IL: University of Illinois Press. 1954

SEI:SW-CMM

SELF, C. Credibility. An integrated approach to communication theory and research, Salves Eds, NJ, 1996

SENAR, J.C.. La Medición de la Repetibilidad y el Error de Medida. Museu de Zoologia, Ap. Correus Barcelona. 1999. http://www.bcn.es/museuciencies_fitxers/imatges/FitxerContingut1201.pdf

SHANKARANARAYAN G., ZIAD, M., WANG, R., Managing Data Quality in dinamyc decision environments. Journal of database management 14. 2003. 14-32

SHANNON, C.. WEAVER, W. The mathematical theory of communication. . Urbana, IL: University of Illinois Press. 1949

SILVERMAN, Michael. Compliance Management for Public, Private, or Non-Profit Organizations. Nueva York: McGraw Hill, 2008.
SP 800-53

STANDARDS AUSTRALIA LIMITED. ASNZ 4360:2004 - Gestión del riesgo. Sidney: Standards Australia Limited, 2004.

Stephan Hartmann and Luc Bovens. A Probabilistic Theory of the Coherence of an Information Set. http://www.gap-im-netz.de/gap4Konf/Proceedings4/pdf/6%20Ek05%20Hartmann.pdf

SUÁREZ, Yadira. La comunicación y las relaciones públicas. Universidad Camagüey. Cuba. 2006

Superintendencia financiera de Colombia – Circular externa 052 de 2007. Octubre

de 2007. Internet: http://www.netsecuritysuite.com/pdf/Norma-052.pdf

TARANTINO, Anthony. Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB's A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices, and Case Studies (Manager's Guide Series). Hoboken, NJ: Wiley, 2006.

THE INSTITUTE OF INTERNAL AUDITORS. International standards for the professional practice of internal auditing (standards). Miami, FL: http://www.theiia.org/, 2009

TILBURG UNIVERSITY. State-of-the-art in the field of compliance languages. 2008

TOULMIN, S. The uses of argument. Cambridge, UK. Cambridge University Press. 1958

TRATADO DE LISBOA: la Unión Europea en el Mundo. Portal de la Unión Europea. 2009

TSENG, Shawn & FOGG, B.J. The Elements of Computer Credibility. Proceedings of ACM CHI 99 Conference on Human Factors in Computing Systems pp. 80-87. NY. ACM Press.

TSENG, Shawn & FOGG, B.J.. Credibility and Computing Technology. Communications of the ACM, vol. 42, issue 5 (May 1999), pp. 39-44.

TURPIN, Andrew; SCHOLER, Falk. "User performance versus precision measures for simple search tasks". Proceedings of the 29th Annual international ACM SIGIR Conference on Research and Development in information Retrieval (Seattle, Washington, USA, August 06-11, 2006) (New York, NY: ACM): 11–18

UNDERWOOD, George M., MAGLIO, Paul P., BARRETT, Rob. User-centered push for timely information delivery. IBM Almaden Research Center. http://www.almaden.ibm.com/cs/wbi/papers/www7/user-centered-push.html

Union Française d'Organismes de Documentation

United Nations (UN) Universal Declaration of Human Rights (1948) Art 12

Universidad de Málaga - Fundación Universitaria Andaluza Inca Garcilaso. Grupo de investigación eumednet. http://www.eumed.net/libros/2007a/239/5d.htm
University of Oulo. Glossary of Vulnerability Testing Terminology. https://www.ee.oulu.fi/research/ouspg/Glossary

US GOVERNMENT. 44 U.S.C., Sec. 3542

VAN DER AALST, W., VAN DONGEN, B. F., HERBST, J., MARUSTER, L., SCHIMM, G., WEIJTERS, A. J. M. M, “Workflow mining: a survey of issues and approaches,” Data and Knowledge Engineering, vol. 47, no. 2, pp. 237–267, 2003.

VIAGGIO, S., A general theory of interlingual mediation, Frank & Timme GmbH, 2006

WALTER, W. Hauck, KOCH, William, ABERNETHY, Darrell, WILLIAMS, Roger L., USP. Making Sense of Trueness, Precision, Accuracy, and Uncertainty. Pharmacopeial Forum. Vol. 34(3) [May–June 2008], pp 838-842

WAND, Y., WANG, R.Y., Anchoring data quality dimensions in ontological foundations, Communications of the ACM 39, 1996, pp. 86–95.
WANG, R.Y., STRONG, D.M. Beyond accuracy: what data quality means to data

consumers. Journal of Management Information Systems 12, 4 (1996), 5–34.

WANG, R.Y.. A product perspective on total data quality management, Communications of the ACM. 1998. Internet: http://mitiq.mit.edu/Publications.htm#1998

WEISSMAN, Tachy. Nformation Theory. Stanford University. 2010

www.mitre.org

www.superfinanciera.gov.co/ConsumidorFinanciero/ce05207.docx

YANG W. Leea, STRONGB, Diane M., KAHNC, Beverly K., WANG, Richard Y.. AIMQ: a methodology for information quality assessment. Elsevier Science B.V., 2002.

ZMUD, R., Concepts, theories and techniques: an empirical investigation of the dimensionality of the concept of information, Decision Sciences 9, 1978, pp. 187–195.

ZUR MUEHLEN, M., ROSEMANN, M., “Integrating risks in business process models,“ in Proceedings of the 16th Australasian Conference on Information Systems, Sydney, November-December 2005.

ANEXO A

ARTICULADO CLAVE EN LA LEGISLACION COLOMBIANA

Ley 23 de 1982. Ley de derechos de autor.

ART 1. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.

ART 2. Los derechos de autor recaen sobre las obras científicas literarias y artísticas las cuales se comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación , tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con letra o sin ella; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los video gramas; las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas o las cuales se asimilan las expresadas por procedimiento análogo a la fotografía a; las obras de arte aplicadas; las ilustraciones, mapas, planos croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias y, en fin, toda producción del dominio científico, literario o artístico que pueda reproducirse, o definirse por cualquier forma de impresión o de reproducción, fonografía, radiotelefonía u otro medio conocido o por conocer.

ART 9. La protección que esta Ley otorga al autor, tiene como título originario la creación intelectual, sin que se requiera registro alguno. Las formalidades que en ella se establecen son para la seguridad jurídica de los titulares de los derechos protegidos.

ART 11. De acuerdo al artículo 35 de la Constitución Nacional "será protegida la propiedad literaria y artística como propiedad transferible, por el tiempo de la vida del autor y ochenta años más, mediante las formalidades que prescriba la Ley.

Ley 1450 de 2011. Ley que modifica la ley de derechos de autor.

ART 28. El artículo 20 de la Ley 23 de 1982 quedará: "Artículo 20. En las obras creadas para una persona natural o jurídica en cumplimento de un contrato de prestación de servicios o de un contrato de trabajo, el autor es el titular originario de los derechos patrimoniales y morales; pero se presume, salvo pacto en contrario, que los derechos patrimoniales sobre la obra han sido transferidos al encargante o al empleador, según sea el caso, en la medida necesaria para el ejercicio de sus actividades habituales en la época de creación de la obra. Para que opere esta presunción se requiere que el contrato conste por escrito. El titular de las obras de acuerdo a este artículo podrá intentar directamente o por intermedia persona acciones preservativas contra actos violatorios de los derechos morales informando previamente al autor para evitar duplicidad de acciones".

Ley 1266 de 2008. Ley de habeas data.

ART 1. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las

informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

ART 2. AMBITO DE APLICACIÓN. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada. Esta ley se aplicará sin perjuicio de normas especiales que disponen confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte de la Fuerza Pública para garantizar la seguridad nacional interna y externa.

Los registros públicos a cargo de las cámaras de comercio se regirán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan.

Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.

ART 4. PRINCIPIOS DE LA ADMINISTRACIÓN DE DATOS. En la presente ley, se

tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;
b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;
c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.
Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;
d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;
e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los

demás derechos constitucionales aplicables;

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

ART 5. CIRCULACIÓN DE INFORMACIÓN. La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos:

a) A los titulares, a las personas debidamente autorizadas por estos y a sus causahabientes mediante el procedimiento de consulta previsto en la presente ley.

b) A los usuarios de la información, dentro de los parámetros de la presente ley.

c) A cualquier autoridad judicial, previa orden judicial.

d) A las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones.

e) A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso.

f) A otros operadores de datos, cuando se cuente con autorización del titular, o

cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.
g) A otras personas autorizadas por la ley.

ART 6. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN. Los titulares tendrán los siguientes derechos:
1. Frente a los operadores de los bancos de datos:
1.1 Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales.
1.2 Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones.
1.3 Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario.
1.4 Solicitar información acerca de los usuarios autorizados para obtener información.

PARÁGRAFO. La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.
La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no

requiere autorización del titular. En todo caso, la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.

2. Frente a las fuentes de la información:

2.1 Ejercer los derechos fundamentales al hábeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales.

2.2 Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones.

2.3 Solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley.

3. Frente a los usuarios:

3.1 Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador.

3.2 Solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en la presente ley.

PARÁGRAFO. Los titulares de información financiera y crediticia tendrán adicionalmente los siguientes derechos:

Podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia.

Así mismo, pueden acudir ante la autoridad de vigilancia para pretender que se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la presente ley

ART 7. DEBERES DE LOS OPERADORES DE LOS BANCOS DE DATOS. Sin perjuicio del cumplimiento de las demás disposiciones contenidas en la presente ley y otras que rijan su actividad, los operadores de los bancos de datos están obligados a:

1. Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de hábeas data y de petición, es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley.

2. Garantizar, que en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley.

3. Permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella.

4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.

5. Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular, cuando dicha autorización sea necesaria, conforme lo previsto en la presente ley.

6. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

7. Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes, en los términos de la presente ley.

8. Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información, en los términos señalados en la presente ley.

9. Indicar en el respectivo registro individual que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho

trámite, en la forma en que se regula en la presente ley.
10. Circular la información a los usuarios dentro de los parámetros de la presente ley.
11. Cumplir las instrucciones y requerimientos que la autoridad de vigilancia imparta en relación con el cumplimiento de la presente ley.
12. Los demás que se deriven de la Constitución o de la presente ley.

ART 8. DEBERES DE LAS FUENTES DE LA INFORMACIÓN. Las fuentes de la información deberán cumplir las siguientes obligaciones, sin perjuicio del cumplimiento de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
1. Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable.
2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
3. Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores.
4. Diseñar e implementar mecanismos para reportar oportunamente la información al operador.
5. Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la presente ley.
6. Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley.
7. Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley.

8. Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite.
9. Cumplir con las instrucciones que imparta la autoridad de control en relación con el cumplimiento de la presente ley.
10. Los demás que se deriven de la Constitución o de la presente ley

ART 9. DEBERES DE LOS USUARIOS. Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los usuarios de la información deberán:
1. Guardar reserva sobre la información que les sea suministrada por los operadores de los bancos de datos, por las fuentes o los titulares de la información y utilizar la información únicamente para los fines para los que le fue entregada, en los términos de la presente ley.
2. Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información.
3. Conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.
4. Cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la presente ley.
5. Los demás que se deriven de la Constitución o de la presente ley.

ART 16. PETICIONES, CONSULTAS Y RECLAMOS.
I. Trámite de consultas. Los titulares de la información o sus causahabientes podrán consultar la información personal del titular, que repose en cualquier banco de datos, sea este del sector público o privado. El operador deberá suministrar a estos, debidamente identificados, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.
La petición, consulta de información se formulará verbalmente, por escrito, o por

cualquier canal de comunicación, siempre y cuando se mantenga evidencia de la consulta por medios técnicos.

La petición o consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

PARÁGRAFO. La petición o consulta se deberá atender de fondo, suministrando integralmente toda la información solicitada.

II. Trámite de reclamos. Los titulares de la información o sus causahabientes que consideren que la información contenida en su registro individual en un banco de datos debe ser objeto de corrección o actualización podrán presentar un reclamo ante el operador, el cual será tramitado bajo las siguientes reglas:

1. La petición o reclamo se formulará mediante escrito dirigido al operador del banco de datos, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. En caso de que el escrito resulte incompleto, se deberá oficiar al interesado para que subsane las fallas. Transcurrido un mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición.

2. Una vez recibido la petición o reclamo completo el operador incluirá en el registro individual en un término no mayor a dos (2) días hábiles una leyenda que diga “reclamo en trámite” y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido y deberá incluirse en la información que se suministra a los usuarios.

3. El término máximo para atender la petición o reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado,

expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

4. En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos (2) días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez (10) días hábiles. En todo caso, la respuesta deberá darse al titular por el operador en el término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de presentación de la reclamación, prorrogables por ocho (8) días hábiles más, según lo indicado en el numeral anterior. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo dentro de los dos (2) días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “reclamo en trámite” y la naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente.

5. Para dar respuesta a la petición o reclamo, el operador o la fuente, según sea el caso, deberá realizar una verificación completa de las observaciones o planteamientos del titular, asegurándose de revisar toda la información pertinente para poder dar una respuesta completa al titular.

6. Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida. La demanda deberá ser interpuesta contra la fuente de la información la cual, una vez notificada de la misma, procederá a informar al operador dentro de los dos (2) días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “información en discusión judicial” y la naturaleza de la misma dentro del registro individual, lo cual

deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente y por todo el tiempo que tome obtener un fallo en firme. Igual procedimiento deberá seguirse en caso que la fuente inicie un proceso judicial contra el titular de la información, referente a la obligación reportada como incumplida, y este proponga excepciones de mérito.

Ley 594 de 2000. Ley general de archivo.

ART 2. AMBITO DE APLICACIÓN. La presente ley comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley.

ART 5. EL SISTEMA NACIONAL DE ARCHIVOS.
a) Es un conjunto de instituciones archivísticas articuladas entre sí, que posibilitan la homogenización y normalización de los procesos archivísticos, promueven el desarrollo de estos centros de información, la salvaguarda del patrimonio documental y el acceso de los ciudadanos a la información y a los documentos;
b) Integran el Sistema Nacional de Archivos: el Archivo General de la Nación, los archivos de las entidades del Estado en sus niveles de la organización administrativa, territorial y por servicios.

Los archivos privados podrán hacer parte del Sistema Nacional de Archivo. Las entidades del Sistema actuarán de conformidad con las políticas y planes generales que para el efecto adopte el Ministerio de la Cultura;

ART 10. OBLIGATORIEDAD DE LA CONFORMACIÓN DE LOS ARCHIVOS PÚBLICOS. El Estado está obligado a la creación, organización, preservación y control de los archivos, teniendo en cuenta los principios de procedencia y orden original, el ciclo vital de los documentos y la normatividad archivística.

ART 12. RESPONSABILIDAD. La administración pública será responsable de la gestión de documentos y de la administración de sus archivos.

ART 13. INSTALACIONES PARA LOS ARCHIVOS. La administración pública deberá garantizar los espacios y las instalaciones necesarias para el correcto funcionamiento de sus archivos. En los casos de construcción de edificios públicos, adecuación de espacios, adquisición o arriendo, deberán tenerse en cuenta las especificaciones técnicas existentes sobre áreas de archivos.

ART 14. PROPIEDAD, MANEJO Y APROVECHAMIENTO DE LOS ARCHIVOS PÚBLICOS. La documentación de la administración pública es producto y propiedad del Estado, y éste ejercerá el pleno control de sus recursos informativos. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.

PARAGRAFO 1o. La administración pública podrá contratar con personas naturales o jurídicas los servicios de custodia, organización, reprografía y conservación de documentos de archivo.

PARAGRAFO 2o. Se podrá contratar la administración de archivos históricos con instituciones de reconocida solvencia académica e idoneidad.

PARAGRAFO 3o. El Archivo General de la Nación establecerá los requisitos y condiciones que deberán cumplir las personas naturales o jurídicas que presten servicios de depósito, custodia, organización, reprografía y conservación de documentos de archivo o administración de archivos históricos.

ART 15. RESPONSABILIDAD ESPECIAL Y OBLIGACIONES DE LOS SERVIDORES PÚBLICOS. Los servidores públicos, al desvincularse de las funciones titulares, entregarán los documentos y archivos a su cargo debidamente inventariados, conforme a las normas y procedimientos que establezca el Archivo General de la Nación, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades.

ART 16. OBLIGACIONES DE LOS FUNCIONARIOS A CUYO CARGO ESTÉN LOS ARCHIVOS DE LAS ENTIDADES PÚBLICAS. Los secretarios generales o los funcionarios administrativos de igual o superior jerarquía, pertenecientes a las entidades públicas, a cuyo carga estén los archivos públicos, tendrán la obligación de velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo y serán responsables de su organización y conservación, así como de la prestación de los servicios archivísticos.

ART 17. RESPONSABILIDAD GENERAL DE LOS FUNCIONARIOS DE ARCHIVO. Los funcionarios de archivo trabajarán sujetos a los más rigurosos principios de la ética profesional, a lo dispuesto en la Constitución Política de Colombia, especialmente en lo previsto en su artículo 15, a las leyes y disposiciones que regulen su labor. Actuarán siempre guiados por los valores de una sociedad democrática que les confíe la misión de organizar, conservar y poner al servicio de la comunidad la documentación de la administración del Estado y aquélla que forme parte del patrimonio documental de la Nación.

ART 18. CAPACITACIÓN PARA LOS FUNCIONARIOS DE ARCHIVO. Las entidades tienen la obligación de capacitar y actualizar los funcionarios de archivo, en programas y áreas de su labor.

ART 19. SOPORTE DOCUMENTAL. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de su archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los requisitos:
a) Organización archivística de los documentos;
b) Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.

PARAGRAFO 1o. Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por la leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información.
PARAGRAFO 2o. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.

ART 21. PROGRAMAS DE GESTIÓN DOCUMENTAL. Las entidades públicas deberán elaborar programas de gestión de documentos, pudiendo contemplar el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivísticos. PARAGRAFO. Los documentos emitidos por los citados medios gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, su integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

ART 24. OBLIGATORIEDAD DE LAS TABLAS DE RETENCIÓN. Será obligatorio para las entidades del Estado elaborar y adoptar las respectivas tablas de retención documental.

ART 26. INVENTARIO DOCUMENTAL. Es obligación de las entidades de la Administración Pública elaborar inventarios de los documentos que produzcan en ejercicio de sus funciones, de manera que se asegure el control de los documentos en sus diferentes fases.

ART 27. ACCESO Y CONSULTA DE LOS DOCUMENTOS. Todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o la ley.
Las autoridades responsables de los archivos públicos y privados garantizarán el

derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las leyes.

ART 46. CONSERVACIÓN DE DOCUMENTOS. Los archivos de la Administración Pública deberán implementar un sistema integrado de conservación en cada una de las fases del ciclo vital de los documentos.

ART 47. CALIDAD DE LOS SOPORTES. Los documentos de archivo, sean originales o copias, deberán elaborarse en soportes de comprobada durabilidad y calidad, de acuerdo con las normas nacionales o internacionales que sean acogidas por el Archivo General de la Nación.

ART 48. CONSERVACIÓN DE DOCUMENTOS EN NUEVOS SOPORTES. El Archivo General de la Nación dará pautas y normas técnicas generales sobre conservación de archivos, incluyendo lo relativo a los documentos en nuevos soportes.

Ley 527 de 1999. Mensajes de datos electrónicos.

ART 1. AMBITO DE APLICACION. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos

ART 5. RECONOCIMIENTO JURIDICO DE LOS MENSAJES DE DATOS. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

ART 6. ESCRITO. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

ART 7. FIRMA. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:
a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.
Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

ART 8. ORIGINAL. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:
a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.
Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

ART 9. INTEGRIDAD DE UN MENSAJE DE DATOS. Para efectos del artículo

anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

ART 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.
En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ART 11. CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

ART 12. CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:
1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.
No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.
Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

ART 13. CONSERVACIÓN DE MENSAJES DE DATOS Y ARCHIVO DE DOCUMENTOS A TRAVÉS DE TERCEROS. El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

ART 14. FORMACION Y VALIDEZ DE LOS CONTRATOS. En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

ART 15. RECONOCIMIENTO DE LOS MENSAJES DE DATOS POR LAS PARTES. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

ART 16. ATRIBUCION DE UN MENSAJE DE DATOS. Se entenderá que un

mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:
1. El propio iniciador.
2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o
3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

ART 18. CONCORDANCIA DEL MENSAJE DE DATOS ENVIADO CON EL MENSAJE DE DATOS RECIBIDO. Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, este último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.
El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

ART 20. ACUSE DE RECIBO. Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:
a) Toda comunicación del destinatario, automatizada o no, o
b) Todo acto del destinatario que indique al iniciador que se ha recibido el mensaje de datos.
Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

ART 21. PRESUNCION DE RECEPCION DE UN MENSAJE DE DATOS. Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que es así.

ART 23. TIEMPO DEL ENVIO DE UN MENSAJE DE DATOS. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

ART 24. TIEMPO DE LA RECEPCION DE UN MENSAJE DE DATOS. De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará así

a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar:

1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o

2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos.

ART 25. LUGAR DEL ENVIO Y RECEPCION DEL MENSAJE DE DATOS. De no

convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:
a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;
b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

Decreto 1151 de 2008. Gobierno en línea.

ART 1. Ambito de Aplicación. Las disposiciones a que se refiere el presente Decreto son de obligatorio cumplimiento para las entidades que conforman la Admi¬nistración Pública, en los términos de los artículos 2° de la Ley 962 de 2005 y 39 de la Ley 489 de 1998.
Parágrafo. Los demás organismos y Ramas del Estado, seguirán los lineamientos señalados en el presente decreto de conformidad con lo previsto en el artículo 209 de la Constitución Política y el artículo 6° de la Ley 489 de 1998, con el fin de garantizar la armonía y articulación en el desarrollo de la Estrategia de Gobierno en Línea.

Ley 962 de 2005. Racionalización de trámites y procedimientos administrativos.

ART 2. AMBITO DE APLICACIÓN. Esta ley se aplicará a los trámites y procedimientos administrativos de la Administración Pública, de las empresas de servicios públicos domiciliarios de cualquier orden y naturaleza, y de los particulares que desempeñen función administrativa. Se exceptúan el

procedimiento disciplinario y fiscal que adelantan la Procuraduría y Contraloría respectivamente.
Para efectos de esta ley, se entiende por "Administración Pública", la definición contenida en el artículo 39 de la Ley 489 de 1998.

ART 3. Las personas, en sus relaciones con la administración pública, tienen los siguientes derechos los cuales ejercitarán directamente y sin apoderado:
A obtener información y orientación acerca de los requisitos jurídicos o técnicos que las disposiciones vigentes impongan a las peticiones, actuaciones, solicitudes o quejas que se propongan realizar, así como a llevarlas a cabo.
A conocer, en cualquier momento, el estado de la tramitación de procedimientos donde tengan la condición de interesados y obtener copias, a su costa, de documentos contenidos en ellos.
A abstenerse de presentar documentos no exigidos por las normas legales aplicables a los procedimientos de que trate la gestión.
Al acceso a los registros y archivos de la administración Pública en los términos previstos por la Constitución y las leyes.

ART 4. DIVULGACIÓN Y GRATUIDAD DE LOS FORMULARIOS OFICIALES. Cuando fuere el caso, todas las entidades y organismos de la Administración Pública deberán habilitar los mecanismos necesarios para poner a disposición gratuita y oportuna de los interesados el formato definido oficialmente para el respectivo período en que deba cumplirse la respectiva obligación, utilizando para el efecto formas impresas, magnéticas o electrónicas.
PARÁGRAFO 2o. En todo caso las entidades de la Administración Pública deberán colocar en medio electrónico, a disposición de los particulares, todos los formularios cuya diligencia se exija por las disposiciones legales.
Para todos los efectos de ley se entenderá que tienen el carácter de formularios oficiales aquellas copias de dichos formularios que obtengan de los medios electrónicos (inciso anterior).

ART 6. MEDIOS TECNOLÓGICOS. Para atender los trámites y procedimientos de su competencia, los organismos y entidades de la Administración Pública deberán ponerlos en conocimiento de los ciudadanos en la forma prevista en las disposiciones vigentes, o emplear, adicionalmente, cualquier medio tecnológico o documento electrónico de que dispongan, a fin de hacer efectivos los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa. Para el efecto, podrán implementar las condiciones y requisitos de seguridad que para cada caso sean procedentes, sin perjuicio de las competencias que en esta materia tengan algunas entidades especializadas.

La sustanciación de las actuaciones así como la expedición de los actos administrativos, tendrán lugar en la forma prevista en las disposiciones vigentes. Para el trámite, notificación y publicación de tales actuaciones y actos, podrán adicionalmente utilizarse soportes, medios y aplicaciones electrónicas.

Toda persona podrá presentar peticiones, quejas, reclamaciones o recursos, mediante cualquier medio tecnológico o electrónico del cual dispongan las entidades y organismos de la Administración Pública.

En los casos de peticiones relacionadas con el reconocimiento de una prestación económica en todo caso deben allegarse los documentos físicos que soporten el derecho que se reclama.

La utilización de medios electrónicos se regirá por lo dispuesto en la Ley 527 de 1999 y en las normas que la complementen, adicionen o modifiquen, en concordancia con las disposiciones del Capítulo 8 del Título XIII, Sección Tercera, Libro Segundo, artículos 251 a 293, del Código de Procedimiento Civil, y demás normas aplicables, siempre que sea posible verificar la identidad del remitente, así como la fecha de recibo del documento.

PARÁGRAFO 1o. Las entidades y organismos de la Administración Pública deberán hacer públicos los medios tecnológicos o electrónicos de que dispongan, para permitir su utilización.

PARÁGRAFO 2o. En todo caso, el uso de los medios tecnológicos y electrónicos

para adelantar trámites y competencias de la Administración Pública deberá garantizar los principios de autenticidad, disponibilidad e integridad.

PARÁGRAFO 3o. Cuando la sustanciación de las actuaciones y actos administrativos se realice por medios electrónicos, las firmas autógrafas que los mismos requieran, podrán ser sustituidas por un certificado digital que asegure la identidad del suscriptor, de conformidad con lo que para el efecto establezca el Gobierno Nacional.

ART 7. PUBLICIDAD ELECTRÓNICA DE NORMAS Y ACTOS GENERALES EMITIDOS POR LA ADMINISTRACIÓN PÚBLICA. La Administración Pública deberá poner a disposición del público, a través de medios electrónicos, las leyes, decretos y actos administrativos de carácter general o documentos de interés público relativos a cada uno de ellos, dentro de los cinco (5) días siguientes a su publicación, sin perjuicio de la obligación legal de publicarlos en el Diario Oficial.

Las reproducciones efectuadas se reputarán auténticas para todos los efectos legales, siempre que no se altere el contenido del acto o documento.

A partir de la vigencia de la presente ley y para efectos de adelantar cualquier trámite administrativo, no será obligatorio acreditar la existencia de normas de carácter general de orden nacional, ante ningún organismo de la Administración Pública.

ART 8. ENTREGA DE INFORMACIÓN. A partir de la vigencia de la presente ley, todos los organismos y entidades de la Administración Pública deberán tener a disposición del público, a través de medios impresos o electrónicos de que dispongan, o por medio telefónico o por correo, la siguiente información, debidamente actualizada:

Normas básicas que determinan su competencia.

Funciones de sus distintos órganos.

Servicios que presta.

Regulaciones, procedimientos y trámites a que están sujetas las actuaciones de

los particulares frente al respectivo organismo o entidad, precisando de manera detallada los documentos que deben ser suministrados, así como las dependencias responsables y los términos en que estas deberán cumplir con las etapas previstas en cada caso.

Localización de dependencias, horarios de trabajo y demás indicaciones que sean necesarias para que las personas puedan cumplir sus obligaciones o ejercer sus derechos ante ellos.

Dependencia, cargo o nombre a quién dirigirse en caso de una queja o reclamo.

Sobre los proyectos específicos de regulación y sus actuaciones en la ejecución de sus funciones en la respectiva entidad de su competencia.

En ningún caso se requerirá la presencia personal del interesado para obtener esta información, la cual debe ser suministrada, si así se solicita por cualquier medio a costa del interesado.

ART 10. UTILIZACIÓN DEL CORREO PARA EL ENVÍO DE INFORMACIÓN. Modifíquese el artículo 25 del Decreto 2150 de 1995, el cual quedará así:

"Artículo 25. Utilización del correo para el envío de información. Las entidades de la Administración Pública deberán facilitar la recepción y envío de documentos, propuestas o solicitudes y sus respectivas respuestas por medio de correo certificado y por correo electrónico.

En ningún caso, se podrán rechazar o inadmitir las solicitudes o informes enviados por personas naturales o jurídicas que se hayan recibido por correo dentro del territorio nacional.

Las peticiones de los administrados o usuarios se entenderán presentadas el día de incorporación al correo, pero para efectos del cómputo del término de respuesta, se entenderán radicadas el día en que efectivamente el documento llegue a la entidad y no el día de su incorporación al correo.

Las solicitudes formuladas a los administrados o usuarios a los que se refiere el presente artículo, y que sean enviadas por correo, deberán ser respondidas dentro del término que la propia comunicación señale, el cual empezará a contarse a

partir de la fecha de recepción de la misma en el domicilio del destinatario. Cuando no sea posible establecer la fecha de recepción del documento en el domicilio del destinatario, se presumirá a los diez (10) días de la fecha de despacho en el correo.

Igualmente, los peticionarios podrán solicitar el envío por correo de documentos o información a la entidad pública, para lo cual deberán adjuntar a su petición un sobre con porte pagado y debidamente diligenciado.

PARÁGRAFO. Para efectos del presente artículo, se entenderá válido el envío por correo certificado, siempre y cuando la dirección esté correcta y claramente diligenciada".

ART 19. PUBLICIDAD Y NOTIFICACIÓN DE LOS ACTOS DE REGISTRO Y TÉRMINO PARA RECURRIR. Para los efectos de los artículos 14, 15 y 28 del Código Contencioso Administrativo, las entidades encargadas de llevar los registros públicos podrán informar a las personas interesadas sobre las actuaciones consistentes en solicitudes de inscripción, mediante la publicación de las mismas en medio electrónico público, en las cuales se indicará la fecha de la solicitud y el objeto del registro.

Los actos de inscripción a que se refiere este artículo se entenderán notificados frente a los intervinientes en la actuación y frente a terceros el día en que se efectúe la correspondiente anotación.

Cuando se publique la actuación de registro en curso en la forma prevista en el inciso primer o de este artículo, los recursos que procedan contra el acto de inscripción podrán interponerse dentro de los cinco (5) días siguientes a la fecha del registro respectivo.

ART 26. FACTURA ELECTRÓNICA. Para todos los efectos legales, la factura electrónica podrá expedirse, aceptarse, archivarse y en general llevarse usando cualquier tipo de tecnología disponible, siempre y cuando se cumplan todos los requisitos legales establecidos y la respectiva tecnología que garantice su

autenticidad e integridad desde su expedición y durante todo el tiempo de su conservación.
La posibilidad de cobrar un servicio con fundamento en la expedición de una factura electrónica se sujetará al consentimiento expreso, informado y por escrito del usuario o consumidor del bien o servicio.

Ley 1273 de 2009. Ley de delitos informáticos.

ART 1. Adiciónase el Código Penal con un Título VII BIS denominado “De la Protección de la información y de los datos”, del siguiente tenor:

CAPITULO I - De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes,

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II - De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

ART 2 Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circustancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: (...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Ley 1341 de 2009. Ley de TICS.

ART 4. INTERVENCIÓN DEL ESTADO EN EL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

1. Proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios.
2. Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal.
3. Promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del Gobierno en Línea.
4. Promover la oferta de mayores capacidades en la conexión, transporte y condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red.
5. Promover y garantizar la libre y leal competencia y evitar el abuso de la posición dominante y las prácticas restrictivas de la competencia.
6. Garantizar el despliegue y el uso eficiente de la infraestructura y la igualdad de oportunidades en el acceso a los recursos escasos, se buscará la expansión, y cobertura para zonas de difícil acceso, en especial beneficiando a poblaciones vulnerables.
7. Garantizar el uso adecuado del espectro radioeléctrico, así como la reorganización del mismo, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de telecomunicaciones responderán jurídica y económicamente por los daños causados a las infraestructuras.
8. Promover la ampliación de la cobertura del servicio.
9. Garantizar la interconexión y la interoperabilidad de las redes de

telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

10. Imponer a los proveedores de redes y servicios de telecomunicaciones obligaciones de provisión de los servicios y uso de su infraestructura, por razones de defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.

11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

12. Incentivar y promover el desarrollo de la industria de tecnologías de la información y las comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones.

13. Propender por la construcción, operación y mantenimiento de infraestructuras de tecnologías de la información y las comunicaciones por la protección del medio ambiente y la salud pública.

Ley 734 de 2002. Código disciplinario único.

ART 25. DESTINATARIOS DE LA LEY DISCIPLINARIA. Son destinatarios de la ley disciplinaria los servidores públicos aunque se encuentren retirados del servicio y los particulares contemplados en el artículo 53 del Libro Tercero de este código.

ART 34. DEBERES. Son deberes de todo servidor público:

4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

Ley 1437 de 2011. Código contencioso administrativo.

ART 4. Las actuaciones administrativas podrán iniciarse:
1. Por quienes ejerciten el derecho de petición, en interés general.
2. Por quienes ejerciten el derecho de petición, en interés particular.
3. Por quienes obren en cumplimiento de una obligación o deber legal.
4. Por las autoridades, oficiosamente.

ART 5. PETICIONES ESCRITAS Y VERBALES. Toda persona podrá hacer peticiones respetuosas a las autoridades, verbalmente o por escrito, por cualquier medio, las cuales deberán contener:
1. La designación de la autoridad a la que se dirigen.
2. Los nombres y apellidos completos del solicitante y de su representante o apoderado, si es el caso, con indicación del documento de identidad y de la dirección.
3. El objeto de la petición.
4. Las razones en que se apoya.
5. La relación de documentos que se acompañan.
6. La firma del peticionario, cuando fuere el caso.
Si quien presenta una petición verbal afirma no saber o no poder escribir y pide constancia de haberla presentado, el funcionario la expedirá en forma sucinta.
Las autoridades podrán exigir, en forma general, que ciertas peticiones se presenten por escrito. Para algunos de estos casos podrán elaborar formularios para que los diligencien los interesados, en todo lo que les sea aplicable, y añadan las informaciones o aclaraciones pertinentes.

A la petición escrita se podrá acompañar una copia que, autenticada por el funcionario respectivo, con anotación de la fecha de su presentación y del número y clase de los documentos anexos, tendrá el mismo valor legal del original y se devolverá al interesado. Esta autenticación no causará derecho alguno a cargo del peticionario.

ART 9. PETICIONES. Toda persona podrá formular peticiones en interés particular. A éstas se aplicará también lo dispuesto en el capítulo anterior.

ART 17. DEL DERECHO A LA INFORMACION. El derecho de petición de que trata el artículo 45 de la Constitución Política incluye también el de solicitar y obtener acceso a la información sobre la acción de las autoridades y, en particular, a que se expida copia de sus documentos, en los términos que contempla este capítulo.

ART 18. INFORMACION GENERAL. Las autoridades mantendrán en sitios de fácil acceso público los documentos relativos a ellas, con información actualizada de interés general acerca de:

1. Las normas que les dan origen y definen sus funciones o su naturaleza y estructura, si es el caso.
2. Las oficinas para formular consultas, entregar y recibir documentos de bienes y conocer las decisiones.
3. Los métodos, procedimientos, formularios y sistemas para el trámite de los diversos asuntos, y los organigramas y manuales de funciones.

Cualquier persona tiene derecho a pedir y obtener copia de los anteriores documentos.

ART 19. INFORMACION ESPECIAL Y PARTICULAR. Toda persona tendrá acceso a los demás documentos oficiales y podrá pedir y obtener copia de ellos. Sin embargo, la petición se negará si la solicitud se refiere a alguno de los documentos que la Constitución Política o las leyes autorizan tratar como

reservados. La decisión negativa será siempre motivada.

ART 25. CONSULTAS. El derecho de petición incluye el de formular consultas escritas o verbales a las autoridades, en relación con las materias a su cargo, y sin perjuicio de lo que dispongan normas especiales.

Estas consultas deberán tramitarse con economía, celeridad, eficacia e imparcialidad y resolverse en un plazo máximo de treinta (30) días.

Las respuestas en estos casos no comprometerán la responsabilidad de las entidades que las atienden, ni serán de obligatorio cumplimiento o ejecución.

Ley 872 de 2003. Gestión de la calidad.

ART 2. ENTIDADES Y AGENTES OBLIGADOS. El sistema de gestión de la calidad se desarrollará y se pondrá en funcionamiento en forma obligatoria en los organismos y entidades del Sector Central y del Sector Descentralizado por servicios de la Rama Ejecutiva del Poder Público del orden Nacional, y en la gestión administrativa necesaria para el desarrollo de las funciones propias de las demás ramas del Poder Público en el orden nacional. Así mismo en las Corporaciones Autónomas Regionales, las entidades que conforman el Sistema de Seguridad Social Integral de acuerdo con lo definido en la Ley 100 de 1993, y de modo general, en las empresas y entidades prestadoras de servicios públicos domiciliarios y no domiciliarios de naturaleza pública o las privadas concesionarios del Estado.

PARÁGRAFO 1o. La máxima autoridad de cada entidad pública tendrá la responsabilidad de desarrollar, implementar, mantener, revisar y perfeccionar el Sistema de Gestión de la Calidad que se establezca de acuerdo con lo dispuesto

en la presente ley. El incumplimiento de esta disposición será causal de mala conducta.

PARÁGRAFO 2o. Las Asambleas y Concejos podrán disponer la obligatoriedad del desarrollo del Sistema de Gestión de la Calidad en las entidades de la administración central y descentralizada de los departamentos y municipios.

ART 3. CARACTERÍSTICAS DEL SISTEMA. El Sistema se desarrollará de manera integral, intrínseca, confiable, económica, técnica y particular en cada organización, y será de obligatorio cumplimiento por parte de todos los funcionarios de la respectiva entidad y así garantizar en cada una de sus actuaciones la satisfacción de las necesidades de los usuarios.

PARÁGRAFO. Este Sistema es complementario a los sistemas de control interno y de desarrollo administrativo establecidos por la Ley 489 de 1998.

El Sistema podrá integrarse al Sistema de Control Interno en cada uno de sus componentes definidos por el Departamento Administrativo de la Función Pública, de acuerdo con las políticas adoptadas por el Presidente de la República.

Ley 87 de 1993. Control interno.

ART 2. OBJETIVOS DEL SISTEMA DE CONTROL INTERNO. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientará al logro de los siguientes objetivos fundamentales:
a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten;
e) Asegurar la oportunidad y confiabilidad de la información y de sus registros;

f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;

ART 4. ELEMENTOS PARA EL SISTEMA DE CONTROL INTERNO. Toda la entidad bajo la responsabilidad de sus directivos debe por lo menos implementar los siguientes aspectos que deben orientar la aplicación del control interno.
i) Establecimiento de sistemas modernos de información que faciliten la gestión y el control;

ART 5. CAMPO DE APLICACIÓN. La presente Ley se aplicarán todos los organismos y entidades de las Ramas del Poder Público en sus diferentes órdenes y niveles así como en la organización electoral, en los organismos de¬ control, en los establecimientos públicos, en las empresas industriales y comerciales del Estado, en las sociedades de economía mixta en las cuales el Estado posea el 90% o más de capital social, en el Banco de la República y en los fondos de origen presupuestal.

ANEXO B – ORGANISMOS DE NORMALIZACIÓN NACIONAL POR PAÍS

Pais	Autoridad – Organismo de normalización
Albania	DPS - General Directorate of Standardization
Algeria	IANOR - Institut algérien de normalisation
Antigua and Barbuda	ABBS - Antigua and Barbuda Bureau of Standards
Argentina	IRAM - Instituto Argentino de Normalización y Certificación CEA - Comité Electrotécnico Argentino
Armenia	SARM - National Institute of Standards and Quality
Australia	SA - Standards Australia - Australian National Committee of the IEC
Austria	ASI - Austrian Standards Institute ÖVE - Austrian Electrotechnical Committee
Azerbaijan	AZSTAND - State Committee on Standardization, Metrology and Patents of the Republic of Azerbaijan
Bahrain	BSMD - Bahrain Standards & Metrology Directorat
Bangladesh	BSTI - Bangladesh Standards and Testing Institution
Belarus	BELST - Committee for Standardization, Metrology and Certification of Belarus BELSTANDART - Belarus National Committee of the IEC
Belgium	CEB - Comité Electrotechnique Belge NBN - Bureau de Normalisation
Bhutan	SQCA - Standards and Quality Control Authority
Bolivia	IBNORCA - Instituto Boliviano de Normalización y Calidad
Bosnia and Herzegovina	BAS - Institute for Standardization of Bosnia and Herzegovina - IEC National Committee of Bosnia & Herzegovina

Botswana	BOBS – Botswana Bureau of Standards
Brazil	ABNT – Associação Brasileira de Normas Técnicas Brazilian National Committee of the IEC
Brunei Darussalam	CPRU – Construction Planning and Research Unit, Ministry of Development
Bulgaria	BDS – Bulgarian Institute for Standardization – Bulgarian National Committee of the IEC
Cambodia	ISC – Institute of Standards of Cambodia
Canada	SCC – Standards Council of Canada - Canadian National Committee of the IEC
Chile	INN – Instituto Nacional de Normalizacion
China	SAC – Standardization Administration of China – Chinese National Committee of the IEC
CSSN	China Standards Information Center
Colombia	ICONTEC – Instituto Colombiano de Normas Técnicas y Certificación – IEC National Committee of Colombia
Congo	OCC – Office Congolais de Contrôle
Costa Rica	INTECO – Instituto de Normas Técnicas de Costa Rica
Croatia	HZN – Croation Standards Institute – National Committee of the IEC
Cuba	NC – Oficina Nacional de Normalización
Cyprus	CYS – Cyprus Organization for Standardization
Czech Republic	UNMZ – Czech Office for Standards, Metrology and Testing - Czech National Committee of the IEC
Denmark	DS – Fonden Dansk Standard – Danish National Committee of the IEC

Dominica	DBOS – Dominica Bureau of Standards
Ecuador	INEN – Instituto Ecuatoriano de Normalización
Egypt	EOS – Egyptian Organization for Standardization and Quality
El Salvador	CONACYT – Consejo Nacional de Ciencia y Tecnología
Estonia	EVS – Eesti Standardikeskus –Estonian National Committee of the IEC
Ethiopia	QSAE – Quality and Standards Authority of Ethiopia
Fiji	FTSQCO – Fiji Trade Standards and Quality Control Office
Finland	SFS – Finnish Standards Association SESKO – Finnish Electrotechnical Standards Association
France	AFNOR – Association française de normalisation UTE – Union Technique de l'Electricité
Georgia	GEOSTM – Georgian National Agency for Standards, Technical Regulation and Metrology
Germany	DIN – Deutsches Institut für Normung DKE – Deutsches Komitee der IEC
Ghana	GSB – Ghana Standards Board
Greece	ELOT – Hellenic Organization for Standardization - Greek National Committee of the IEC
Guatemala	COGUANOR – Comisión Guatemalteca de Norma
Guyana	GNBS – Guyana National Bureau of Standards
Honduras	COHCIT – Consejo Hondureño de Ciencia y Tecnología e Innovación
Hong Kong, China	ITCHKSAR – Innovation and Technology Commission
Hungary	MSZT – Magyar Szabványügyi Testület – Hungarian National Committee of the IEC
Iceland	IST – Icelandic Standards - IEC National Committee of Iceland

India	BIS – Bureau of Indian Standards – Indian National Committee of the IEC
Indonesia	BSN – Badan Standardisasi Nasional – Indonesian National Committee of the IEC
Iran, Islamic Republic of	ISIRI – Institute of Standards and Industrial Research of Iran – Iranian National Committee of the IEC
Iraq	COSQC – Central Organization for Standardization and Quality Control Ministry of Planning and Development Cooperation
Ireland	NSAI – National Standards Authority of Ireland Electro-Technical Council of Ireland
Israel	SII – Standards Institution of Israel – IEC National Committee of Israel
Italy	UNI – Ente Nazionale Italiano di Unificazione CEI – Comitato Elettrotecnico Italiano
Jamaica	JBS – Bureau of Standards, Jamaica
Japan	JISC – Japan Industrial Standards Committee – Japanese National Committee of the IEC
Jordan	JISM – Jordan Institution for Standards and Metrology
Kazakstan	KAZMEMST – Committee for Technical Regulation and Metrology – Kazakhstan National Committee of the IEC
Kenya	KEBS – Kenya Bureau of Standards – IEC National Committee of Kenya
Korea, Republic of	KATS – Korean Agency for Technology and Standards – Korean National Committee of IEC
Kuwait	KOWSMD – Public Authority for Industry, Standards and Industrial Services Affairs
Kyrgyzstan	KYRGYZST – National Institute for Standards and Metrology of the Kyrgyz Republic

Latvia	LVS – Latvian Standard – Latvian National Committee of the IEC
Lebanon	LIBNOR – Lebanese Standards Institution
Liberia	LDS – Liberia Division of Standards
Libyan Arab Jamahiriya	LNCSM – Lybian National Centre for Standardization and Metrology
Lithuania	LST – Lithuanian Standards Board – Lithuanian National Committee of the IEC
Luxembourg	ILNAS – Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services – Comité National CEI du Luxembourg
Macau, China	CPTTM – Macau Productivity and Technology Transfer Center
Macedonia, former Yugoslav Republic of	ISRM – Standardization Institute of the Republic of Macedonia
Malaysia	DSM – Department of Standards Malaysia – Malaysian National Committee of the IEC
Malta	MSA – Malta Standards Authority – IEC Maltese National Committee
Mauritius	MSB – Mauritius Standards Bureau
Mexico	DGN – Dirección General de Normas – Mexican National Committee of the IEC
Moldova, Republic of	INSM – National Institute of Standardization and Metrology of the Republic of Moldova
Mongolia	MASM – Mongolian Agency for Standardization and Metrology
Morocco	SNIMA – Service de normalisation industrielle marocaine
Nepal	NBSM – Nepal Bureau of Standards and Metrology
Netherlands	NEN – Nederlands Normalisatie-Instituut – Netherlands National Committee of the IEC

New Zealand	SNZ – Standards New Zealand – New Zealand Electrotechnical Committee
Nicaragua	DTNM – Dirección de Tecnología, Normalización y Metrología
Nigeria	SON – Standards Organisation of Nigeria
Norway	SN – Standards Norway NEK – Norsk Electroteknisk Komite
Oman	DGSM – Directorate General Specifications and Measurements
Pakistan	PSQCA – Pakistan Standards and Quality Control Authority – Pakistan National Committee of the IEC
Palestine	PSI – Palestine Standards Institution
Panama	COPANIT – Comisión Panameña de Normas Industriales y Técnicas
Papua New Guinea	NISIT – National Institute of Standards and Industrial Technology
Paraguay	INTN – Instituto Nacional de Tecnología, Normalización y Metrología
Peru	INDECOPI – Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
Philippines	BPS – Bureau of Product Standards
Poland	PKN – Polish Committee for Standardization – Polish National Committee of the IEC
Portugal	IPQ – Instituto Português da Qualidade – Portuguese National Committee of the IEC
Qatar	QS – Qatar General Organization for Standards and Metrology
Romania	ASRO – Asociatia de Standardizare din România – Romanian National Committee of the IEC
Russian Federation	GOST-R – Federal Agency on Technical Regulating and Metrology – Russian Federation Committee for the IEC

Rwanda	RBS – Rwanda Bureau of Standard
Saint Lucia	SLBS – Saint Lucia Bureau of Standards
Saint Vincent and the Grenadines	SVGBS – St. Vincent and the Grenadines Bureau of Standards
Saudi Arabia	SASO – Saudi Standards, Metrology and Quality Organization – Saudi Arabian National Committee of the IEC
Senegal	ASN – Association Sénégalaise de Normalisation
Serbia	ISS – Institute for Standardization of Serbia – IEC National Committee of Serbia
Seychelles	SBS – Seychelles Bureau of Standards
Singapore	SPRING SG – Standards, Productivity and Innovation Board – Singapore National Committee of the IEC
Slovakia	SUTN – Slovak Standards Institute – Slovak Electrotechnical Committee (SEV)
Slovenia	SIST – Slovenian Institute for Standardization – Slovenian IEC National Committee
South Africa	SABS – South African Bureau of Standards – South African National Committee of the IEC
Spain	AENOR – Asociación Española de Normalización y Certificación – Comite Nacional Espanol de la CEI
Sri Lanka	SLSI – Sri Lanka Standards Institution
Sudan	SSMO – Sudanese Standards and Metrology Organization
Swaziland	SWASA – Swaziland Standards Authority
Sweden	SIS – Swedish Standards Institute SEK – Svenska Elektriska Kommissionen
Switzerland	SNV – Swiss Association for Standardization CES – Swiss Electrotechnical Committee

Syrian Arab Republic	SASMO – The Syrian Arab Organization for Standardization and Metrology
Tanzania	TBS – Tanzania Bureau of Standards
Thailand	TISI – Thai Industrial Standards Institute –Thai National Committee of the IEC
Trinidad and Tobago	TTBS – Trinidad and Tobago Bureau of Standards
Tunisia	INNORPI – Institut National de la Normalisation et de la Propriété Industrielle – Comité national tunisien de la CEI
Turkey	TSE – Türk Standardlari Enstitüsü – Turkish National Committee of the IEC
Uganda	UNBS – Uganda National Bureau of Standards
Ukraine	DSSU – State Committee of Ukdraine on Technical Regulation and Consumer Policy – Ukrainian National Committee of the IEC
United Arab Emirates	ESMA – Emirates Authority for Standardization and Metrology
United Kingdom	BSI – British Standards Institution – British Electrotechnical Committee
Uruguay	UNIT – Instituto Uruguayo de Normas Técnicas
USA	ANSI – American National Standards Institute – U.S. National Committee of the IEC
Uzbekistan	UZSTANDARD - Agency for Standardization, Metrology and Certification of Uzbekistan
Venezuela	FONDONORMA – Fondo para la Normalización y Certificación de la Calidad
Viet Nam	STAMEQ – Directorate for Standards and Quality – IEC Vietnamese National Committee
Zimbabwe	SAZ – Standards Association of Zimbabwe