UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

DISEÑO DE UN SISTEMA DE GOBIERNO, RIESGOS Y CUMPLIMIENTO PARA SER ALINEADO A DISTINTAS NORMATIVAS Y REGULACIONES EN PEQUEÑAS Y MEDIANAS EMPRESAS

TRABAJO TERMINAL DE GRADO

QUE PARA OBTENER EL GRADO DE
MAESTRO EN ADMINISTRACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTA

PABLO CORONA FRAGA

Dra. en C. Ed ARACELI ROMERO ROMERO

TUTOR ACADÉMICO

(Marzo, 2016)

C.I.E.P./0545/2015
Toluca, México, a 27 de mayo de 2015

DRA. EN C.ED. ARACELI ROMERO ROMERO
PROFESORA DE TIEMPO COMPLETO
P R E S E N T E

Por este conducto y en el marco de las nuevas disposiciones de la Legislación Universitaria, me permito invitarle a fungir como Tutor Académico para dirigir el Trabajo Terminal de Grado denominado: "*Diseño de un sistema de Gobierno, Riesgos y cumplimiento para alinearlo a distintas normativas y regulaciones en pequeñas y medianas empresas* ", con número de registro 546/2015, que presenta el C. Pablo Corona Fraga con número de cuenta 11230643, egresado de la Maestría en Administración de Tecnologías de Información (Modalidad a Distancia) , de la promoción 2013-2014.

Sin otro particular por el momento, aprovecho la ocasión para reiterarle mi más alta estima.

A T E N T A M E N T E
"PATRIA, CIENCIA Y TRABAJO"
"2015, Año del Bicentenario Luctuoso de José María Morelos y Pavón"

M. A.E. VÍCTOR MANUEL ORTEGA GARCÍA
COORDINADOR DE LA MAESTRÍA EN ADMINISTRACIÓN

c.c.p. Archivo.

Cerro de Coatepec, s/n Ciudad Universitaria, Toluca, México. C.P. 50100
Tel. 2 14 02 50 / 2 14 01 71 / 2 13 81 33 / 2 15 47 44 ext. 128 www.fca.uaem.mx, posgrado1317fca@gmail.com

Toluca, México 12 de Febrero 2016

M.A.E . Victor Ortega García
Coodinador de Estudios de Posgrado de la Facultad de Contaduría y Administración
PRESENTE

Por este conducto, me permito informarle que doy por concluida mi función como Tutor Académico del trabajo terminal de grado "***Diseño de un sistema de Gobierno, Riesgos y Cumplimiento para alinearlo a distintas normativas y regulaciones en pequeñas y medianas empresas***". Registrado con el número **546/2015**, desarrollado por el alumno **Pablo Corona Fraga,** con número de cuenta 11230643.

Toda vez que fueron atendidas las observaciones señaladas y que se cumplen los requisitos metodológicos establecidos para tal efecto, por lo que extiendo mi autorización para que el interesado continúe con los trámites correspondientes para la obtención del grado de **Maestría en Administración de Tecnologías de Información (Modalidad a Distancia).**

Sin otro particular, hago propicia la ocasión para enviarle un cordial saludo.

A T E N T A M E N T E

Dra. en C. Ed. Araceli Romero Romero

TUTORA ACADÉMICA

Fecha: 14 de marzo de 2016

Una vez que el (la) alumno(a) **Corona** **Fraga** **Pablo**

Apellido Paterno Apellido Materno Nombre(s)

Egresada(o) de la Maestría en Administración de Tecnologías de Información (Modalidad a Distancia), promoción 2013-2014, con número de cuenta 1230643, ha presentado de acuerdo al artículo 54 del Reglamento de los Estudios Avanzados de la Universidad Autónoma del Estado de México, el Trabajo Terminal de Grado titulado: "Diseño de un sistema de Gobierno, Riesgos y Cumplimiento para alimentarlo a distintas normativas y regulaciones en pequeñas y medianas empresas". Que ha sido dirigido por el Dr. en A. José Antonio López Suarez quien ha emitido su aprobación final, por lo tanto se autoriza la impresión de la Dra. en C. Ed. Araceli Romero Romero ejemplares requeridos, atendiendo las siguientes especificaciones de impresión:

- Entregar 1 ejemplar electrónico (PDF) del Trabajo Terminal de Grado a la Coordinación de Investigación y Estudios de Posgrado de la F.C.A.
- Entregar a la Coordinación de Investigación y Estudios de Posgrado de la F.C.A. constancia de donación a la biblioteca de la Facultad de dos libros y dos ejemplares impresos del Trabajo Terminal de Grado. Para el año 2016, la impresión de los ejemplares será en tamaño carta y empastado (pasta gruesa o pasta delgada) color marrón con letras doradas. El diseño de la portada se proporciona en archivo electrónico.

A T E N T A M E N T E
"PATRIA, CIENCIA Y TRABAJO"
"2016, 60 Aniversario de la Universidad Autónoma del Estado de México"

DRA. EN C. ED. ARACELI ROMERO ROMERO
Coordinadora de Investigación y Estudios de Posgrado

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
COORDINACIÓN DE INVESTIGACIÓN Y ESTUDIOS DE POSGRADO

c.c.p. Archivo

1/1

Agradecimientos

Agradezco a mi familia, por la formación que me dieron, por inculcarle valores y principios desde niño, que me hacen ser quien soy hoy en día. Gracias por enseñarme que el amor y la unión son las herramientas más importantes para la vida y hacerme ver que "la disciplina tarde o temprano vencerá la inteligencia". A mi madre por enseñarme a ser paciente, positivo, soñador e idealista. A mi padre por su amistad, sus enseñanzas y disciplina; ambos ayudaron a forjar mi personalidad y la manera en la que me desenvuelvo en el mundo. A los dos mi admiración y respeto como personas y como padres, pues me ayudaron a entender que no hay mejor manera de vivir y entender a Dios que a través de la vida en comunidad y de anteponer el interés común al personal. A mi hermano por ser un ejemplo e inspiración para conseguir este grado. Eres una gran persona y te admiro, tanto en lo personal como en lo profesional. A mi esposa por el apoyo para logar este objetivo y por siempre estar ahí cuando la necesito, por seguirme en mis locuras e invitarme a las suyas. Somos el mejor equipo y eres la mejor compañera que se podría tener en esta vida. Gracias por ser idealista y siempre ver el lado positivo de las cosas, por ayudarme a enfocarme y darle importancia a las cosas que realmente lo tienen. A mis hijas por su cariño y por inspirarme a querer ser cada día una mejor persona para darles ejemplo. Estoy seguro que lograrán todo lo que se propongan, siempre visualícense en la cima, hasta que lleguen a disputarla o negociarla con aquellos que admiraron.

A NYCE, en particular a Carlos Pérez y Salvador Sánchez por su apoyo para cursar estos estudios de maestría, por creer en mí y brindarme la oportunidad de desarrollarme como persona y profesional. A mis compañeros y colegas de trabajo por su apoyo y paciencia, a Mayté y Fabiola por su ayuda para que este proyecto se hiciera realidad, por sus ideas, por la dedicación y esfuerzo aún más allá de su deber laboral. A Miriam y Jaime por su apoyo y diligencia para concretar los proyectos y permitirme tener el tiempo para dedicarlo a este proyecto.

A mi asesor de maestría, la Doctora Araceli Romero por invitarme a ser parte de esta maestría, por su apoyo, paciencia y dedicación. Eres la culpable de que esté escribiendo estas líneas y en verdad te agradezco la oportunidad.

A Ted Humphreys por brindar ideas frescas y revolucionar mi visión de un tema que creí que dominaba, espero seguir aprendiendo de ti muchos años Master Yoda.

A todos los demás, amigos, compañeros colegas que ayudaron de alguna u otra manera a este trabajo, sería imposible mencionarlos a todos. En realidad, a la humanidad entera, gracias por coincidir, hagamos de esta la mejor versión de la realidad que pueda existir, pensando siempre en el bien común, que es la mejor manifestación de la voluntad de Dios.

Pablo Corona

Índice

Agradecimientos 4
Introducción 6
ANTECEDENTES 7
DESCRIPCIÓN DEL PROBLEMA 8
PLANTEAMIENTO DEL PROBLEMA 9
JUSTIFICACIÓN 11
OBJETIVOS 12
OBJETIVO GENERAL 12
OBJETIVOS ESPECÍFICOS 12
CAPÍTULO I: : MARCO CONCEPTUAL 13
CAPÍTULO II: MARCO CONTEXTUAL 22
CAPÍTULO III: DIAGNÓSTICO Y RESULTADOS DEL ANÁLISIS 30
CAPÍTULO IV: DISEÑO DEL SISTEMA DE CUMPLIMIENTO MÚLTIPLE 40
Diseño de flujos y estructura del Sistema de Cumplimiento Múltiple 40
Características de los controles 45
Requerimientos para la parametrización del Sistema de Cumplimiento Múltiple 53
Arquitectura y componentes tecnológicos de una Red Semántica 54
Evaluación y selección de la metodología y lenguaje para el desarrollo del Sistema 56
Análisis de los requerimientos y diseño de las pruebas 58
CONCLUSIONES Y RECOMENDACIONES 65
CAPÍTULO V: BIBLIOGRAFÍA 67
Referencias 67
Índice de ilustraciones 70
ANEXO 1 71
ANEXO 2 80

Introducción

“Para hacer frente a algunos problemas estratégicos, algunas organizaciones han desarrollado iniciativas conocidas como Gestión, Riesgos y Cumplimiento (GRC), las cuales permiten una revisión integral mediante sus funciones de riesgos y control, además de mejorar su eficiencia y eficacia”. (J.Anderson, 2009)

La estrategia de negocio es fundamental para asegurar la permanencia y éxito de las organizaciones en un mercado cada vez más competitivo. Por ello, es necesario que esta estrategia sea apalancada por herramientas automatizadas que permitan la toma de decisiones, el control y la gestión de las actividades organizacionales para monitorear el desempeño y controlar los resultados que se derivarán de los planes de negocio, requisitos reglamentarios, regulatorios o legales.

La implementación y utilización de herramientas que permitan dar seguimiento a la Gestión de Riesgos y Cumplimiento proporciona beneficios como la gestión del conocimiento, la optimización de recursos, así como una mejor capacidad de respuesta y verificación del cumplimiento legal o regulatorio, lo que permite la entrega de servicios o productos eficaces y una mayor satisfacción del cliente.

Lo anterior se ve reflejado en la capacidad de una organización de dar trazabilidad al cumplimiento de sus objetivos, al origen de dichos objetivos en los intereses de las partes interesadas y a su materialización en las actividades diarias de la organización.

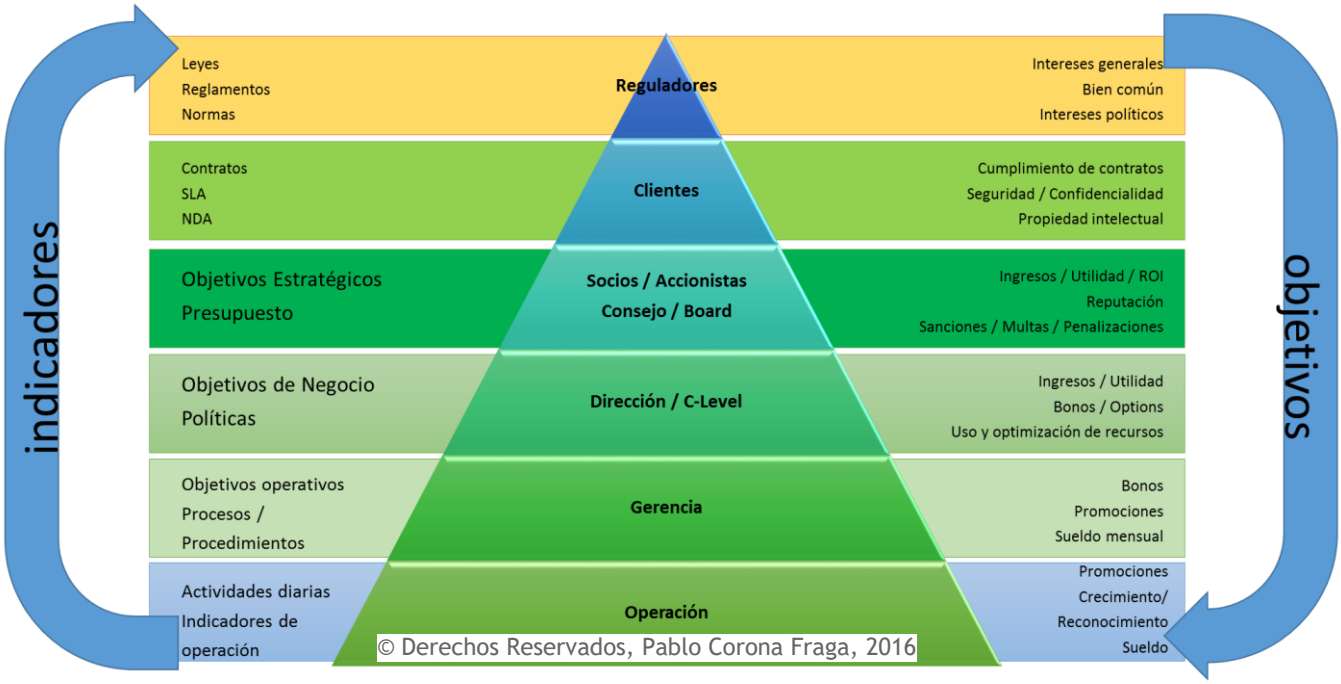


Ilustración 1. Intereses de las partes interesadas y su alineación a los objetivos

ANTECEDENTES

Todas las organizaciones, sin importar su tamaño, buscan el cumplimiento de objetivos que provienen de las partes interesadas de la organización, el contexto en el cual existen y las regulaciones aplicables a su actividad. La *Gestión* es el conjunto de actividades que se desarrollan para la consecución de dichos objetivos; para ello, se establece un plan y posteriormente se lleva a cabo. Sin embargo, ante la variabilidad de las condiciones del entorno, la limitada experiencia en la realización de las actividades, el surgimiento de nuevas necesidades y otros factores tanto internos como externos, la implantación de los planes no siempre es exitosa, por lo cual es necesario verificar cuáles fueron los factores que dieron pie a las desviaciones y tomar las acciones necesarias para corregirlas, de modo que se cuente con una nueva versión del plan que tenga mejores posibilidades de éxito. Esto fue descrito por Deming en su famoso ciclo Planificar-Hacer-Verificar-Actuar (*Plan-Do-Check-Act*); (Deming, 1989).

De este modo, los planes se mantienen en constante evolución en búsqueda de la adaptación a las condiciones cambiantes del entorno y de la operación, lo que se convierte en lo que los cazadores llaman un "objetivo en movimiento". El comandante y después presidente de los Estados Unidos de América, Dwight D. Eisenhower, decía «*In preparing for battle I have always found that plans are useless, but planning is indispensable*», «En la preparación de la batalla siempre he encontrado que los planes son inútiles, pero la planificación es indispensable».

Así que la gestión está basada en el principio de falibilidad de los planes y busca implementar las acciones que los corrijan. Sin embargo, esto puede dar pie a que existan equivocaciones que deriven en que los objetivos no sean alcanzados en los tiempos requeridos, con los recursos establecidos o de la forma esperada, y es entonces que surge el concepto de gobernabilidad corporativa.

La OCDE define el *Gobierno corporativo* o *Gobernabilidad* como los medios por los cuales las organizaciones son dirigidas y controladas (OCDE, 1989). De modo que, si la gestión permite el error para buscar la consecución de un objetivo, la gobernabilidad establece lineamientos de control para definir márgenes de error permisibles, a fin de poner límites a la gestión para asegurar el cumplimiento de las expectativas de las partes interesadas.

Regresando a aquellos factores antes mencionados que impiden la exitosa implementación de los planes, nos encontramos con el concepto de *riesgo*. La norma ISO 31000 de *Gestión de Riesgos* (ISO 31000, 2013) define al riesgo como "Efecto que crea incertidumbre sobre los objetivos", por lo que consideraremos cada uno de esos factores como riesgos que deberán ser atendidos de manera que la organización pueda alcanzar los objetivos planteados.

Anteriormente mencionamos que los objetivos también pueden provenir de la exigencia de una regulación aplicable a la organización. Estas regulaciones pueden ser leyes, reglamentos, normas de cumplimiento obligatorio, requisitos contractuales y otros compromisos adquiridos por las vías legales. La satisfacción de estos requisitos se define como *cumplimiento*.

DESCRIPCIÓN DEL PROBLEMA

La problemática se presenta cuando las organizaciones no son capaces de identificar adecuadamente a sus partes interesadas y los intereses que tiene cada una de ellas, así como traducir estas necesidades en objetivos, máxime cuando estos no son específicos, medibles, agresivos, realistas y con un tiempo definido (Objetivos SMART, 2016).

Posteriormente, la problemática crece cuando esos objetivos no permean a las actividades organizacionales ni sirven para el establecimiento de objetivos por área, que a su vez se reflejen en actividades operativas con entradas y salidas, de las cuales se derivan métricas con las que se generan Indicadores Clave de Desempeño (KPI por sus siglas en inglés) y que estos sean una forma de identificar el cumplimiento de los objetivos.

Tarantino (Tarantino, 2008) propone 3 simples medidas para mejorar la gobernabilidad, la gestión de riesgos y el cumplimiento.

> **SIMPLE SUGGESTIONS TO IMPROVE GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE (GRC)**
>
> **TAKE A HOLISTIC APPROACH TO GRC.**
>
> **Organizations.** An expensive and painful approach to the subject of governance, risk management, and compliance (GRC) is to treat it in a piecemeal and disjointed fashion, as a series of unrelated tasks, and as an unfair and added cost with few tangible benefits—a necessary evil to doing business. A more sensible approach is to accept improved governance as a strategic imperative and key to the growth and prosperity of all organizations.
>
> This entails setting the example at the top of the organization and then having all managers take ownership to the process. Once this occurs, the lower-level activities of risk management and the internal controls to meet laws, regulations, and standards will start to fall into place.
>
> It is natural for companies to complain about the cost of complying with regulations and best practice frameworks. Many of the loudest critics fail to mention that the high costs of compliance are caused by decades of neglect, mergers and acquisitions, and the shortsightedness of their management. The internal control improvements forced by regulations will ultimately make organizations more efficient and therefore more profitable.
>
> …
>
> **MAP PROCESSES TO CONTROLS TO AUDITED REGULATIONS. Organizations.**
>
> In order to avoid redundant compliance activities, it is critical to create a matrix that captures the relationships among business processes, the risks associated with processes, the internal controls deployed to mitigate the risks, the tests used to validate the effectiveness of the controls, and finally the regulations to which the internal controls apply. The example of accounts payable illustrates the point.
>
> …
>
> **RATIONALIZE AND PRIORITIZE RISKS. Organizations.** Even the smallest organization can implement a process to rationalize and quantify risks. It can be as simple as creating a scoring system for three or more variables of risk such as economic impact (severity), likeliness of occurrence (frequency), and ability to detect (discovery). Such a system requires a consensus from the audit committee down to the business owners of each organization. Those risks and controls with the highest risk scores would obviously receive the greatest level of effort and should be the first candidates for process and technology improvements. (Tarantino, 2008)

En resumen: Es necesario utilizar una visión holística para la implementación de la Gobernabilidad, Riesgos y Cumplimiento (GRC), es decir una visión que contemple los distintos aspectos organizacionales y el contexto externo e interno como un todo. Mapear los procesos y controles con las regulaciones y esquemas de cumplimiento a los que debe apegarse la organización, y medir y priorizar los riesgos para implementar medidas que permitan dar tratamiento adecuado y aseguren el cumplimiento de los objetivos organizacionales.

Un sistema informático de GRC adecuadamente diseñado e implantado permitiría establecer una relación directa entre cada una de las actividades realizadas por la organización, sus métricas, los KPI, los objetivos de negocio y las expectativas de las partes interesadas, de forma que todos sean componentes de una sola maquinaria que busca una meta en común.

PLANTEAMIENTO DEL PROBLEMA

En los últimos años, el incremento del mercado de software en México fue de 14 puntos porcentuales. Según datos de Select (SELECT, 2013), el aumento se debió a la demanda de soluciones tecnológicas de T.I. abocadas al procesado y análisis datos. Este estudio indica que entre 2012 y 2020 las áreas de TI mexicanas gestionarán 50 veces más información, lo que representa un enorme reto para la seguridad de la información y el almacenamiento de datos.

La información está compuesta por datos que en un contexto tienen un significado y son útiles; ésta es comunicada a un receptor para tomar decisiones. La información se considera de calidad cuando cumple con los siguientes elementos:

Es exacta – No contiene errores.
Es oportuna – Está disponible en el momento que se requiere.
Es relevante – Íntegra o completa.

Según datos de la Dirección General de Normas, existen 1 749 empresas mexicanas con un sistema de gestión certificado, de las cuales menos del 1% cuenta con dos o más sistemas de gestión implementados e integrados. La mayoría de estas empresas gestionan su documentación de forma tradicional, es decir, mantienen su documentación en papel, lo que provoca que la información no cuente con los elementos de calidad antes mencionados. Las principales causas son la sobre documentación de sus procesos y la falta de tiempo para la revisión y el mantenimiento de sus documentos. Adicionalmente, el sector de tecnologías de la información demanda la aplicación e integración con normas especializadas para este sector.

En la actualidad, existen en el mercado herramientas automatizadas especializadas en un solo estándar o proceso, lo que dificulta la integración de esas herramientas con otros estándares o bien requieren de una mayor inversión derivada de la necesidad de adquirir más herramientas.

En el sector de tecnologías de información, TI, la demanda de productos y servicios que cumplan con la calidad, los niveles de servicio acordados y los controles de seguridad que protejan la información y la privacidad de los datos personales se ha convertido en un requisito obligado si se pretende participar en proyectos privados y gubernamentales. Esto ha provocado la elaboración de

normas tanto internacionales como nacionales, por ejemplo las normas de Sistemas de Gestión especializadas en Tecnologías de Información como son: NMX-I-20000-1-NYCE, NMX-I-27001-NYCE, ISO/IEC 20000-1, ISO/IEC 27001 y la creación de nuevas leyes, como la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Actualmente las organizaciones del sector TI se enfrentan con la necesidad de atender los requisitos de negocio de la operación del producto o servicio que proporcionan, además de cumplir con los requisitos normativos, regulatorios o legales. Estos requisitos exigen mantener un Sistema de gestión cuya piedra angular es la generación de evidencia, así como su constante análisis y mejora, considerando los riesgos asociados al sector, la competencia y las debilidades de la organización.

Estas actividades significan una gran inversión de tiempo para el mantenimiento y control de información documentada, además de personal dedicado a las tareas de revisión, verificación y mejora constante.

Recientes estudios revelan que solo el 20% (ISO Survey, 2014) de las organizaciones con un sistema de gestión implementado logran mantenerlo por más de 3 años, y menos del 5% dan cumplimiento a más de dos referencias normativas. Una de las principales causas es la falta de tiempo y de recursos para la revisión y el mantenimiento constante.

Otro de los principales problemas para estas organizaciones es la falta de integración de su información documentada con todos los requisitos legales vigentes, debido a la actualización constante de los propios estándares y leyes, lo que en la mayoría de los casos eleva los costos para la contratación de personal extra que es necesario para la revisión y adecuación de los documentos.

JUSTIFICACIÓN

Se propone sentar las bases para el desarrollo de una aplicación automatizada para la adecuación de una herramienta que permita el diseño y creación de un sistema que sirva para controlar los documentos, manuales, procedimientos y registros basados en uno o varios sistemas de gestión integrados y que permita el mapeo con varios estándares, regulaciones o leyes.

La evaluación del cumplimiento es uno de los factores que permiten a las empresas asegurar su competitividad y posicionarse en las diversas esferas de influencia dentro y fuera de la organización. Esta evaluación de cumplimiento puede estar enfocada hacia aumentar la certidumbre de los accionistas e inversionistas sobre la solidez de su inversión y la gobernabilidad que tienen sobre los procesos de la organización. También puede estar enfocada hacia requisitos establecidos por un cliente de forma que pueda asegurar que el proveedor cuenta con las condiciones necesarias para asegurar los servicios comprometidos o para contar con un respaldo emitido por un tercero que eleve el nivel de confiabilidad para la selección de proveedores en los procesos de adquisiciones.

Las organizaciones dedican una gran cantidad de recursos a implementar, supervisar y evaluar estos esquemas de cumplimiento y, en muchos casos, cada área maneja la documentación en formatos y sistemas distintos, lo que entorpece la revisión y recolección de evidencia, además de aumentar el tiempo y el costo dedicados al cumplimiento.

Por ello es pertinente contar con una herramienta que facilite el cumplimiento de múltiples regulaciones y requisitos por medio de políticas, procesos y procedimientos que sean transversales en la organización y que permitan de forma sencilla identificar las actividades a realizar por cada uno de los actores, las responsabilidades que estos tienen y los elementos que resultarán de cada una de ellas.

Esta herramienta, en adelante referida como “Sistema de cumplimiento múltiple”, contará con dos partes principales; la primera parte está enfocada en la inclusión y mantenimiento de requisitos legales, comúnmente conocidos como leyes, regulaciones, normas o acuerdos legales, donde será posible actualizar los requisitos de acuerdo a los documentos oficiales vigentes. Estos requisitos deberán siempre estar asociados a un elemento de la segunda parte principal la cual se identificará como el Sistema de Gestión.

La segunda parte, como se indica, estará enfocada al Sistema de Gestión de la organización, la cual contendrá los elementos básicos de un sistema de gestión y los elementos específicos del documento oficial vigente. Esta parte estará estructurada de acuerdo al ciclo de mejora continua para estos sistemas, basado en cuatro fases: planear, hacer, verificar y actuar.

Entre los principales beneficios de esta herramienta se encuentra la automatización de estas cuatro fases, especialmente de la planeación, la verificación y la mejora. Además, permitirá la actualización constante de los requisitos aplicables, la elaboración automática de documentos, riesgos y revisión automática de tendencias, lo que facilitará una adecuada toma decisiones.

OBJETIVOS

OBJETIVO GENERAL

Diseñar un sistema de cumplimiento múltiple que permita a las organizaciones planear, documentar y recabar evidencia de los procesos, políticas, directrices, manuales y procedimientos que los lleven al cumplimiento de sus labores diarias, de los compromisos con clientes, accionistas y las regulaciones aplicables a la organización, y que permita la generación automática de tendencias basada en la información documentada en el sistema, tomando como base una herramienta existente.

OBJETIVOS ESPECÍFICOS

- Definir y documentar la estructura del Sistema de cumplimiento múltiple,
- Analizar los requerimientos para la parametrización de herramientas,
- Analizar los requerimientos y diseñar las pruebas requeridas para el Sistema de cumplimiento múltiple.

CAPÍTULO I: : MARCO CONCEPTUAL

La sociedad de la información, de acuerdo a la CEPAL en la Declaración de Bávaro (2003a), es:

«Un sistema económico y social donde el conocimiento y la información constituyen fuentes fundamentales de bienestar y progreso, que representa una oportunidad para nuestros países y sociedades, si entendemos que el desarrollo de ella en un contexto tanto global como local requiere profundizar principios fundamentales tales como el respeto a los derechos humanos dentro del contexto más amplio de los derechos fundamentales, la democracia, la protección del medio ambiente, el fomento de la paz, el derecho al desarrollo, las libertades fundamentales, el progreso económico y la equidad social».

Sistemas de información

Un sistema de información se compone por tres elementos: humano, tecnológico y organizacional. Bajo esta perspectiva, el concepto de información se define en términos de tres niveles de semiótica: datos que pueden ser procesados automáticamente por un sistema de aplicaciones corresponden al nivel de sintaxis; en el contexto de un individuo que interpreta los datos, estos son convertidos en información, lo que corresponde al nivel semántico; por último, la información se convierte en conocimiento cuando un individuo conoce (entiende) y evalúa la información (por ejemplo para una tarea específica), esto corresponde al nivel pragmático.

Para CORNELLA (Cornella, 2000), *«las sociedades del conocimiento son las organizaciones y las personas que se enfrentan a la necesidad de gestionar la información de manera eficiente. La desproporción entre el volumen creciente de información a la que se tiene acceso y la escasa disponibilidad de conocimiento, expone a las organizaciones e individuos a un mayor riesgo de caer en la brecha cognitiva».*

Tipos de Sistemas de información

Las organizaciones que pretenden sobrevivir en la sociedad del conocimiento deberán incrementar su capital intelectual, además de diseñar y aplicar nuevas estrategias de generación de conocimiento.

El principal uso que se da a los Sistemas de Información (SI), es el de optimizar el desarrollo de las actividades de una organización con el fin de ser más productivos y obtener ventajas competitivas, en primer término, se puede clasificar a los sistemas de información en:

- Sistemas Competitivos
- Sistemas Cooperativos
- Sistemas que modifican el estilo de operación del negocio

La primera clasificación se basa en la jerarquía de una organización y se llamó el modelo de la pirámide (Beynon-Davies, 2002); véase la Ilustración 2.

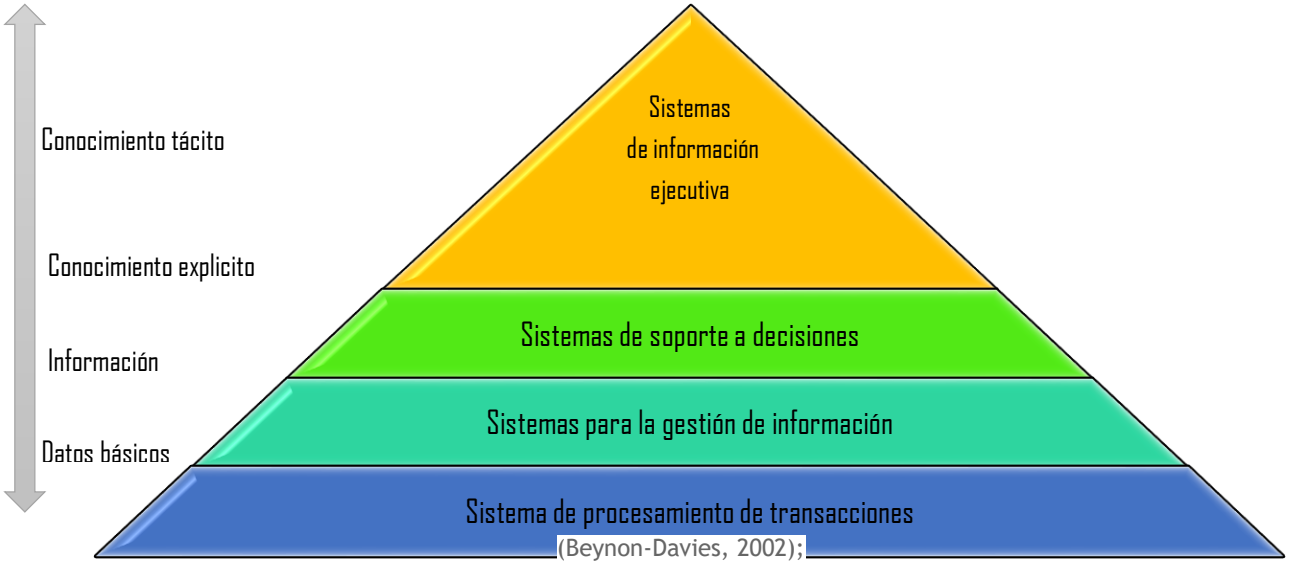
Modelo de la pirámide. Según la función a la que vayan destinados o el tipo de usuario final del mismo, los SI pueden clasificarse en:

Sistema de procesamiento de transacciones (TPS).- Gestiona la información referente a las transacciones producidas en una empresa u organización; también se le conoce como Sistema de Información operativa.

Sistemas para la gestión de información (MIS).- Orientados a solucionar problemas empresariales en general.

Sistemas de soporte a decisiones (DSS).- Herramienta para realizar el análisis de las diferentes variables de negocio con la finalidad de apoyar el proceso de toma de decisiones.

Sistemas de información ejecutiva (EIS).- Herramienta orientada a usuarios de nivel gerencial, que permite monitorizar el estado de las variables de un área o unidad de la empresa a partir de información interna y externa a la misma. Es en este nivel donde los sistemas de información manejan información estratégica para las empresas.



(Beynon-Davies, 2002);

Ilustración 2. Modelo de la pirámide.

Estos sistemas de información no surgieron simultáneamente en el mercado; los primeros en aparecer fueron los TPS, en la década de los 60. Sin embargo, con el tiempo, otros sistemas de información comenzaron a evolucionar; los primeros proporcionan información a los siguientes a medida que aumenta la escala organizacional. Entre ellos se encuentran:

Sistemas de automatización de oficinas (OAS).- Aplicaciones destinadas a ayudar al trabajo diario del administrativo de una empresa u organización.

Sistema Planificación de Recursos (ERP).- viene de las primeras letras: Enterprise Resource Planning, cuyo objetivo es la planificación de los recursos de una organización. Típicamente se lo ha utilizado en empresas productivas que han seguido metodologías de planificación MRPII. El objetivo es tener claramente identificado cómo llegar a los productos finales desde la materia prima; es decir, desde un inventario de materia prima e insumos poder determinar la cantidad que llegaremos a generar de productos finales para ponerlos a disposición del mercado. Integran la información y los procesos de una organización en un solo sistema.

Sistema experto (SE).- Emulan el comportamiento de un experto en un dominio concreto.

Los últimos fueron los SE, que alcanzaron su auge en los 90 —aunque estos últimos tuvieron una tímida aparición en los 70 que no se utilizó ya que la tecnología no estaba suficientemente desarrollada.

Sistemas de información estratégicos

Pueden considerarse como el uso de la tecnología de la información para respaldar o dar forma a la estrategia competitiva de la organización, al plan de ésta para incrementar o mantener su ventaja competitiva o bien para reducir la ventaja de sus competidores.

Su función primordial es crear una diferencia con respecto a los competidores de la organización —o salvar dicha diferencia— que la hagan más atractiva para los potenciales clientes. Por ejemplo, en la banca, hace años que se implantaron los cajeros automáticos, pero en su día, las entidades que primero ofrecieron este servicio disponían de una ventaja con respecto a sus competidores, y hoy día cualquier entidad que pretenda ofrecer servicios bancarios necesita contar con cajeros automáticos si no quiere iniciar con una desventaja respecto al resto de entidades de este sector. En este sentido, los cajeros automáticos se pueden considerar sistemas de información estratégicos.

La función de estos SI es lograr ventajas que los competidores no posean, tales como ventajas en costos y servicios diferenciados con clientes y proveedores, además de apoyar el proceso de innovación de productos dentro de la empresa. Suelen desarrollarse dentro de la organización, por lo tanto no pueden adaptarse fácilmente a paquetes disponibles en el mercado.

Entre las características más destacables de estos sistemas se pueden señalar:

a) Beneficios de Sistemas de información estratégicos
- Cambian significativamente el desempeño de un negocio al medirse por uno o más indicadores clave, entre ellos, la magnitud del impacto.
- Contribuyen al logro de una meta estratégica.
- Generan cambios fundamentales en la forma de dirigir una compañía, la forma en que compite o en la que interactúa con clientes y proveedores.

b) Clasificación según su entorno de aplicación
- Entorno transaccional: Una transacción es un suceso o evento que crea/modifica los datos. El procesamiento de transacciones consiste en captar, manipular y almacenar los datos, y también, en la preparación de documentos; en el entorno transaccional, por tanto, lo importante es qué datos se modifican y cómo, una vez que ha terminado la transacción. Los TPS son los SI típicos que se pueden encontrar en este entorno.
- Entorno decisional: Este es el entorno en el que tiene lugar la toma de decisiones; en una empresa, las decisiones se toman a todos los niveles y en todas las áreas (otra cosa es si esas decisiones son estructuradas o no), por lo que todos los SI de la organización deben estar preparados para asistir en esta tarea, aunque típicamente son los DSS los que se encargan de esta función. Si el único SI de una compañía preparado para ayudar a la toma de decisiones es el DSS, éste debe estar adaptado a todos los niveles jerárquicos de la empresa.

En la era post-industrial —la era de la información— el enfoque de las compañías ha cambiado de la orientación hacia el producto a la orientación hacia el conocimiento. En este sentido el mercado compite hoy en día en términos del proceso y de la innovación, en lugar del producto. El énfasis ha cambiado de la calidad y la cantidad de producción hacia el proceso de producción en sí mismo, y los servicios que acompañan este proceso.

El mayor de los activos de una compañía hoy en día es su información, representada por su personal, su experiencia, su conocimiento, y sus innovaciones (patentes, derechos de autor, secreto comercial). Para poder competir, las organizaciones deben poseer una fuerte infraestructura de información en cuyo corazón se sitúa la infraestructura de la tecnología de información, de tal manera que el sistema de información se centre en estudiar las formas para mejorar el uso de la tecnología que soporta el flujo de información dentro de la organización. Un sistema de información debe brindar la totalidad de los elementos que conforman los datos, en una estructura robusta, homogénea y flexible ante los futuros cambios.

El crecimiento de las Tecnologías de la información y comunicaciones

Los flujos de información y la comunicación se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social y productiva.

El de tecnologías de información y comunicaciones (TIC) es un término que contempla toda forma de tecnología usada para crear, almacenar, intercambiar y procesar información. Su objetivo principal es la mejora y el soporte a los procesos de operación y negocios para incrementar la competitividad y productividad de las personas y organizaciones en el tratamiento de cualquier tipo de información.

Un estudio realizado por diversas organizaciones líderes en el sector (AMITI, CANIETI, FMD, 2006) indica que entre 2012 y 2020 las áreas de TI mexicanas gestionarán 50 veces más información, lo que representa un enorme reto para la seguridad de la información y el almacenamiento de datos.

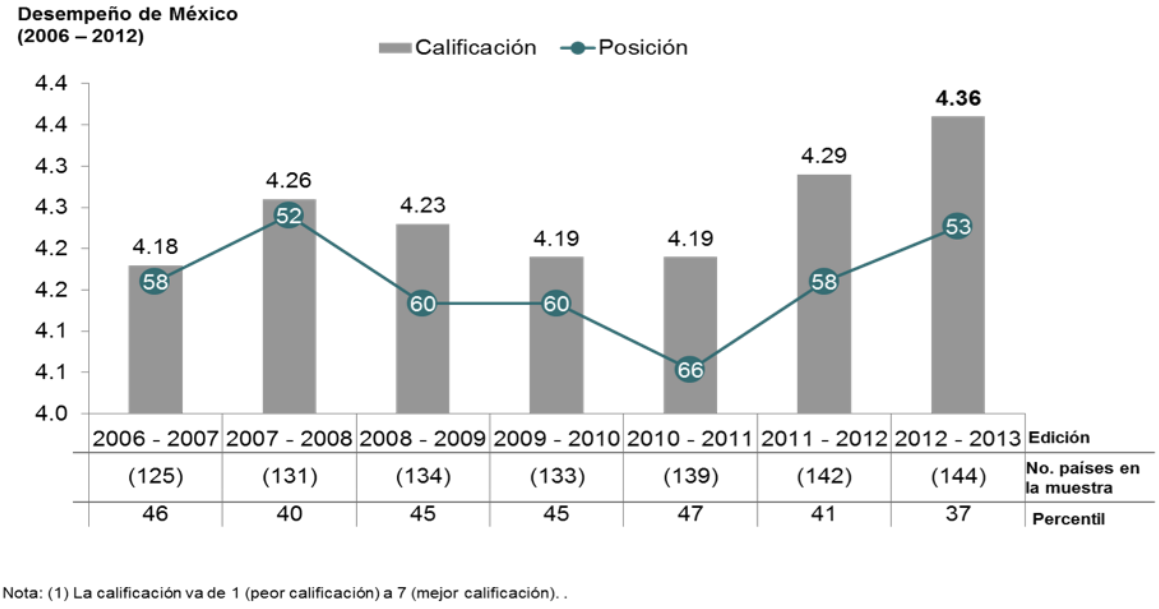
Principales retos de empresas Mexicanas

Las empresas Mexicanas compiten no solamente con las empresas nacionales sino con aquellas que vienen del exterior, produciendo bajo diferentes sistemas financieros estados de derecho y una cultura laboral distinta, entre muchos otros factores que determinan la competitividad; se trata de una serie de elementos que además de multiplicarse, quedaron fuera del control de las empresas.

El Reporte Global de Competitividad 2012-2013 (Foro Económico Mundial, 2014) —elaborado anualmente por el Foro Económico Mundial (WEF, por sus siglas en inglés), organización con sede en Suiza— define la competitividad como el conjunto de instituciones, políticas y otros factores que determinan el nivel de productividad de un país.

En este reporte, México avanzó cinco posiciones con respecto a la edición 2011–2012, pasando del lugar 58 al 53. Por segundo año consecutivo, México vuelve a mostrar una mejora importante en dicho reporte, avanzando 13 posiciones en total, pasando de la posición 66 en la edición de hace

dos años, a la 53 en la edición actual. Véase la Gráfica 1, Desempeño global de México y Tabla 1, Índice global de competitividad.



Nota: (1) La calificación va de 1 (peor calificación) a 7 (mejor calificación). .

Ilustración 3. Desempeño Global de México.

Desempeño Global de México (Foro Económico Mundial, 2014)

Si bien en los últimos años México ha mejorado, se continúa perdiendo competitividad en el área de tecnología, y la eficiencia en el Mercado Laboral, en el que una regulación rígida y poco funcional ha provocado un rezago en este tema, inhibiendo a su vez el crecimiento de la economía en su conjunto. Véase la Tabla 1

Índice global de competitividad. (Foro Económico Mundial, 2014)

Pilar	*2011-2012*		*2012-2013*		*Cambio en posición*
	Calificación	*Posición*	*Calificación*	*Posición*	
Índice Global de Competitividad	**4.29**	**58**	**4.36**	**53**	**5**
Instituciones	3.44	103	3.59	92	11
Infraestructura	3.98	66	4.03	68	-2
Ambiente Macroeconómico	5.25	39	5.21	40	-1
Salud y educación básica	5.69	69	5.71	68	1
Educación superior y capacitación	4.07	72	4.11	77	-5
Eficiencia del mercado de bienes	4.08	84	4.2	79	5
Eficiencia del mercado laboral	3.92	114	4.01	102	12
Desarrollo del mercado financiero	3.92	83	4.15	61	22
Preparación tecnológica	3.75	63	3.8	72	-9
Tamaño de mercado	5.55	12	5.58	12	0
Sofisticación empresarial	4.11	56	4.26	44	12
Innovación	3.19	63	3.33	56	7

Tabla 1. Índice global de competitividad.

Independientemente de cómo se mida, todos los organismos internacionales coinciden en esta tendencia.

Perder competitividad, también implica que el país deja de ser atractivo para los inversionistas e incluso que las empresas mexicanas simplemente cesan de producir. Esto se traduce en menos probabilidades de empleo, menos ingresos fiscales y menor calidad de vida para los mexicanos.

La estrategia de negocio es fundamental para asegurar la permanencia y éxito de las organizaciones en un mercado cada vez más competitivo, por ello es necesario que esta estrategia sea apalancada por herramientas automatizadas que permitan la toma de decisiones.

Minería de datos

En los últimos años ha surgido el concepto de "Minería de datos" que es el conjunto de técnicas y tecnologías que permiten explorar grandes bases de datos —de manera automática o semiautomática— con el objetivo de encontrar patrones repetitivos, tendencias o reglas que expliquen el comportamiento de los datos en un determinado contexto.

En el mundo han ocurrido sucesos que han contribuido a una transformación de la industria TIC, entre los que se encuentran los cambios en la ubicación de la producción global de bienes TIC, motivados por el avance vertiginoso de China y otros países asiáticos.

Este cambio no sólo se ha gestado en la industria de equipos, sino también en los servicios TIC que transforman la distribución global de la producción de software. En los últimos seis años, el balance de la industria TIC en México es positivo, con un crecimiento acumulado de 26 por ciento, superior al de la economía.

Adicionalmente se han creado y adoptado diferentes estándares o modelos basados en Sistemas Gestión, que son un conjunto de elementos interrelacionados o que interactúan para dirigir y controlar actividades que ayuden a mejorar la eficacia del servicio mediante el logro de objetivos específicos.

Estos sistemas están basados en la metodología PHVA (Planificar-Hacer-Verificar-Actuar) que también se conoce como el Ciclo de Deming, en honor a su creador Edwards Deming (Deming, 1989). Véase la Ilustración 4, la cual indica cuatro fases:

Planificar: definir los objetivos y los medios para conseguirlos.
Hacer: implementar la visión preestablecida.
Verificar: comprobar que se alcanzan los objetivos previstos con los recursos asignados.
Actuar: analizar y corregir las desviaciones detectadas, así como proponer mejoras a los procesos utilizados.

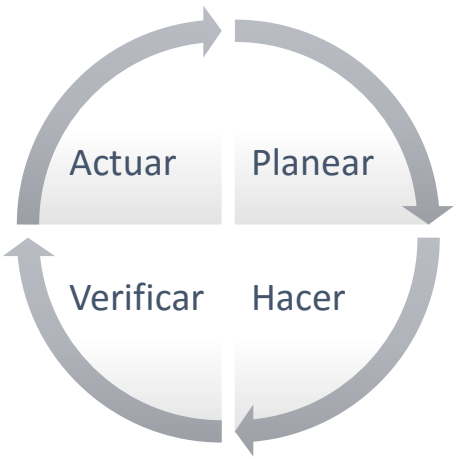


Ilustración 4. Modelo de PHVA

Por su naturaleza, estos sistemas requieren la creación y mejora constante de políticas, procesos, procedimientos, planes y otros documentos que permitan la generación y análisis de información para la toma de decisiones y la mejora continua.

Estos estándares son elaborados por la Organización Internacional de Normalización, y su adopción en las diferentes organizaciones a nivel mundial ha ido aumentando en forma significativa. De acuerdo con estudios recientes de ISO (*International Organization for Standardization*, Organización Internacional de Normalización). Hasta el año 2014, se habían entregado 1,609,294 certificados bajo las normas emitidas por esta organización, lo que significó un crecimiento del 3%. La Tabla 2 muestra el Índice de normas emitidas por la Organización Internacional de Normalización -ISO 2014 (ISO Survey, 2014).

Standard	number of certificates in 2014	number of certificates in 2013	evolution	evolution in %
ISO 9001	1 138 155	1 126 460	11 695	1 %
ISO 14001	324 148	301 622	22 526	7 %
ISO 50001	6 778	4 826	1 952	40 %
ISO/IEC 27001	23 972	22 349	1 623	7 %
ISO 22000	30 500	26 847	3 653	14 %
ISO/TS 16949	57 950	53 723	4 227	8 %
ISO 13485	27 791	25 655	2 136	8 %
ISO 22301	1 757			
TOTAL	**1 609 294**	**1 561 482**	**47 812**	**3 %**

Tabla 2. Índice de normas emitidas por la Organización Internacional de Normalización -ISO 2014

Este estudio muestra un incremento del 13% en el uso de estándares de Sistemas de Gestión de Tecnologías de la información como son; las normas: ISO/IEC 27001 Requisitos para un Sistema de Gestión de Seguridad de la Información, ISO/IEC 20000-1 Requisitos para un Sistema de Gestión de Servicios, ISO/IEC 22301 Requisitos para un Sistema de Gestión de Continuidad de Negocio.

Los resultados de este estudio ubican a México en el segundo lugar con más de 3 500 certificados emitidos durante el año 2012, únicamente superado por Estados Unidos.

Este estudio internacional llamado “ISO Survey 2014” (ISO Survey, 2014) indica que la ISO 9001 la norma con la mayor cantidad de certificados emitidos, si bien cada año hay un incremento en el número de certificaciones ISO 9001, esto no quiere decir que se estén incrementando al mismo ritmo que en años anteriores. Por ejemplo, La Ilustración 5 muestra que el crecimiento en el número de certificados se ha ido estancando mundialmente desde el año 2010, podemos observar que el ritmo en el cual están creciendo el número de certificaciones se ha ido desacelerando desde hace ya un tiempo atrás.

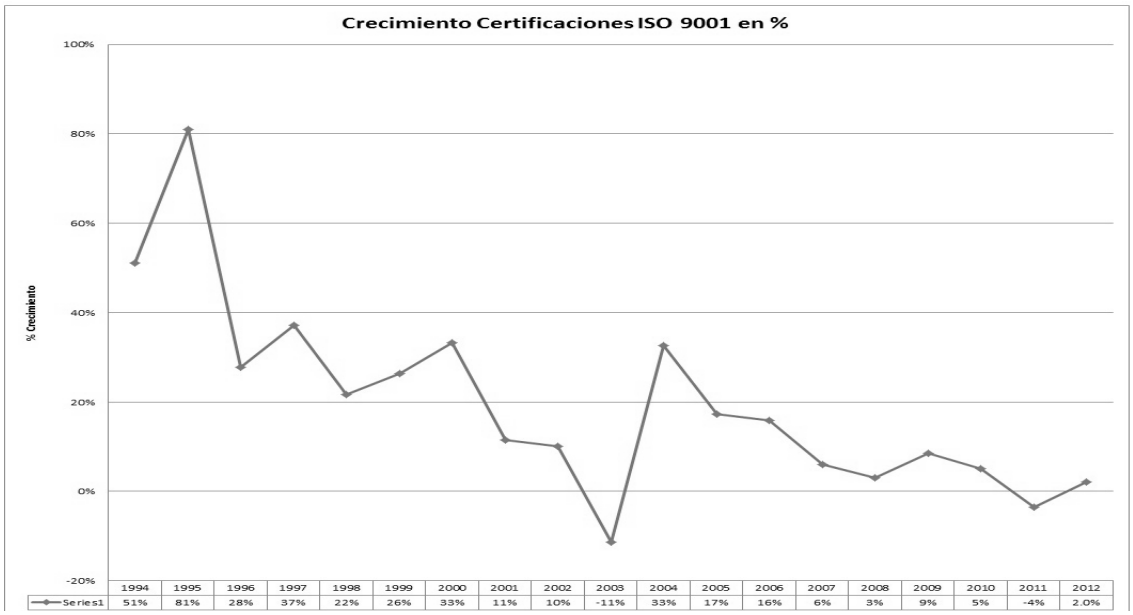


Ilustración 5. Crecimiento Certificaciones ISO 9001 en porcentaje.

Actualmente no existen estudios formales sobre esta desaceleración, sin embargo se ha detectado que uno de los principales motivos, es que el cumplir y mantener el cumplimiento de una normativa o regulación ha recaído en una sola área, como el área legal, de calidad o normatividad y no se logra permear en toda la organización, debido principalmente a que no hay integración de los procesos organizacionales con las diferentes normativas.

En México se han implementado programas gubernamentales y privados para la promoción y adopción de estos estándares por medio de la Secretaria de Economía y de la Asociación Mexicana de la Industria de Tecnologías de Información, lo que ha ayudado a la adopción de más de un modelo o estándar en las organizaciones de manera que se incremente su productividad y competitividad.

Según datos de la Dirección General de Normas de la Secretaría de Economía, existen 1 749 empresas mexicanas con un sistema de gestión certificado, de las cuales menos del 1% cuenta con dos o más sistemas de gestión implementados e integrados.

A partir de esta necesidad, la Organización Internacional de Estándares ha elaborado guías para la integración entre los diferentes Sistemas de Gestión, como la ISO/IEC 27013 que es una guía de integración entre las normas ISO/IEC 20000-1 e ISO/IEC 27001.

El sistema de gestión de una organización comprende la planeación, organización, dirección y control; es el patrón global basado en diferentes modelos como Ciclo de Deming e ITIL, y está relacionado fundamentalmente con la toma de decisiones para planear y controlar el esfuerzo de la organización.

CAPÍTULO II: MARCO CONTEXTUAL

Los sistemas de información se han vuelto un elemento clave para el establecimiento del diseño de flujos de negocio y toma de decisiones, los cuales identifican la necesidad de control sobre los riesgos que afectan el cumplimiento de la continuidad del negocio. La Ilustración 6 muestra la relación entre estos elementos. A esta cualidad de control se le llama Gobernabilidad.

Gobernabilidad

La palabra de origen latín "Gobernanza" según la Real Academia Española, (RAE, 2001), es la acción y efecto de gobernar o gobernarse; la definición más reciente indica que gobernabilidad es el arte o la manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía. El término *Gobernabilidad*, que en su primera acepción de la RAE significa cualidad de gobernable, y que suele emplearse sobre todo en relación con su contrario (ingobernabilidad), es, en su segunda acepción, un sinónimo de gobernanza.

La Gobernanza incluye el ejercicio de la autoridad legal y regulatorio, así como el uso de recursos institucionales para la gestión de las organizaciones. También es un área de la economía que estudia las cuestiones relacionadas con la separación y la segregación de la propiedad y de control. Relaciones de gobernanza incluyen aquellas entre los directores de consejo, los propietarios, gerentes, empleados, proveedores, clientes, reguladores y comunidades.

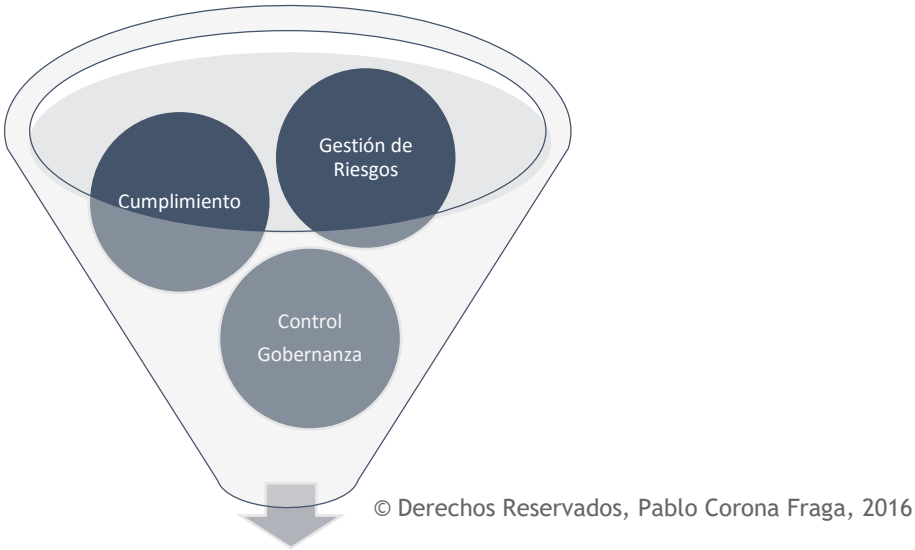


Ilustración 6. Gobernabilidad.

El gobierno corporativo es el proceso por medio del cual una organización defiende los intereses de las partes involucradas o interesadas (*stakeholders*), que pueden incluir miembros del consejo, la compañía de ejecutivos, empleados, accionistas, proveedores, clientes y la comunidad en la que opera la organización. La gobernanza se refiere a la relación entre los que gobiernan y los

gobernados. En el plano político, el gobierno corporativo es la relación existente entre el gobierno y sus ciudadanos, e incluye tres requisitos: conocer el estado actual, saber hacia dónde se tiene que ir, y conocer cómo se está avanzando. Esta relación puede verse en la Ilustración 7.
La desviación entre estos tres requisitos se conoce como *Análisis de brecha*.

Para realizar un análisis de las deficiencias, se involucran tres áreas de la toma de decisiones: quién está gobernando, quién está siendo gobernado, y qué recursos o activos han de ser desplegados en el proceso. Los requisitos y la toma de decisiones se aplican a los gobiernos y las corporaciones por igual. La Ilustración 4 muestra las partes interesadas considerando ambos planos.

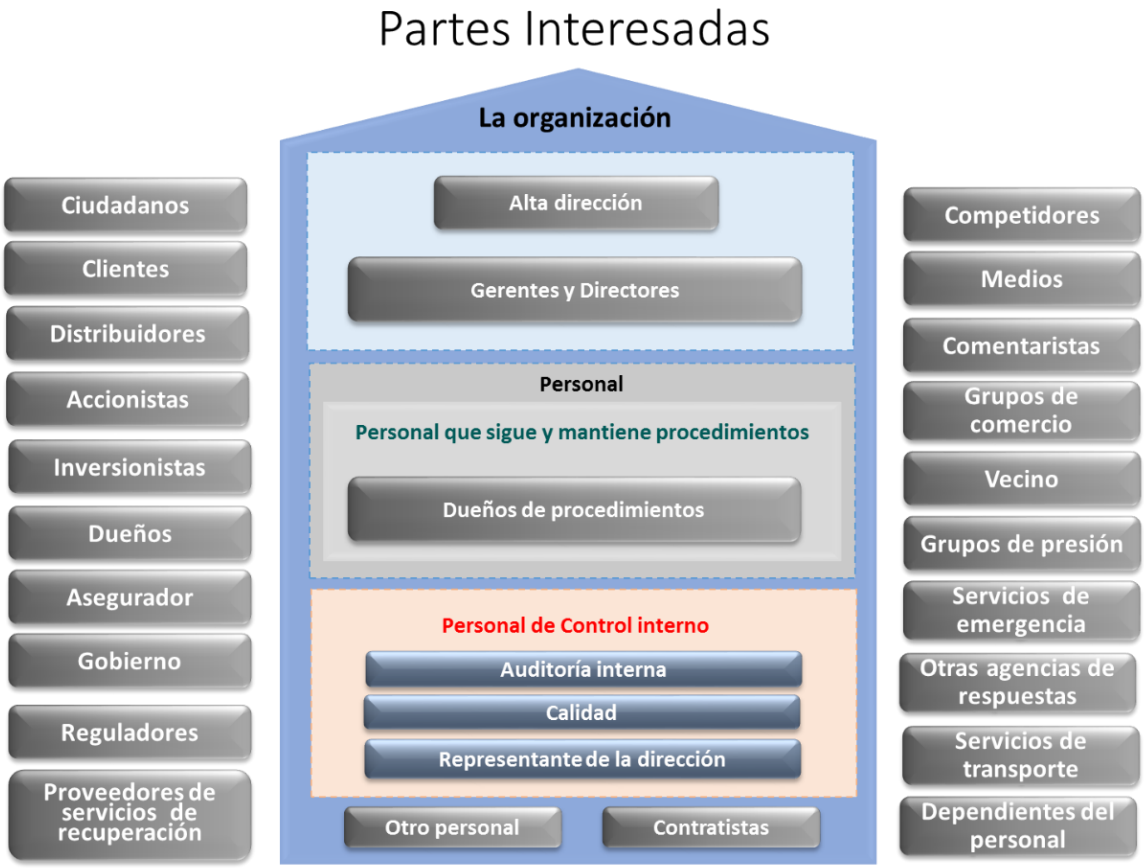


Ilustración 7. Partes interesadas. Adaptación del modelo de partes interesadas ISO 22301

Principios comúnmente aceptados de gobierno corporativo
Independientemente de las condiciones de la jurisdicción nacional y local, existen algunos principios (Tarantino, 2008) y temas de gobierno corporativo que han sido ampliamente adoptados a través de los años.

Derechos y trato justo de Accionistas. Las empresas tienen que escuchar las preocupaciones de los accionistas y respetar sus derechos. Esto incluye la comunicación abierta y bidireccional, así como la participación de los accionistas en las juntas directivas.

Funciones y responsabilidades de la Junta Directiva. Las juntas de gobierno corporativo robustas necesitan miembros expertos y enfocados que cuenten con cierto grado de experiencia. Es esencial contar con una mezcla de miembros independiente con credenciales fuertes y miembros internos con experiencia en la organización.

Comportamiento ético y profesional. Las empresas necesitan una cultura de cumplimiento y ética, no sólo un código de ética. Las voces de los directores se refuerzan por medio de acciones, no sólo con las palabras.

Transparencia y divulgación de información financiera. Las empresas necesitan procesos fuertes, bien documentados y de controles para proporcionar consistentemente una total transparencia en la información financiera. Los resultados necesitan seguir las normas aceptadas, las mejores prácticas y ser auditados por expertos internos y externos independientes. También es necesario defender y fomentar denunciantes internos, que a menudo son el mejor medio para descubrir errores y fraude en la información financiera.

Los controles internos son un componente clave de todos los regímenes para mejorar la gestión empresarial en general, para reducir los riesgos, y específicamente para proporcionar transparencia financiera consistente. Los debates sobre el alcance de los controles internos se han prolongado durante décadas, pero la mayoría está de acuerdo en que los controles internos que impactan en la caída de informes financieros están dentro del alcance del gobierno corporativo. En varios modelos para la gestión de riesgos se indica que la cuantificación y priorización de los riesgos es clave para el éxito de los controles.

Riesgos

La definición de riesgo comúnmente se refiere a la posibilidad de una pérdida o un daño creado por una actividad o por una persona. La gestión de riesgos busca identificar los activos o mediciones del riesgo para posteriormente desarrollar contramedidas para tratar o manejar el riesgo. Comúnmente esto no significa eliminar el riesgo, pero sí buscar mitigar o minimizar su impacto. El riesgo no debería verse como algo inherentemente malo. Todas las oportunidades vienen con algún grado de riesgo.
Una organización que es totalmente reacia al riesgo es probable que no sea muy atractiva para los inversionistas y puede ser condenada, en última instancia, al fracaso.
La norma ISO 31000 (ISO 31000, 2013), define como riesgo al efecto de incertidumbre sobre los objetivos; indica que un efecto es desviación esperada positiva y negativa, y los objetivos pueden tener diferentes aspectos como: financieros, de seguridad, de salud y ambientales, además de que pueden tener diferentes niveles como: estratégicos, organizacionales, por proyecto, por productos o por proceso. Los objetivos se caracterizan frecuentemente por asociarse a eventos potenciales y consecuencias o una combinación de estos, los cuales incluyen cambios en las circunstancias y una probabilidad de ocurrencia asociada.

Eventos

La norma define un evento como una ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas. Un evento también puede consistir en algo que no esté ocurriendo, y se identifica también como “incidente” o “accidente”. Los riesgos pueden ser internos o externos.

Ilustración 8. Gestión de riesgos de cumplimiento.

Fuente del riesgo

Como se muestra en la Ilustración 8, un elemento o la combinación de varios elementos con potencial intrínseco para dar lugar a un riesgo se conoce como la "*fuente del riesgo*". Esta fuente puede ser tangible o intangible. Algunas fuentes de riesgos pueden ser: relaciones comerciales y legales, circunstancias económicas, comportamientos humanos, eventos naturales, circunstancias políticas, aspectos tecnológicos y técnicos, actividades organizacionales o actividades individuales, entre otros. Estos eventos pueden ser positivos o negativos y pueden estar asociados a las partes interesadas, a las cuales se conoce como *"Agente del riesgo".*

Gestión del Riesgo

De acuerdo a la norma ISO 31000, la gestión de riesgos se define como las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo identificado.

La gestión de riesgos para la tecnología de la información (TI) es un reto cada vez mayor como requisito de cumplimiento, creciendo a un ritmo exponencial y con impacto en todas las áreas de TI. Las altas tasas de rotación para los Jefes de información (CIO) y los directores de tecnología (CTO) son evidencia de la creciente carga y tensión puesta en las organizaciones de TI. A medida que aumenta la presión sobre los responsables financieros, se hacen cada vez mayores las demandas de TI para mejorar la puntualidad, la exactitud y el costo de almacenamiento, de archivo, de cifrado, así como la búsqueda, la recuperación, la información financiera consolidada, las alertas, los documentos y la gestión de documentos, el correo electrónico y los controles de mensajería instantánea, etcétera.

La gestión de riesgos incluye el establecimiento del contexto, la identificación, el análisis, la evaluación, el tratamiento y el monitoreo del riesgo. La gestión de riesgos se utiliza principalmente en riesgos negativos.

Cumplimiento

Se define como cumplimiento el actuar en conformidad o de acuerdo a las leyes, regulaciones, protocolos o estándares establecidos. En México se cuenta con más de 800 Normas Oficiales Mexicanas (DGN, 2016) lo que significa que su cumplimiento es obligatorio. Adicionalmente, se cuenta con 289 leyes o regulaciones (DOF, 2014). El incremento de leyes y regulaciones se debe principalmente a la necesidad de proteger el bienestar de una nación y crecimiento económico. Por ello, el costo del incumplimiento es muy alto y puede tener consecuencias tangibles o intangibles.

Consecuencias

Todo riesgo tiene consecuencias para las partes interesadas. Estas consecuencias pueden ser positivas o negativas; el resultado depende de su impacto, del tratamiento y de los controles relacionados con el riesgo. Las consecuencias pueden ser de diferentes tipos, y las más comunes son: civiles, financieras, de reputación, legales u organizacionales.

Controles

El control según la norma ISO 31000 se define como la medida que modifica un riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica o cualquier otra acción que modifica un riesgo. Sin embargo, indica que no siempre los controles pueden cumplir con el efecto deseado, por ello es necesario su monitoreo y eficacia. Así como el riesgo y la oportunidad van de la mano, el cumplimiento y los controles internos van de la mano. Véase la Ilustración 9.

Responsable del control

De acuerdo con la norma ISO/IEC 27001 que establece los requisitos para un sistema de gestión de seguridad de la información, —donde uno de los elementos principales es la gestión de riesgos—es necesario asignar a un responsable del riesgo, quien regularmente es responsable también del mantenimiento de los controles asociados al riesgo.

Ilustración 9. Componentes de un control.

Tratamiento

Las opciones para el tratamiento de riesgos dependen en gran medida de las circunstancias y del nivel de riesgos. La norma ISO 31000 establece opciones de tratamiento de riesgo:

- Evitar el riesgo decidiendo si se continúa con la actividad que da lugar a un riesgo. Esta opción se utiliza comúnmente para riesgos negativos;
- Tomando o incrementando el riesgo de manera que se persiga una oportunidad. Opción de tratamiento para riesgos positivos;

- Mitigar el riesgo, modificando la probabilidad o consecuencias mediante el establecimiento de medidas de control. Opción para riesgos positivos y negativos;
- Compartir el riesgo con otras partes, mediante contratos o pólizas. Opción comúnmente utilizada para riesgos negativos;
- Retener el riesgo, es decir no se realizan acciones y se informa a las partes interesadas sobre la existencia del riesgo; opción para riesgos positivos y negativos.

La selección más apropiada para la opción de tratamiento de riesgo involucra el balance de los costos y esfuerzos de implementación contra los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros.

La norma ISO/IEC 27001 (ISO 27001, 2013) establece la necesidad de elaborar un plan de tratamiento de riesgo, sin embargo no existen requisitos normativos que indiquen qué elementos debería incluir este plan. Tarantino establece en su libro de gobernabilidad (Tarantino, 2008) que este plan debería contener información sobre:

A. Descripción del riesgo
B. Responsable del riesgo
C. Controles asociados al riesgo (de acuerdo al anexo A)
D. Medidas de control (incluyendo documentación para su mantenimiento y control)
E. Medición de su eficacia
F. Resultado de la eficacia del control
G. Referencias sobre las acciones correctivas o de mejora asociadas al riesgo

Esto ayuda a identificar claramente la relación entre la gestión del riesgo, la operación y la mejora de los controles asociados.

Eficacia

Los mecanismos para monitorear el control y la forma para medir su eficacia deberían estar documentados; para ello se identifica el indicador clave de desempeño, conocido como KPI, que puede estar relacionado a otros controles, incidentes o eventos significativos que pueden ocasionar un riesgo.

Herramientas para la Gestión de Riesgos de Cumplimiento

El manejo de sistemas de información es muy importante para los planes de la empresa. Contar con la tecnología adecuada es la parte fácil; el reto es adecuar la tecnología a las necesidades de la organización. Alcanzar un alto grado de adecuación es un aspecto principal para el éxito de la compañía. Cualquier decisión para invertir en algo de la empresa significa más que un compromiso de tiempo, esfuerzo y recursos financieros.

Actualmente existen en el mercado aplicaciones automatizadas que permiten el cumplimiento con alguno de estos estándares, sin embargo no permiten su integración con otros requisitos ni actualización constante.

A continuación se muestra un análisis de las herramientas existentes en el mercado que ayudan a la administración de un sistema de gestión de riesgos de cumplimiento:

Herramienta	Sitio	Descripción
SecureGRC	https://www.egestalt.com/securegrc-ent.html	Solución integral de monitoreo de seguridad de TI y gestión de cumplimiento que simplifica y reduce el tiempo necesario para la vigilancia de la seguridad, el cumplimiento normativo y el proceso de certificación.
ORCA GRC Suite	http://www.gcpglobal.com/orca-descripcion.php	La diversidad de soluciones en prevención de riesgos que ofrece ORCA y el respaldo de expertos multidisciplinarios para la entrega de servicios consultivos le permite diferenciarse de la mayoría de sus competidores dando como resultado la optimización operativa, la reducción de costos y la simplificación de las operaciones, así como el mejoramiento de la visibilidad y la toma de decisiones para propiciar un Gobierno Corporativo más eficiente.
SoftExpert GRC Suite	http://www.softexpert.es/gestion-gobierno-riesgos-reglamentaciones.php	Ofrece una estructura de gobernanza que posibilita una tomada de decisión eficaz y cambios comportamentales. Ofrece a la organización una implementación viable y eficiente de la gobernanza corporativa y de TI.
ARIS Risk & Compliance Manager	http://www.softwareag.com/corporate/solutions/ebpm/grc/overview/default.asp	Software para eficientar la gestión de riesgo del cumplimiento.

Tabla 3. Comparativa de aplicaciones GRC

Matriz de Evaluación de herramientas

La siguiente matriz muestra la evaluación de las herramientas contra las características básicas para un sistema de información de cumplimiento:

Herramienta	Servicios de	Búsqueda en	Enrutamiento	Administración	Soporte para	Digitalización de	Colabor	Soporte para	Gestión de	Gestión de	Flujos de	Gestión de	Gestión de	Integración con	Seguridad
SecureGRC	X	/	/	X	X	-	/	-	/	/	X	-	/	/	X
ORCA GRC Suite	X	/	/	X	X	/	X	/	/	X	X	-	X	/	X
SoftExpert GRC Suite	X	/	-	X	X	-	/	-	/	/	/	-	/	-	/
ARIS Risk & Compliance Manager	X	X	X	X	X	/	X	/	X	X	X	X	X	/	X

Tabla 4. Matriz de evaluación de herramientas GRC

X= Cumple /= Cumple parcialmente - = No cumple

El desarrollo de la herramienta a la medida fue descartado por la dificultad que significa asumir el riesgo en cuanto a la seguridad y el aseguramiento de la calidad por parte del departamento de TI, quienes debido a la saturación de trabajo no podrían dedicar el tiempo suficiente a ello. Por otra parte, la contratación de una empresa que desarrolle el software a la medida supera en tiempo y costos las ofertas de los sistemas licenciados.

Conclusión

Si bien el sistema con mejores calificaciones es *ARIS Risk & Compliance Manager*, éste no brinda una plataforma que cumpla con los objetivos de flexibilidad, escalabilidad y tipos de relaciones que se requieren.

Por lo tanto, el diseño de un sistema que permita dar trazabilidad al cumplimiento de objetivos, identificando las actividades que se realizan, los roles, las responsabilidades, así como los datos de entrada y salida de cada una de ellas, aportaría valor de forma importante al seguimiento y al cumplimiento de los objetivos organizacionales. Para ello será necesario el uso de una plataforma que ya cuente con las características de seguridad y aseguramiento de calidad requeridas.

En la Ilustración 1. Intereses de las partes interesadas y su alineación a los objetivos se observa cómo los intereses de las distintas partes interesadas pueden relacionarse con cada uno de los objetivos a los distintos niveles organizacionales, hasta llegar a los más operativos. De igual manera estos objetivos pueden ser medidos por medio de indicadores que provienen de los resultados de esas actividades operativas y que permiten a los niveles superiores conocer el estado del cumplimiento de sus objetivos con respecto de los resultados de las actividades de los niveles que están por debajo de ellos.

Douglas R. Hofstadter en Gódel, Escher y Bach: Una esterna trenza dorada (Hofstadter, 1980) Capítulo 9: "Mumon and Gödel" dice:

“Relying on words to lead you to the truth is like relying on an incomplete formal system to lead you to the truth. A formal system will give you some truths, but as we shall soon see, a formal system, no matter how powerful—cannot lead to all truths.”

Basarse en palabras para encontrar la verdad es como basarse en un Sistema formal incompleto para llegar a la verdad. Un sistema formal nos dará algunas verdades, pero como veremos, un sistema formal, no importando qué tan poderoso, no puede darnos todas las verdades.

Esta es la razon por la que las redes semánticas pueden acercarse más a la representación de los equemas de la vida real, más allá de los esquemas formales.

CAPÍTULO III: DIAGNÓSTICO Y RESULTADOS DEL ANÁLISIS

Tipo de estudio

El tipo de estudio considerando su **finalidad** es aplicado, pues contribuye a la resolución de los problemas derivados del mantenimiento de cumplimiento con diferentes leyes, normas y regulaciones. El **lugar de estudio** fue *In situ*, puesto que se realizó dentro del organismo encargado de evaluar la conformidad de normas mexicanas relacionadas con las tecnologías de la información.

En cuanto a las **fuentes de información**, también consideradas como **instrumentos**, se consideran dos tipos:

- *Documental:* Se consultaron diferentes metodologías y normas relacionadas con sistemas de gestión, aplicaciones automatizadas especializadas en la gestión, mejora continua, cumplimiento, gobernabilidad y riesgos.
- *De campo:* Se consultaron diferentes estudios relacionados con las diversas problemáticas de organizaciones privadas y gubernamentales, primordialmente mexicanas, relacionadas con la gestión y mantenimiento de cumplimiento de las diferentes leyes normas y regulaciones en el sector de tecnologías de la información. Adicionalmente, se hizo un análisis de las diferentes aplicaciones existentes en mercado enfocadas a la gestión de cumplimiento.

El **alcance** de la investigación está enfocado a cuatro tipos:

i. *Exploratorio:* Se buscaron las diferentes posibles causas que provocan la falta de cumplimiento constante y sus consecuencias, las cuales estuvieron basadas en los estudios y las experiencias de los auditores encargados de evaluar la conformidad.
ii. *Descriptivo:* El diseño de la metodología propuesta para la educación de la herramienta automatizada para resolver la falta de cumplimiento describe las propiedades y características de cada una las entidades.
iii. *Correlacional:* La metodología propuesta describe las diferentes relaciones entre las diferentes entidades y sus variables.
iv. *Explicativo:* Este ensayo intenta resolver la problemática mediante la identificación de su causa raíz.

El **universo muestra** en el que se basó este ensayo es el sector de tecnologías de la información del mercado mexicano, aunque para la investigación de las posibles soluciones se consultaron estudios internacionales. La selección de las variables de estudio está enfocada en:

1. La estructura de cumplimiento propuesta.
2. La identificación de los elementos que ayuden a mantener este cumplimiento y su relación con la estructura de cumplimiento.
3. La automatización de estos elementos por medio de una herramienta tecnológica.

Hipótesis de trabajo

H1: Si se automatizan los procesos de las organizaciones y los requisitos de cumplimiento, se incrementará el nivel de control de los mismos.
H2: Si se incrementa el nivel de control de los procesos y se relaciona con los requisitos de cumplimiento, se aumentará su nivel de cumplimiento.
H3: Cuanto mayor sea el nivel de cumplimiento de las organizaciones mexicanas, mayor será el nivel de competitividad y demanda de los servicios o productos que ofrecen, elevando la calidad de los mismos.

Características con las que debe contar el "Sistema de cumplimiento múltiple"

- Flexibilidad para presentar la información
- Facilidad de uso para la captura de información
- Escalabilidad para crecer con los requerimientos de la organización y complejidad de esquemas de cumplimiento
- Capacidad de administrar relaciones de un nodo a muchos otros nodos

Técnicas de análisis y procesamiento de la información

Uno de los problemas esenciales de la informática es la representación de la información. En un principio se pensó que podía diferenciarse netamente entre información y conocimiento, aquélla como el soporte material para almacenar éste (Shannon, 1949) y se dedicó al estudio de la información en el sentido puramente ingenieril del término; pero la dicotomía antes apuntada —útil desde el punto de vista metodológico y técnico— a veces se ha tornado con un sentido más ontológico, conduciendo al error de que cada uno de los términos de dicho binomio pudieran tener existencia independiente.

En particular, en los sistemas informáticos se han distinguido siempre dos tipos de información: programas y datos (Dahl, 1972) (Imperio, 1965) (Knuth, 1968); pero el conocimiento que en ellos subyace se ha considerado implícito. El programa expresa un algoritmo y a él se prestaba la máxima atención, debido, en general, a su complejidad frente a la relativa sencillez de los datos sobre los que actuaba, cuya organización estaba establecida en el interior del programa. Cuando se presentó la situación de que un mismo conjunto de datos debía ser usado por varios programas distintos, aquellos debían organizarse de tal manera que pudieran ser utilizados por los distintos programas y construirse estos teniendo en cuenta aquella organización.

Al principio, los criterios de organización de los datos se apoyaban en la forma de su almacenamiento físico y su localización, de forma que los programas pudieran encontrar y recuperar los datos necesarios para su ejecución, y así aparecen los bancos de datos. Pero la supeditación de la organización de los datos a la estructura física de su almacenamiento puso de manifiesto que la estructuración de los datos no debía estar determinada por la estructura física de la memoria de una computadora, por sus formas de acceso ni por la naturaleza formal de los datos, sino teniendo muy en cuenta el contenido semántico de los mismos.

Surgió la necesidad de organizar los datos atendiendo a su significación, a la semántica que relaciona los datos unos con otros; así surgieron las denominadas bases de datos (Borkin, 1980) (Date, 1981). Según el tipo de conexión entre ellos aparecieron distintas estructuras de datos y las bases de datos correspondientes se agruparon en tres grandes clases denominadas: bases jerárquicas (cuando su estructura es un árbol), en red (cuando la estructura en árbol se modifica permitiéndose relacionar algunos nodos de ramas distintas entre sí), o bases relacionales (cuando se emplea el uso de relaciones y del cálculo relacional y proposicional). De esta forma fue quedando más patente el uso del aspecto semántico de los datos en su organización. Con ello se establecía que las bases de datos son, en realidad, un modelo de representación del conocimiento de un dominio específico.

De esta manera, observamos cómo por medio de un camino con apariencia tan técnico como es el del desarrollo de las bases de datos, llegamos a concomitancias y espacios comunes con lo esencial de los lenguajes naturales: la representación del conocimiento.

Diversas ciencias han buscado lenguajes —o formas distintas al lenguaje natural— para representar el conocimiento (o parte del conocimiento) específico de las mismas; ejemplo de ello es el lenguaje de las matemáticas y, en alguna medida, el de la formulación química, pero es esencialmente la lógica simbólica la que de forma más clara deja patente la existencia de otros lenguajes distintos al natural, para expresar con más precisión y de forma más adecuada cierta parcela del conocimiento humano.

En la actualidad, uno de los problemas esenciales de la informática es precisamente la búsqueda de modelos que nos faciliten la representación del conocimiento (Bobrow, 1973) (ScHANK, 1973) (Trost, 1981). Las técnicas de la inteligencia artificial y, en particular, de los grafos semánticos nos brindan algunas herramientas para formular estos modelos.

Se describe ahora un sistema en el que se utilizan para la representación del conocimiento los grafos semánticos y al que se le ha denominado SENECA (*Semantic Networks for Conceptual Analysis*). Mediante este sistema se trata la representación del conocimiento dado sobre un dominio particular del saber, para lo que se necesita determinar con precisión el dominio de conocimiento elegido, descomponerlo en sus partes y en los elementos considerados esenciales para su descripción e integrar estos elementos mediante las relaciones significativas que podamos establecer entre aquellas partes y sus elementos.

Según el dominio que se quiera representar, las relaciones que intervengan en la integración serán específicas, pero tomadas de un conjunto más general. Es importante el cálculo o inducción de nuevas relaciones no establecidas *a priori* en la representación. Así, también es de interés el aspecto dinámico y variable de este tipo de representación en la definición de objetivos, conceptos y procedimientos.

Terminaremos con algunas reflexiones sobre la aparición de un nuevo nivel de lenguaje que se está produciendo en la actualidad y que significará un salto cualitativo de tanta envergadura como lo fue la aparición del lenguaje escrito con respecto del oral.

Bases de datos relacionales

La aparición de las bases de datos se debió al gran incremento en tamaño y en número de los bancos de datos. Por una parte, era necesario integrar los dispersos bancos de datos en un solo sistema, y por otra, que esta integración se hiciera teniendo en cuenta fundamentalmente los aspectos semánticos de la información almacenada.

La integración de la información presenta numerosas ventajas, como: reducir la redundancia de los datos almacenados, evitar la inconsistencia o contradicción que pueda presentarse entre los datos almacenados, facilitar la compartición de la información contenida en la base de datos, normalizar la forma de representar los datos, y facilitar la seguridad de la información (Fernandez, 1981) en el sentido de hacerla solo accesible a las personas autorizadas para ello. Por otra parte, las bases de datos toman una organización que proviene de la naturaleza de la información, del significado de los datos dentro del campo de aplicación específica.

Las bases de datos existentes suelen clasificarse, de acuerdo con la estructura con que se organizan los datos, en bases jerárquicas, bases en red, y bases relacionales. Las bases de datos jerárquicas son las que se ajustan a las normas establecidas por el grupo de trabajo de CODASYL (Committee, 1971) (Taylor, 1976) dedicado a Bases de Datos cuya estructura se ajusta a la de un árbol. La información contenida en la base está organizada por descomposiciones conceptuales sucesivas; para obtener un dato habrá que recorrer la rama que nos conduzca a él, y este recorrido nos agrega información sobre el propio dato. Las bases de datos en red modifican la estructura del árbol, permitiendo relacionarse a nodos que no están sobre la misma rama; de esta forma se logra flexibilizar en la rígida estructura del árbol y enriquecer así su contenido semántico.

Las bases relacionales (CoDD, 1979) utilizan para su organización la teoría matemática de las relaciones. Cada registro es considerado como una N-upla de una relación determinada. Con el cálculo de predicados o bien, con el álgebra de relaciones, podemos obtener datos con una gran versatilidad sin necesidad de que al incorporarlos a la base deba averiguarse todas las formas por las que puede ser localizado. Para acceder a la información contenida en una Base de Datos, suelen usarse lenguajes especiales llamados lenguaje de consulta (*Query Language*), con una estructura propia, que va desde lenguajes documentales altamente codificados, a lenguajes pseudo-naturales. La tendencia es que se puedan realizar consultas a las bases de datos en lenguaje natural [8]. En general, la información obtenida de una Base como respuesta a una consulta es utilizada como datos de un programa mediante el que se obtienen unos resultados. En la actualidad los programas a usar en cada caso se extraen de colecciones de programas, o paquetes de programas memorizados por el ordenador de forma análoga a como lo están los datos. Estas conexiones de programas reciben el nombre de bibliotecas de programas. En la actualidad se están buscando sistemas que integren a los Bancos de Datos y a las bibliotecas de Programas y que, tras una consulta realizada al ordenador, el sistema, de forma automática, localice los datos y los programas necesarios, y haga actuar estos sobre aquellos para obtener la respuesta. Los sistemas de este tipo se denominan Bases Activas de Datos (BAD), o Bases Dinámicas de Datos; en ellos, los programas como información que son, estarían incluidos entre los datos de la base. Los lenguajes de consulta deberán saber distinguir lo que es un programa (acción) del resto de la información almacenada en la Base.

Redes semánticas

Con el desarrollo de las bases de datos ha quedado patente que éstas deben ser modelos mediante los cuales se pueda representar en medios informáticos el conocimiento sobre los que actúan los programas. Sentado esto, el paso siguiente es estudiar directamente la representación del conocimiento (Anderson, 1977), con independencia de las características de las máquinas y de la forma que en ellas se memoriza la información.

Atendiendo a esta idea aparecen diversas metodologías mediante las que se pretende conseguir una representación del conocimiento, tomando en consideración esencialmente los aspectos semánticos de la información.

Toda esta búsqueda de formas de representación del conocimiento, motivada por imperativos pragmáticos, ha conducido a que las principales universidades, así como los laboratorios de investigación de las grandes empresas industriales, hayan emprendido proyectos de investigación sobre métodos de representación del conocimiento, conectados en la mayoría de los casos con problemas de lenguaje natural, utilizando técnicas de inteligencia artificial.

Toda esta actividad investigadora la engloba Winograd (Winograd, 1983) dentro de lo que denomina paradigma «cognitivo» —que considera compuesto de los paradigmas «generativo» y «computacional»— y que fundamenta en los siguientes principios:

1) El dominio propio de estudio es la estructura del conocimiento que posee un individuo que usa el lenguaje.
2) Este conocimiento debe entenderse como reglas formales relativas a estructuras de símbolos.

En el número de enero de 1982 del *SIGART Newsletter* —una publicación trimestral del Grupo de Interés Especial sobre Inteligencia artificial de la *Association for Computing Machinery*— se incluye una sección especial dedicada a Lenguaje Natural, en el que se reseñan 65 grupos de trabajo dedicados a la investigación de Procesamiento de Lenguaje Natural, la mayoría de los cuales utilizan sistemas de representación del conocimiento; esos grupos pertenecen a universidades como Berkeley, Cambridge U. K., Paris, Hamburgo, MIT, Illinois, Roma, Stanford, Turín, Yale, entre otras.
Dentro de este marco, se describe un sistema de representación del conocimiento, al que se le ha denominado SENECA (Garcia Camarero E. V., 1980) (Garcia Camarero E. , 1980), usando como herramienta la estructura formal llamada grafo semántico.

La técnica de redes semánticas ofrece un medio empírico de acceso a la organización cognitiva del conocimiento. Por tanto, puede proporcionar datos referentes a la organización e interpretación interna de los significantes. También indica cómo la información fue percibida individualmente en el curso de la composición del aprendizaje social y provee indicios fundamentales acerca de la tendencia a actuar basándose en ese "universo cognitivo". (Krech, Crutchfied, & Ballachey, 1975), suponen que el ambiente físico y el social aprendido por el individuo, facilitan el entendimiento del mundo social y solución de problemas. Por tanto, suponen que existen problemas sociales que provocan necesidades comunes a las personas, llevándolas a organizar el conocimiento ganado empíricamente con el fin de actuar eficazmente de manera colectiva frente a situaciones específicas.

Se trata de obtener la representación del conocimiento que se posee sobre un dominio del saber determinado; por tanto, la primera tarea a realizar consiste en determinar con precisión el dominio de conocimiento elegido, después, descomponerle en sus partes y en los elementos considerados esenciales para su descripción y por último integrarlo mediante las relaciones significativas que se puedan establecer entre aquellas partes o elementos.

La representación adoptada utiliza redes semánticas, es decir, grafos orientados con etiquetas en los vértices y en los arcos. Los vértices representan las partes o elementos del dominio considerado y los arcos las relaciones establecidas entre ellos. Las etiquetas asociadas a los vértices indican el tipo de elemento de conocimiento que tomamos en consideración y la etiqueta asociada a los arcos nos indica la relación establecida entre los elementos correspondientes al nodo origen y al nodo extremo.

La siguiente definición formal de red semántica se considera como un sistema formado por $G = (N, R, T_{N,} T_{R,} \Phi 1, \Phi 2)$

Consiste en un conjunto finito no vacío, N, de nodos, con una relación R definida entre ellos $R \subset N \times N$ cuyos elementos denominamos arcos, dos conjuntos de símbolos $T_{N,}$ y T_R denominados respectivamente etiquetas y relaciones, y dos funciones de asignación $\Phi 1$ y $\Phi 2$ tales que:

$\Phi 1: N \rightarrow T_{N,}$
$\Phi 2: R \rightarrow T_{R,}$

De hecho, la relación *R* debe considerarse como la unión de tantas relaciones Rα como símbolos α existan en T_R donde definimos

$R\alpha = \Phi_2^{-1}(\alpha)$

Al trabajar con este tipo de redes semánticas, las cuestiones que se presentan son:

1) Determinar los nodos (conceptos, objetos, características etcétera), que se encuentran en determinada relación con otros nodos.
2) Agregar nodos a la red mediante determinadas relaciones con otros nodos. Representando relaciones con elementos con su clase (*Es un*), Parte con un todo (*Tiene-un*).
3) Inferir relaciones entre nodos, no dadas explícitamente, en función de otras relaciones que los vinculan.

Mediante el punto 1 se pretende facilitar respuestas a consultas realizadas a la red semántica; en esta operación juega un papel importante la idea de proximidad semántica y que se desarrolla más abajo. El punto 2 indica una operación mediante la que se incrementa la información contenida en la red. El punto 3 alude a la posibilidad de establecer relaciones entre nodos no dadas explícitamente durante la construcción inicial de la red o durante los sucesivos incrementos producidos externamente pero que puede inferirse a partir de las relaciones ya establecidas. De igual forma se pueden suprimir relaciones en la representación que puedan ser inferidas posteriormente.

Resalta la idea de que al hablar de nodos de una red, se hace referencia de hecho a los conceptos, objetos, atributos, etcétera, en que se ha descompuesto el dominio de conocimiento con fines de representación. Véase la Ilustración 10. Representación del conocimiento de una red semántica.

Características de las redes semánticas:

- Redes complejas organizadas en jerarquías
- No tienen un vocabulario prefijado de representación
- Representación en procesamiento de lenguaje natural
- Formalismo muy limitado para dominios más complejos
- Fácil comprensión

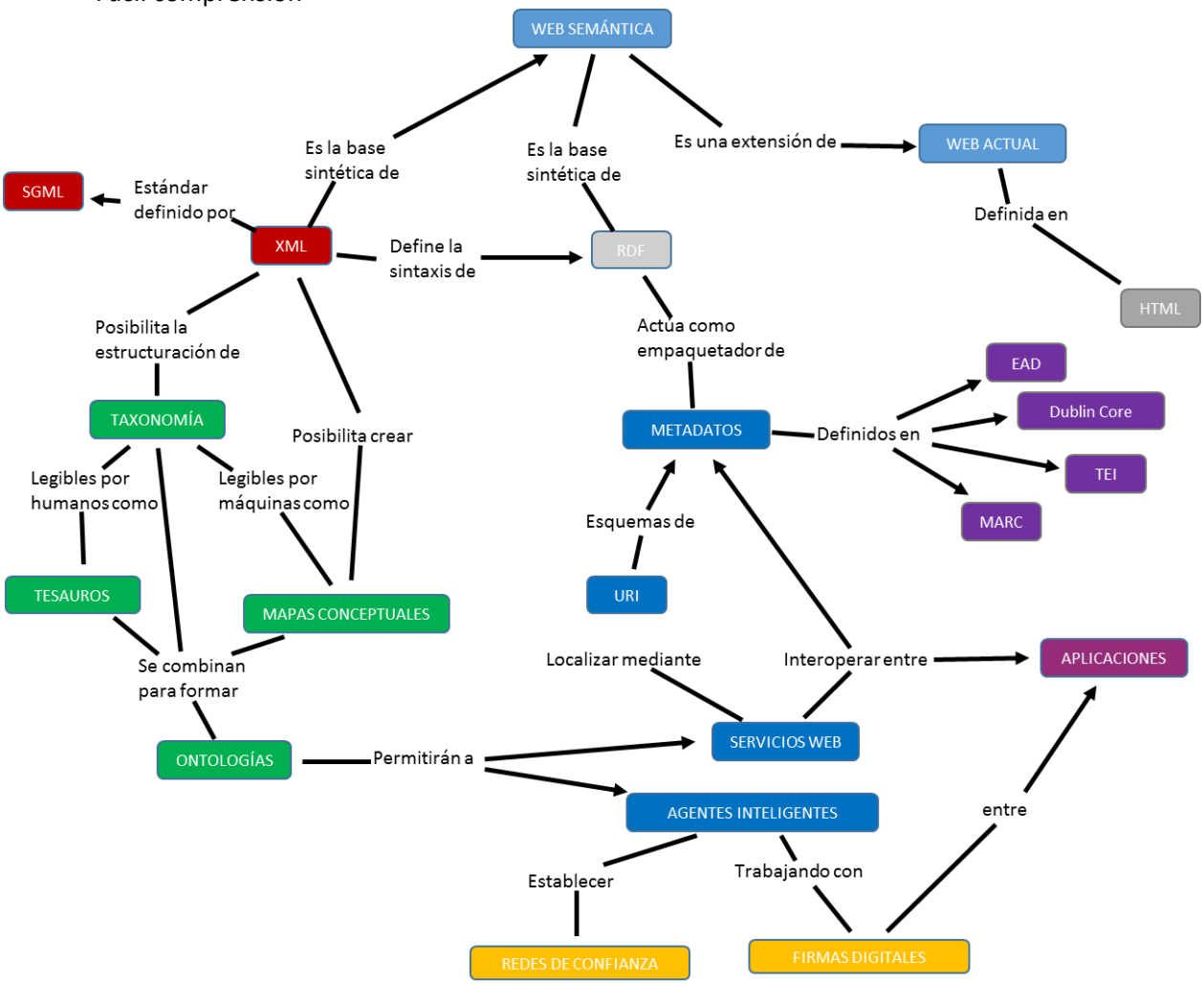


Ilustración 10. Representación del conocimiento de una red semántica.
(Keilyn Rodríguez Perojo y Rodrigo Ronda León, 2005)

Las redes semánticas son la base para muchos de los sistemas de inteligencia artificial modernos.

“Sometimes it seems as though each new step towards AI, rather than producing something which everyone agrees is real intelligence, merely reveals what real intelligence is not.” (Hofstadter, 1980)

A veces parece que cada paso hacia la inteligencia artificial, en vez de producer alqo en lo que todos estén de acuerdo que es realmente inteligente, meramente revela lo que no significa ser inteligente.

Funcionalidad

El objetivo de las redes semánticas es desarrollar una infraestructura para generar datos que las computadoras puedan entender, de tal forma que puedan ser compartidos y procesados no sólo por personas sino también por herramientas automatizadas.

Un ejemplo es realizar una búsqueda sobre todos los vuelos a Praga para mañana por la mañana usando un sistema de búsqueda universal. Lo ideal sería obtener unos resultados exactos sobre la búsqueda. Sin embargo la realidad es otra. La Ilustración 11 muestra los resultados inexactos que se obtendrían con el uso de cualquier sistema de búsqueda actual, el cual ofrecería información variada sobre Praga pero que no tiene nada que ver con lo que realmente el usuario buscaba. El paso siguiente por parte del usuario es realizar una búsqueda manual entre esas opciones que aparecen, con la consiguiente dificultad y pérdida de tiempo.

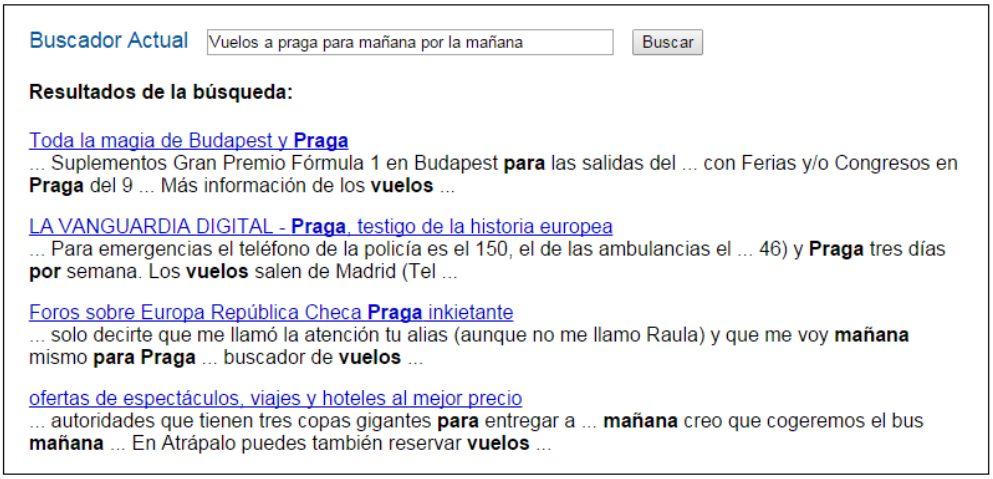


Ilustración 11. Resultados obtenidos con un Sistema de búsqueda normal.

Con la incorporación de una red semántica a este sistema, los resultados de la búsqueda serían exactos. La Ilustración 12 muestra los resultados obtenidos por medio de un buscador semántico. Estos resultados ofrecen al usuario la información exacta que estaba buscando. La ubicación geográfica desde la que el usuario envía su pregunta es detectada de forma automática sin necesidad de especificar el punto de partida, elementos de la oración como "mañana" adquirirían significado, convirtiéndose en un día concreto calculado en función de un "hoy". Algo semejante ocurriría con el segundo "mañana", que sería interpretado como un momento determinado del día. Todo ello por medio de una Red en la que los datos pasan a ser información llena de significado. El resultado final sería la obtención de forma rápida y sencilla de todos los vuelos a Praga para mañana por la mañana.

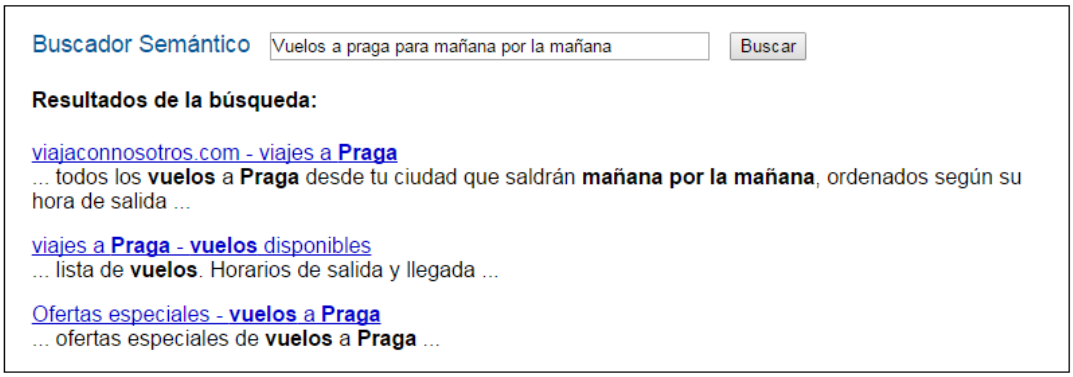


Ilustración 12. Resultados obtenidos con un sistema de búsqueda semántico.

Conclusión sobre Técnicas de análisis y procesamiento de la información

El esquema necesario para modelar el "Sistema de cumplimiento múltiple" será más fácilmente representado por medio de una red semántica de forma que se puedan mapear las relaciones entre los distintos nodos de información a modo de grafos con múltiples relaciones y posibilidades de interacción entre ellas.

CAPÍTULO IV: DISEÑO DEL SISTEMA DE CUMPLIMIENTO MÚLTIPLE

Diseño de flujos y estructura del Sistema de Cumplimiento Múltiple

En la Ilustración 13 se muestra el diseño de flujos para el Sistema de cumplimiento múltiple basado en la Metodología PHVA y los requisitos genéricos de los sistemas de gestión existentes actualmente.

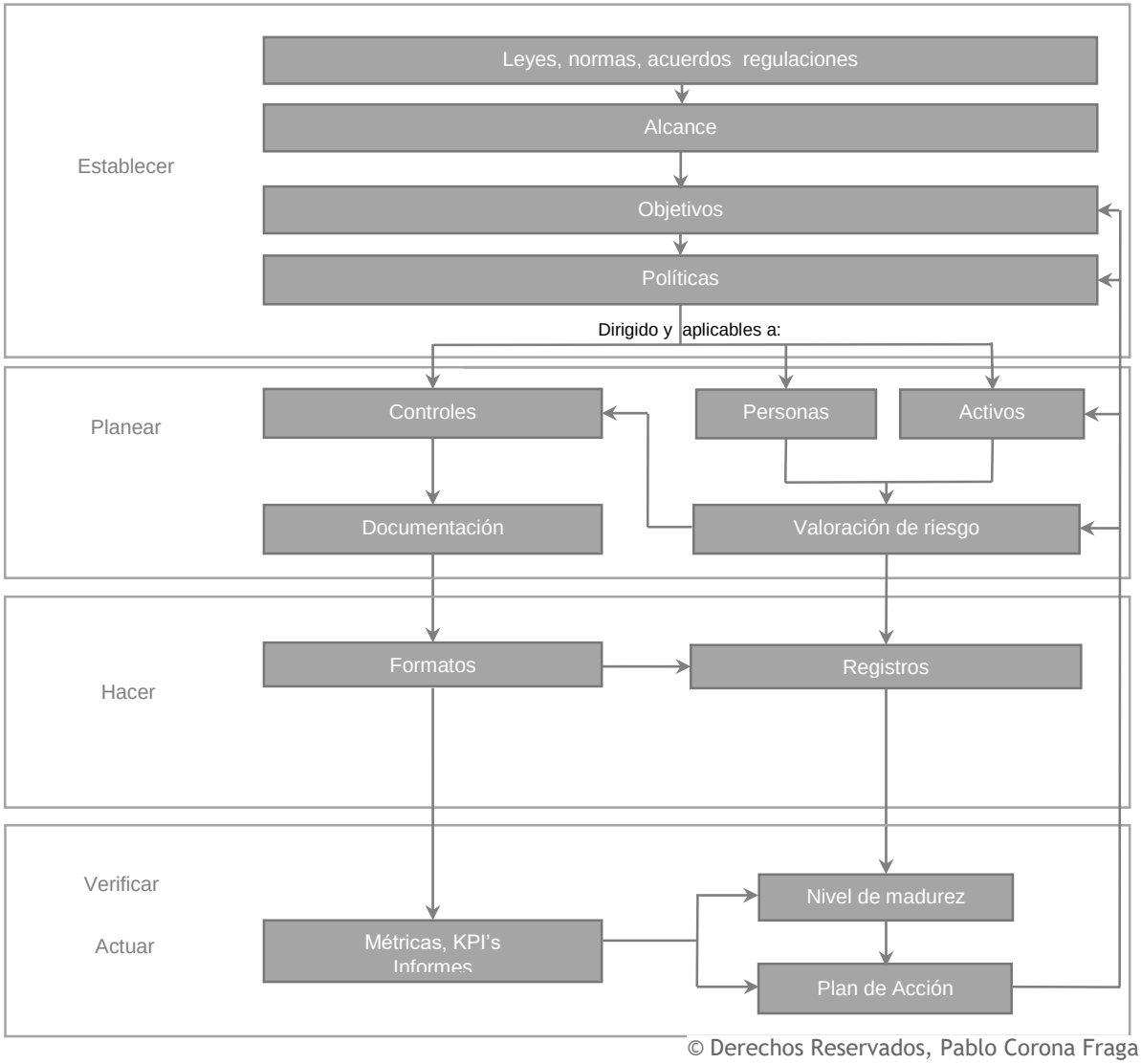


Ilustración 13. Diseño de flujos del sistema de GRC.

Descripción Metodológica

El diseño de la aplicación está basado principalmente en la metodología PHVA, también conocida como el "Ciclo de Deming", el cual se describe en la Tabla 5.

Etapa	Descripción
Establecer	Para esta aplicación se decide incluir esta etapa con el objetivo de documentar las leyes, normas, regulaciones alcances y políticas generales aplicables a la organización y objetivos a cumplir. Dentro de la metodología PHVA esta etapa está incluida en la etapa de planeación.
Planear	Se realiza la valoración de riesgos y con base a los resultados se diseñan y documentan las políticas específicas, procedimientos, objetivos, controles y métricas aplicables de acuerdo a las leyes, normas, regulaciones, alcances objetivos y políticas generales.
Hacer	Se implementa y opera según lo planificado. Se generan registros
Verificar	Con base a los registros se mide lo realizado contra las políticas, objetivos, procedimientos, controles, leyes, normas, regulaciones generales e informan los resultados.
Actuar	Se revisan los resultados de la verificación, se identifica el nivel de madurez, se planean y ejecutan acciones correctivas, preventivas y de mejora y se actualiza la valoración de riesgos y realizan mejoras a las políticas específicas, procedimientos, objetivos, controles, métricas

Tabla 5. Descripción del ciclo PHVA.

Descripción de Relaciones

A continuación, se describen las entidades de cada etapa, sus atributos y relaciones. Las relaciones se establecen de acuerdo al modelo Entidad-Relación. El cual describe lo siguiente:

Dado un conjunto de relaciones en el que participan dos o más conjuntos de entidades, la correspondencia de cardinalidad indica el número de entidades con las que puede estar relacionada una entidad dada.

Dado un conjunto de relaciones binarias y los conjuntos de entidades A y B, la correspondencia de cardinalidades puede ser:

- Uno a Uno: (1:1) Una entidad de A se relaciona únicamente con una entidad en B y viceversa (ejemplo relación vehículo - matrícula: cada vehículo tiene una única matrícula, y cada matrícula está asociada a un único vehículo).

- Uno a varios: (1: N) Una entidad en A se relaciona con cero o muchas entidades en B. Pero una entidad en B se relaciona con una única entidad en A (ejemplo vendedor - ventas).

- Varios a Uno: (N: 1) Una entidad en A se relaciona exclusivamente con una entidad en B. Pero una entidad en B se puede relacionar con 0 o muchas entidades en A (ejemplo empleado-centro de trabajo).

- Varios a Varios: (N: M) Una entidad en A se puede relacionar con 0 o muchas entidades en B y viceversa (ejemplo asociaciones- ciudadanos, donde muchos ciudadanos pueden pertenecer a una misma asociación, y cada ciudadano puede pertenecer a muchas asociaciones distintas).

Descripción de la Etapa "Establecer"

A continuación, se describe la primera etapa para el Sistema de cumplimiento múltiple. En esta etapa es donde se documentan los requisitos de leyes o regulaciones o normas. El sistema deberá tener un módulo para la actualización de estas leyes o normas. Es necesario que el sistema cuente con módulos para la gestión de usuarios de manera que solo personal autorizado pueda actualizar este módulo. Se debe contar con un módulo para el Sistema de cumplimiento múltiple de la organización. Este módulo deberá documentar los elementos, procedimientos o actividades que soporten el cumplimiento de requisitos. La relación entre ambos módulos es muy importante para una mejor trazabilidad y control del Sistema de cumplimiento múltiple. En la etapa de "Establecer" es necesario se documenten el alcance, objetivos, políticas objetivos del Sistema de Gestión de la organización. En la Tabla 6 se muestra mayor detalle de esta etapa.

Etapa	Entidad	Descripción	Atributos	Relaciones
Establecer	Ley regulación, norma, acuerdo o contrato	Documento de referencia que establece requisitos dentro de un determinado ámbito, que deben cumplirse.	∞Nombre de la ley regulación, norma, acuerdo o contrato	∞Nombre del Alcance ∞Nombre de Políticas Generales *Relación (1:N)*
			∞Requisito específico	∞Nombre de Política Específica
	Alcance	Documento que indica la extensión y límites que abarcará el cumplimiento, e incluye generalmente una descripción de las ubicaciones y las unidades y servicios de la organización.	∞Nombre del alcance	∞Nombre de Políticas Generales ∞Requisitos específicos ∞Objetivos *Relación (N:M)*
			Descripción general (Inmueble, Unidades, Servicios)	
	Objetivos	El propósito o meta de un Proceso, una Actividad o una Organización en su totalidad. Los Objetivos se expresan generalmente como metas medibles.	∞Nombre del objetivo	∞Nombre de Política General y/o especifica ∞Nombre del procedimiento ∞Nombre del control *Relación (N:M)*
			Descripción del objetivo	
			Medición	∞Métricas *Relación (1:N)*
			Recursos	∞Activos ∞Controles ∞Procedimiento *Relación (1:N)*
			Responsable	∞Personas (activo) *Relación(1:1)*

			Fecha límite	
	Políticas	Documento formal que contiene las intenciones y expectativas de gestión. Las Políticas se utilizan para dirigir las decisiones, y asegurar un desarrollo e implementación coherente y apropiado	∞Nombre de la política	*De acuerdo al tipo*
			Tipo: General Descripción General	∞Nombre de la ley regulación, norma, acuerdo o contrato *Relación (N:M)*
			Tipo: Especifica Descripción General	∞Requisitos específicos *Relación (N:M)*
	Dirigido y/o Aplicables	Entidad que servirá de enlace para indicar la aplicabilidad de las políticas	*Relacionar a los elementos, al menos una relación* ∞	Activos Controles Procedimiento *Relación (1:N)*

Tabla 6. Etapa de Establecer de la herramienta GRC.

Descripción de la Etapa "Planear"

Los servicios que brindan valor al negocio deberán ser identificados en función de su aportación, los activos que los soportan y los riesgos a los que están sometidos. En la Ilustración 14 se muestra el diseño de cumplimiento y riesgos por activos y servicios.

Ilustración 14. Diseño de cumplimiento y riesgos por activo y servicios.

En esta etapa se documenta la información de los activos, las amenazas y vulnerabilidades asociadas a los activos; las relaciones entre los elementos permitirán una trazabilidad necesaria para gestionar los riesgos y la mejora de los activos.

En la Tabla 7 se muestran a detalle las entidades de esta etapa.

Etapa	Entidad	Descripción	Atributos	Relaciones
Planear	Activo	Es cualquier elemento que tiene valor para la organización. Hay muchos tipos de activos, que incluyen: a)La documentación; b)El software, como los programas de las computadoras; c)Los recursos físicos, por ejemplo una computadora; d)Los servicios; e)El personal y sus cualidades, habilidades y experiencia;	∞Nombre del activo Tipo de activo ∞Valor del activo Valor de la confidencialidad *Valor numérico de 1 a 3* Valor de la integridad *Valor numérico de 1 a 3* Valor de la disponibilidad *Valor numérico de 1 a 3*	∞Nombre del riesgo ∞Nombre de la amenaza ∞Nombre de la vulnerabilidad *Relación (N:M)*
			Propietario del activo	∞Personas (activo) *Relación(1:1)*
	Valoración de riesgo	**Valoración de riesgo** Proceso general de la **identificación del riesgo**, el **análisis de riesgo** y la **evaluación de riesgos.** **Identificación del riesgo** Proceso de encontrar, reconocer y describir los riesgos. **Análisis de riesgo** **Evaluación de riesgos** Proceso de la comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable	∞Nombre del riesgo Descripción del riesgo ∞Nombre de la vulnerabilidad Descripción de la vulnerabilidad Valor de la vulnerabilidad *Valor numérico de 1 a 3* ∞Nombre de la amenaza Descripción de la amenaza Valor de la amenaza *Valor numérico de 1 a 3*	∞Activos *Relación (N:M)*
			∞Probabilidad de ocurrencia Frecuente (1 /20 días) | Periódico (1/60 días) | Regular (1/90 días)	∞Nombre de la amenaza *Relación(1:1)*
			∞Riesgo estimado Fórmula matemática del Riesgo estimado = Evaluación de la Vulnerabilidad * Evaluación de la Amenaza * Valor de activo *Probabilidad	∞Nombre de la vulnerabilidad ∞Nombre de la amenaza ∞Probabilidad de ocurrencia *Relación(1:1)*
			∞Nivel de riesgo Es la categorización del riesgo estimado de acuerdo a los siguientes parámetros Alto 1 a 81 | Medio 82 a 163 | Bajo 164 a 243	∞Riesgo estimado *Relación(1:1)*
			∞Impacto Fórmula matemática = Nivel de riesgo * impacto	∞Nivel de riesgo ∞Probabilidad de ocurrencia *Relación(1:1)*
			∞Opción de tratamiento	∞Impacto

			Es la categorización del resultado del impacto de acuerdo a los siguientes parámetros: Aceptar (1), Mitigar (2, 3, 4) Transferir (6), Evitar (9)	*Relación(1:1)*

Tabla 7. Etapa de Planear de la herramienta GRC.

Características de los controles

Los controles deberán enfocarse a la detección y en la medida de lo posible estar suficientemente automatizados para garantizar que los objetivos de control se cumplen, los objetivos de control deberán estar alineados con el plan de tratamiento de riesgo. Véase la Ilustración 15.

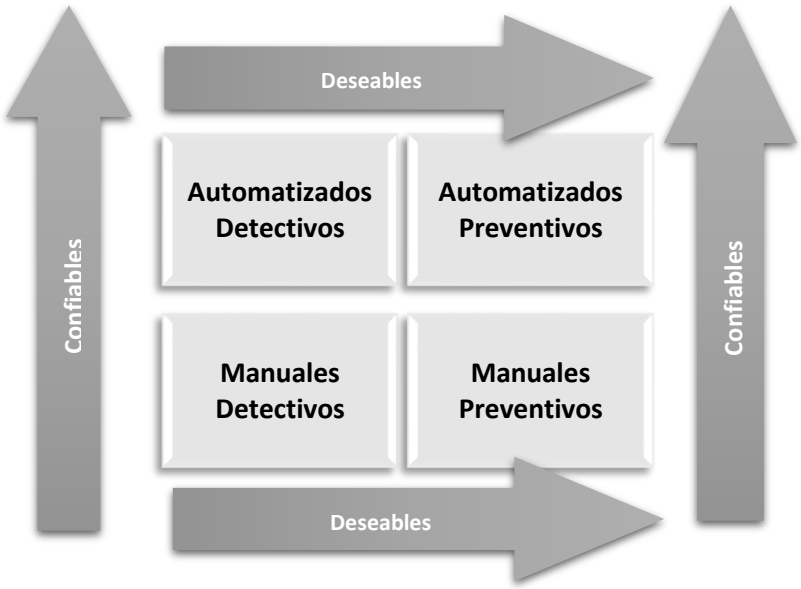


Ilustración 15. Características de los controles.

En la Tabla 8 se muestran los atributos y relaciones de la entidad enfocada a los controles.

Etapa	Entidad	Descripción	Atributos	Relaciones
Planear	Control	Medio de gestión del riesgo que incluye políticas procedimientos directrices, prácticas o estructuras de la organización, que pueden ser de naturaleza administrativa, técnica, de gestión o legal	Nombre del control	Requisito normativo *Relación(N:M)*
			Descripción del control	Requisito normativo *Relación(N:M)*
			Tipo	Administrativo Técnico Físico *Relación(1:1)*

		Actividades, tecnología, activo o prácticas asociados a un control que ayuda a mitigar, eliminar o evitar algún riesgo.	Nombre de medidas internas	Nombre del control *Relación(1:1)*
			Descripción de la Medida de medidas internas	Nombre del control *Relación(1:1)*
			Operación de la Medida de Seguridad	Políticas *Relación(N:M)* Manuales *Relación(N:M)* Procedimientos *Relación(N:M)* Actividad *Relación(N:M)*
			Mantenimiento de la medida de seguridad	Políticas *Relación(N:M)* Procedimientos *Relación(N:M)* Actividad *Relación(N:M)*
			Plan de tratamiento	Riesgos asociado *Relación(N:M)* Tipo de control *Relación(1:1)* Nivel de madurez *Relación(1:1)* KPIs *Relación(N:M)*

Tabla 8. Etapa de Planear – Controles.

En esta fase, es necesario que los controles se asocien con la documentación para su operación y mantenimiento de manera que puedan gestionar estos riesgos. La documentación puede ser políticas, procedimientos o actividades, a la cual se le debe asignar un responsable para su realización.

En la Tabla 9se describen los atributos relacionados con las entidades Política y Procedimiento.

Etapa	Entidad	Descripción	Atributos	Relaciones
Planear	Política	Documento formal que contiene las intenciones y expectativas de gestión. Las Políticas se utilizan para dirigir las decisiones, y asegurar un desarrollo e implementación coherente y apropiado de los Procesos, Estándares, Roles, Actividades, Infraestructura etc.	Nombre de la política especifica	Requisito normativo *Relación(N:M)*
			Descripción de la política	
			Relaciones	Requisito normativo *Relación(N:M)* Control *Relación(N:M)*
	Procedimiento	Forma especificada de llevar a cabo una actividad o un proceso	Nombre del procedimiento	Nombre de la política especifica *Relación(N:M)*
			Descripción del procedimiento	
			Actividades	Responsable *Relación(N:M)*
			Relaciones	Requisito normativo *Relación(N:M)* Control *Relación(N:M)* KPI's *Relación(N:M)*

Tabla 9. Etapa de Planear –Documentación.

Descripción de la Etapa "Hacer"

En esta etapa se generan los registros que demuestren el complimiento, para ello se elaboran formatos o plantillas electrónicas. En la Tabla 10 se muestran las características de estas entidades.

Etapa	Entidad	Descripción	Atributos	Relaciones
Hacer	Formato	Documento que estandariza la manera en la que es presentada la información.	Nombre del Formato	Políticas *Relación(N:M)* Procedimientos *Relación(N:M)*
			Descripción del formato	
	Registro	Un Documento que contiene el resultado u otro tipo de salida desde un Proceso o Actividad. Los registros son la evidencia de que una Actividad tuvo lugar, y podría ser en papel o formato electrónico.	Nombre del registro	Nombre del Formato *Relación(N:N)*
			Periodo del registro	
			Registro	Fuente de datos *Relación(N:M)*

Tabla 10. Etapa de Hacer.

Descripción de la Etapa "Verificar"

En esta etapa la herramienta debe permitir la configuración de indicadores clave de desempeño (KPI) y con ello permitir la automatización de informes. Se consideran niveles de madurez para los procesos y gestión. La Ilustración 16 muestra los niveles de madurez de los procesos que se describen a continuación:

Documentado: Se cuenta con procesos documentados, pero no se muestra evidencia de su implementación.

Implementado: Las actividades documentadas se están realizando, pero no hay evidencia de la operación del proceso.

Registros: El proceso está documentado, implementado y se cuentan con registros que demuestren su operación.

Mejora Continua: Se realizan mejoras al proceso documentado de acuerdo a la información que muestran los registros.

Control y Monitoreo: Se revisa constantemente que la operación se realice de acuerdo a lo documentado y se detectan desviaciones.

Automatizado: La operación del proceso se realiza de forma sistemática, de acuerdo al proceso documentado.

KPI e informes: Se establecen indicadores e informes que permiten visualizar su desempeño.

Ilustración 16. Niveles de madurez para la automatización de procesos.

La automatización de los procesos y actividades deberá ser un objetivo en el mediano plazo, de forma que la organización dedique menos tiempo a las tareas de gestión y más tiempo a las actividades que le generan réditos. La Ilustración 17 y la Tabla 11 muestran los Niveles de madurez para la gestión.

Niveles de madurez para la gestión

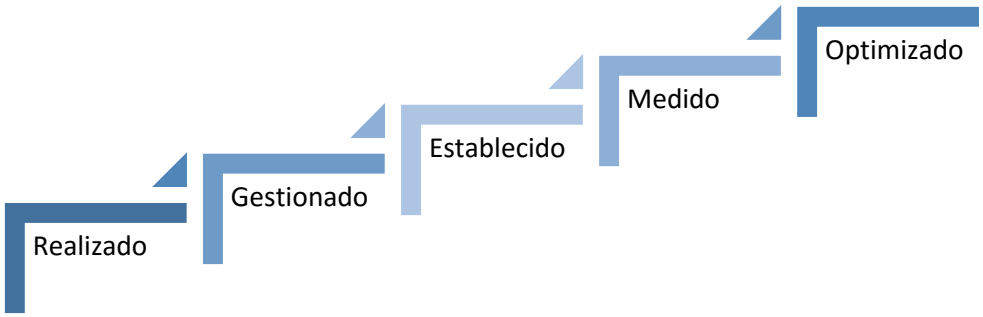


Ilustración 17. Niveles de madurez para la gestión.

Niveles de Madurez	Descripción
Realizado	Se realizan las actividades de trabajo pero no se sabe cómo.
Gestionado	Se demuestra que las actividades cumplen con lo documentado.
Establecido	Las actividades realizadas cumplen con los requisitos legales o normativos.
Medido	Se mide el nivel de cumplimiento de las actividades realizadas.
Optimizado	Se realizan mejoras a las actividades de acuerdo a su nivel de cumplimiento.

Tabla 11. Niveles de madurez para la gestión.

Establecimiento de métricas para el monitoreo del desempeño

Para poder monitorear el desempeño del proceso y la gestión es necesario establecer qué información se requiere para iniciar el proceso, conocer qué información genera o sus salidas, identificar qué se debe medir o informar por medio del establecimiento de métricas, mecanismos para medirlo e identificar aquellas métricas que sean clave para el desempeño, es decir indicadores clave de desempeño, KPI, y finalmente establecer metas con respecto a los KPI identificados. Véase la Ilustración 18.

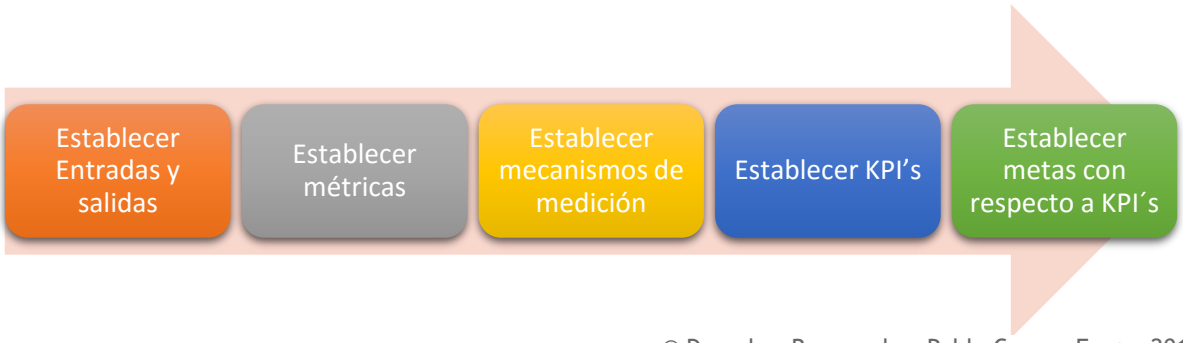


Ilustración 18. Métricas para el monitoreo del desempeño.

Establecimiento de acciones correctivas / preventivas

Con base en el monitoreo de los indicadores establecidos, es necesario implementar acciones que atiendan las desviaciones o que permitan relizar cambios en la organización que la lleven a la mejora contínua. Estas acciones están representadas en la Ilustración 19.

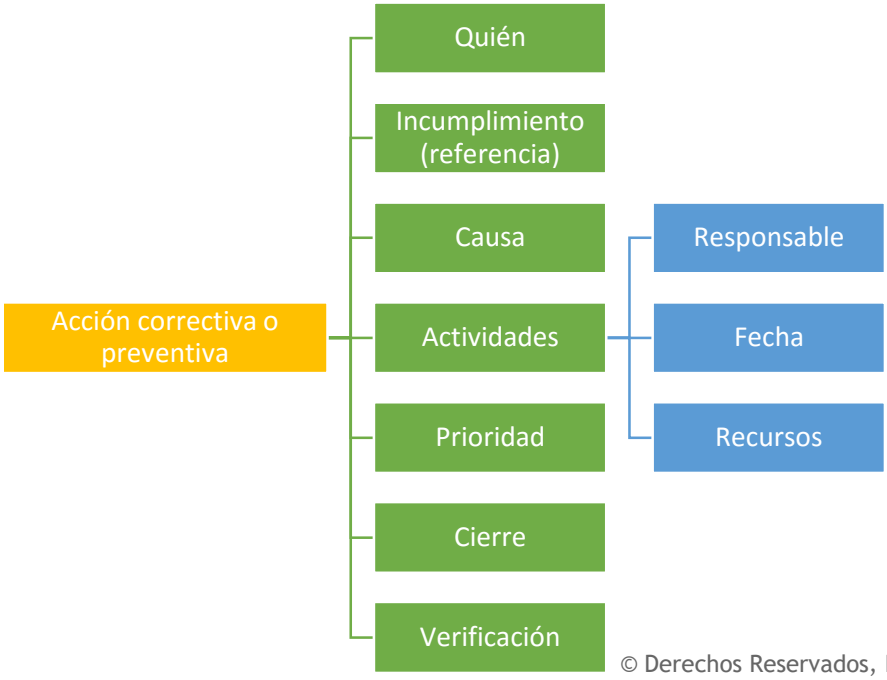


Ilustración 19. Establecimiento de acciones correctivas / preventivas.

Cuando el sistema haya presentado desviaciones con respecto a los Factores Críticos de desempeño, deberán implementarse acciones correctivas o preventivas. Las acciones correctivas deben tener un responsable que vele por que las acciones se lleven a cabo y se eliminen las desviaciones. Debe estar referenciado el requisito incumplido el cual puede ser una actividad, un proceso, un procedimiento, una ley o una regulación afectada; debe indicar la causa por la cual no se cumplió con el requisito; es necesario se establezca su nivel de importancia o prioridad y que incluya un plan de acción que

cuente con actividades, responsables y los recursos que se requieren para llevarlo a cabo. Finalmente es necesario realizar y verificar si las acciones fueron realizadas.

En la Tabla 12 se describe la etapa de “Verificar” del diseño propuesto.

Etapa	Entidad	Descripción	Atributos	Relaciones
Verificar	KPI’s	Métricas claves que sirven para medir el desempeño de los Procesos, los Servicios, Controles o las Actividades. Los KPIs deberían ser seleccionados de tal forma que aseguren el control de la Eficiencia, la Efectividad, y la Rentabilidad.	Nombre de la métrica	Procedimiento *Relación(1:1)*
			Descripción de la métrica	
			Mecanismo de medición	Plan de tratamiento *Relación(N:M)*
	Informes	Documento que contiene detalles de uno o más KPIs y tendencias de acuerdo a los registros generados de los procesos, los Servicios, controles o las Actividades y sirve para informar el desempeño del cumplimiento.	Nombre del reporte	KPI’s *Relación(1:N)*
			Descripción del reporte	
			Frecuencia de medición	Periodo del registro *Relación(1:1)*
			Nombre de la Fuente de datos	KPI’s *Relación(N:M)*
			Tendencias	Registro *Relación(N:M)*
			Conclusiones	Tendencias *Relación(N:M)*

Tabla 12. Etapa de Verificar.

En la Tabla 13 se describe la etapa de “Actuar” del diseño propuesto.

Etapa	Entidad	Descripción	Atributos	Relaciones
Actuar	Acciones correctivas y preventivas	Acción correctiva: Es la acción para eliminar la causa o reducir la probabilidad de ocurrencia de una no conformidad detectada u otra situación inesperada. Acción preventiva: Es la acción para evitar o eliminar las causas o reducir la probabilidad de ocurrencia de una no conformidad detectada u otra situación indeseada.	∞Folio	∞Nombre del reporte *Relación(N:M)* Conclusiones
			Tipo de acción Correctiva |Preventiva	
			Nombre de la acción	∞Folio *Relación(1:1)*
			Referencia del requisito incumplido	*Relación(1:N)*
			Prioridad Alta |Media | Baja	∞Folio *Relación(1:1)*
			Responsable	∞Personas (activo) *Relación(1:1)*
			Acciones	∞Número consecutivo del Plan de acción, Fecha de inicio *Relación(1:N)*

			Verificación	Plan de acción *Relación(1:1)* KPI's
			Cierre	Plan de acción Fecha de cierre *Relación(1:1)*
	Plan de acción	Propuesta detallada que describe las Actividades y Recursos necesarios para la consecución de una desviación u objetivo.	Número consecutivo	Acciones *Relación(N:1)*
			Fecha de inicio	
			Fecha de cierre	Cierre *Relación(1:1)*
			Descripción de la actividad	Acciones *Relación(1:N)*
			Responsable de la actividad	∞Personas (activo) *Relación(1:1)*
			Recursos necesarios para la actividad	Descripción de la actividad *Relación(1:1)*

Tabla 13. Etapa de Actuar.

Requerimientos para la parametrización del Sistema de Cumplimiento Múltiple

La definición más general alrededor de la noción de requerimiento es la que brinda el Instituto de Ingeniería Electrónica y Eléctrica (IEEE) (Institute for Electronics and Electrical Engineers, 1997)

(1) Una condición o necesidad de un usuario para resolver un problema o alcanzar un objetivo.
(2) Una condición o capacidad que debe estar presente en un sistema o componentes de sistema para satisfacer un contrato, estándar, especificación u otro documento formal.
(3) Una representación documentada de una condición o capacidad documentada como las descritas en (1) y (2).

Existen diferentes tipos de requerimientos, pero únicamente se consideraron requerimientos no funcionales (Somerville, 2004). Estos requerimientos son restricciones sobre los servicios y funcionalidades ofrecidos por el sistema. Estos incluyen restricciones en el tiempo que se debe demorar un proceso, restricciones sobre el proceso de desarrollo y estándares. Los requerimientos no funcionales aplican usualmente sobre el sistema como un todo. Estos normalmente no aplican a características o servicios particulares del sistema.

El nivel de descripción de los requerimientos fue alineado a la definición de negocio de Wiegers (Wiegers, 2003), que los define como aquellos requerimientos que representan objetivos de alto nivel para la organización o el cliente que requiere el producto. Estos requerimientos son la necesidad principal por la cual se empieza la construcción o mejora del producto. Estos requerimientos se caracterizan por ser descritos de manera muy generalizada en términos de beneficios o necesidades de la organización y se expresan en un lenguaje natural. En ocasiones son llamados los objetivos del software. En ese sentido la Tabla 14 describe los requerimientos no funcionales para el Sistema de Cumplimiento Múltiple.

REQUERIMIENTOS	DESCRIPCIÓN
DESEMPEÑO	El sistema debe estar disponible y funcionar dentro de la organización y desde cualquier navegador. Debe permitir concurrencia de usuarios.
SEGURIDAD	El sistema debe controlar el acceso y privilegios de los administradores y usuarios. Debe proteger la integridad de los datos que procese el sistema y deben existir mecanismos que protejan la conexión con otros sistemas o base de datos. El sistema debe contar mecanismos contra administradores y usuarios que ingresen desde internet. Debe contar con mecanismos de validación de información.
ESCABILIDAD	El sistema debe permitir la adición de nuevas funcionalidades, modificar o eliminar las funcionalidades existentes.
FACILIDAD DE USO	El sistema debe ser intuitivo de manera que sea fácil de usar. El sistema debe emitir mensajes de error que permitan la identificación de problemas.
INTEROPERABILIDAD	El sistema debe permitir el intercambio y relación de información entre los diferentes módulos, base de datos y otros sistemas en tiempo real.

Tabla 14. Requerimientos de la Herramienta de Cumplimiento Múltiple.

Arquitectura y componentes tecnológicos de una Red Semántica

Los principales componentes de la web semántica son los metalenguajes y los estándares de representación XML, XML Schema, RDF, RDF Schema, OWL y SPRAQL. Véase la Ilustración 20

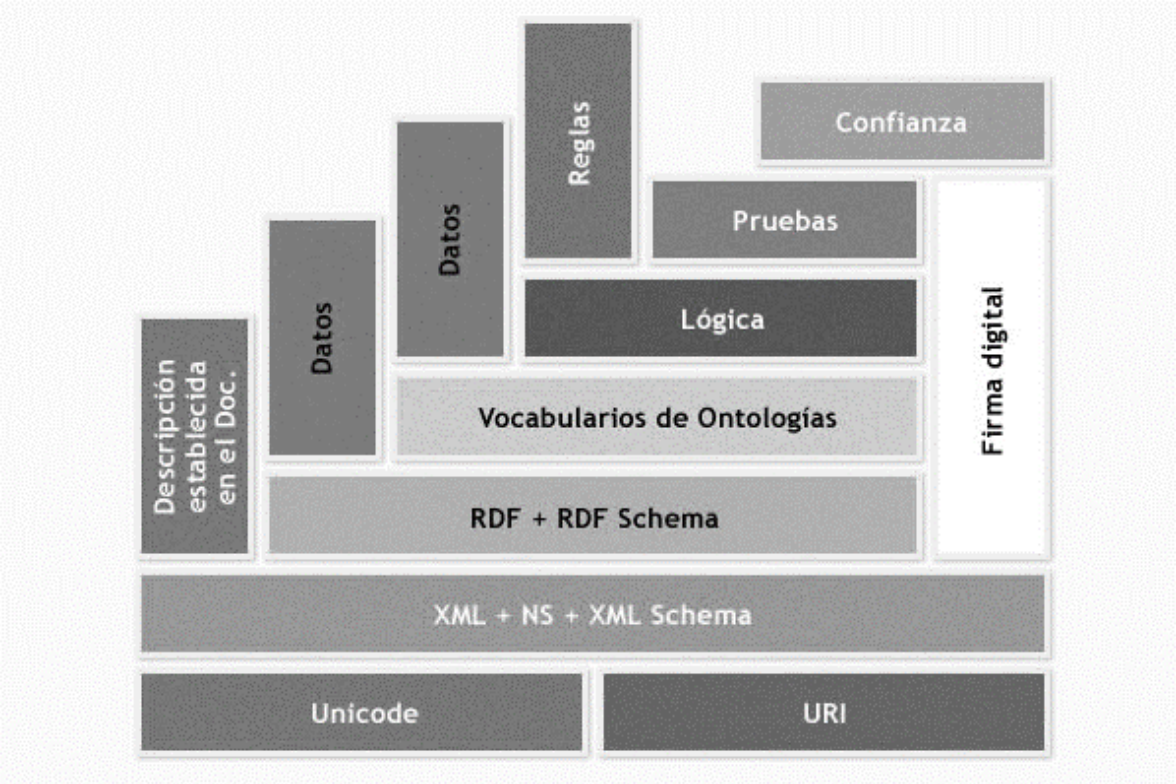


Ilustración 20. Componentes de un Red Semántica. (Berners-Lee, s.f.)

Las capas primarias de esta tecnología están elaboradas con los códigos URI (cuya función es identificar los recursos XML), Unicode y Namespace. Mediante RDF y RDF Schema se agrega la información descriptiva mientras que las ontologías definen la relación entre los metadatos. Las capas superiores están conformadas por las reglas y la lógica que permiten que los agentes automáticos procesen información extremadamente compleja (Cacheiro y Lago, 2008).

URI, *Uniform Resource Identifier* o *Identificador de recursos uniformes*, por sus siglas en inglés, es una cadena de caracteres que identifica los recursos de una red de forma unívoca. La diferencia respecto a un localizador de recursos uniforme (URL) es que estos últimos hacen referencia a recursos que, de forma general, pueden variar en el tiempo. Dentro de una red semántica se utiliza para identificar los recursos XML.

XML, eXtensible Markup Language o Lenguaje de marcas extensible, por sus siglas en inglés, es un lenguaje de marcas desarrollado por el *World Wide Web Consortium (W3C)* utilizado para almacenar datos en forma legible; proporciona una sintaxis básica para la estructura del contenido dentro de los documentos, pero sin asociar restricciones semánticas sobre el significado del contenido.

XML Schema, estándar que define la estructura de los documentos XML que estén asignados a tal esquema y los tipos de datos válidos para cada elemento y atributo. Este estándar permite proporcionar y restringir la estructura y el contenido de los elementos dentro de los documentos XML.

RDF, Resource Description Framework o Marco de descripción de recursos es un lenguaje simple para expresar modelos de datos que se refiere a los objetos y sus relaciones. RDF proporciona información descriptiva sobre los recursos que se encuentran en la web. Es similar a los enfoques de modelado conceptual clásicos como entidad-relación o diagramas de clases, ya que se basa en la idea de hacer declaraciones sobre los recursos —en particular, recursos web— en forma de expresiones sujeto-predicado-objeto. Estas expresiones se conocen como triples en terminología RDF. El sujeto indica el recurso y el predicado denota rasgos o aspectos del recurso y expresa una relación entre el sujeto y el objeto. Un modelo basado en RDF puede representarse con la sintaxis XML.

RDF Schema o Esquema RDF, es un vocabulario para describir las propiedades y las clases de los recursos RDF con una semántica para establecer jerarquías de generalización entre dichas propiedades y clases.

SPARQL *SPARQL Protocol and RDF Query Language*. Es un protocolo y un lenguaje de consulta que permite hacer búsquedas sobre los recursos de la web semántica utilizando distintas fuentes de datos.

OWL, *Web Ontology Language, o Lenguaje de Ontologías Web* es un mecanismo para desarrollar vocabularios específicos y definir ontologías que permiten asociar recursos. Una ontología define los términos utilizados para describir y representar un área de conocimiento determinada y también da cuenta de la relación entre estos conceptos.

SemanticWebBuilder (SWB) es una suite de productos que sirven como plataforma para el **desarrollo de aplicaciones y portales semánticos**, creada por el Fondo de Información y Documentación para la Industria, INFOTEC, Centro de Investigación y Desarrollo Tecnológico del CONACYT.

La suite *SemanticWebBuilder* está conformada por una serie de herramientas que permiten la evolución de los sitios web convencionales (sin significado), hacia los portales que cumplan con la visión de la Web Semántica (con significado), permitiendo exponer en **formatos estándar como RDF todo el conocimiento generado**, además de contar con un Modelo (ontología) que permita el intercambio de esta información entre los diferentes sistemas.

SWB Platform es el núcleo de la suite de herramientas. Es el principal componente de la plataforma para la construcción de modelos semánticos, como base para la definición de una ontología general, la cual sirve de referencia para la **creación acelerada de aplicaciones semánticas** (nuevos productos).

Esta plataforma permite definir en una ontología (**OWL**) la estructura de información, la arquitectura de objetos, sus dependencias y su representación gráfica, de forma que mediante estos elementos se pueda ejecutar un proceso automatizado que genera el código del modelo de objetos definido y su persistencia en una base de datos semántica (basada en **RDF**). Véase Ilustración 21

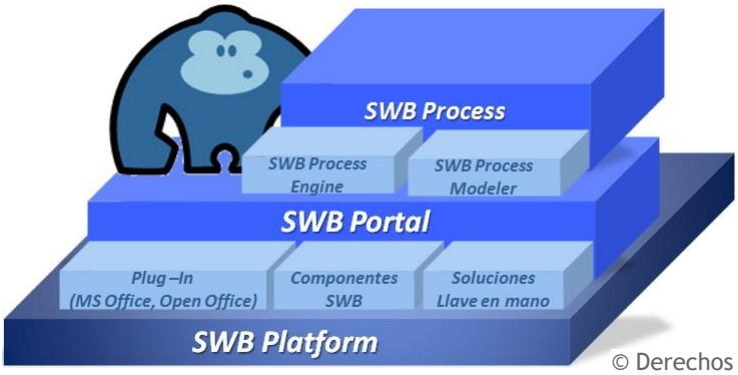


Ilustración 21. Estructura del Sistema Semantic Web Builder.

SemanticWebBuilder se compone de un conjunto de herramientas que **dan significado a la información** obtenida de fuentes internas o externas, para su posterior integración, filtrado y presentación. *SemanticWebBuilder* nos permitirá:

1. Avanzar en la ruta Semántica hacia la Web 3.0.
2. Incorporar elementos de colaboración como redes sociales, comunidades, blogs, wikis.
3. Agilizar la implementación de portales con el uso de sitios predefinidos.
4. Reducir los tiempos de desarrollo gracias a los componentes para crear aplicaciones basadas en modelos semánticos.
5. Mejorar la clasificación y búsqueda de información para que pueda ser compartida entre diferentes organizaciones, estableciendo así una federación de información.

La ontología (lenguaje) de la plataforma incluirá elementos que podrán ser reutilizados para la creación de nuevos productos:

1. Administración de usuarios (repositorios)
2. Seguridad (reglas, roles, grupos y permisos)
3. Navegación (sitios y páginas)
4. Diseño gráfico (plantillas, diseño de interfaz)
5. Administración de componentes (aplicaciones, contenidos, estrategias)
6. Dispositivos
7. Lenguajes

La plataforma permite definir en la ontología la estructura de información, la arquitectura de objetos, sus dependencias y su representación gráfica, de forma que mediante estos elementos se pueda **ejecutar un proceso automatizado que permita generar el código del modelo de objetos definido y su persistencia en una base de datos semántica** (basada en RDF).

SWB es una plataforma de Código abierto desarrollada por INFOTEC. Por la naturaleza de INFOTEC (centro de investigación), y buscando como principal objetivo el apoyo a la comunidad más que el beneficio económico, se tomó la decisión de liberar el producto bajo un esquema de código abierto con la finalidad de:

1. Apoyar al crecimiento de la industria de TI en el país.
2. Incrementar el potencial de penetración en el mercado.
3. Abrir una oportunidad de negocio a la iniciativa privada.
4. Buscar el apoyo de la comunidad para crecer y evolucionar la herramienta.

Esta decisión está encaminada a brindar a la sociedad en general la oportunidad de contar con herramientas que le permitan el desarrollo de nuevas oportunidades de negocio en distintos ámbitos.

Análisis de los requerimientos y diseño de las pruebas

Para la creación de un sistema de GRC utilizando una red semántica es necesario crear una ontología que defina las entidades y relaciones que dan cumplimiento a los esquemas, y que permita establecer vínculos con otros sistemas de almacenamiento, procesamiento y respaldo de la información, tanto a nivel físico como electrónico.

> «El término 'ontología' es utilizado en filosofía para hablar acerca de una 'teoría sobre la existencia' y fue adoptado por la comunidad de inteligencia artificial para definir una categorización y las relaciones entre sus términos.
>
> En el contexto de la ingeniería web, una ontología representa una taxonomía y un conjunto de reglas de inferencia. La taxonomía define las clases de objetos y de relaciones entre dichos objetos. Las clases, subclases y relaciones entre entidades son herramientas de gran potencia para usarlas en la Web Semántica.
>
> De acuerdo con Sabino Pariente, Maestro en Ciencias de la Computación y consultor de desarrollo en Infotec, «Las ontologías están encargadas de proporcionar el medio para representar el conocimiento contenido en la web y así trabajar con conceptos y relaciones.»
>
> «La Web semántica requiere necesariamente de ontologías para representar conocimiento, ya que son el mecanismo que permite exponer el modelo conceptual que existe detrás de cada página o recurso Web», asegura (Pariente, 2013).
>
> «Las ontologías tienen los siguientes componentes que servirán para representar el conocimiento de algún dominio:
>
> **Conceptos**: son las ideas básicas que se intentan formalizar; pueden ser clases de objetos, métodos, planes, estrategias, procesos de razonamiento, etcétera.
>
> **Relaciones**: representan la interacción y enlace entre los conceptos del dominio, y suelen formar la taxonomía del dominio; por ejemplo subclase-de, parte-de, parte-exhaustiva-de, conectado-a, etcétera.
>
> **Funciones**: son un tipo concreto de relación donde se identifica un elemento mediante el cálculo de una función que considera varios elementos de la ontología. Por ejemplo, pueden aparecer funciones como categorizar-clase, asignar fecha, etcétera.
>
> **Instancias**: se utilizan para representar objetos determinados de un concepto.
>
> **Axiomas**: son teoremas que se declaran sobre relaciones que deben cumplir los elementos de la ontología. Por ejemplo: "Si A y B son de la clase C, entonces A no es subclase de B", "Para todo A que cumpla la condición C1, A es B", etcétera. Estos últimos componentes, los axiomas, permiten junto con la herencia de conceptos, inferir conocimiento que no esté indicado explícitamente en la taxonomía de conceptos.»

La ontología propuesta consiste en la definición de conceptos como Esquemas de cumplimiento, Normas, Regulaciones, Leyes, Objetivos, Intereses de partes interesadas, requisitos, objetivos, actividades, riesgos, controles, entregables, activos principales y secundarios, así como las relaciones que existen entre ellos.

Con base en las relaciones entre los objetivos e indicadores de los distintos niveles de la organización, que se muestran en la Ilustración 1, podemos identificar la forma en la que estas relaciones ayudan a dar trazabilidad y visibilidad en el cumplimiento de objetivos por medio de la medición de los distintos indicadores por cada nivel.

Uno de los elementos que se identificó como muy importante al momento de crear la ontología es el rol que juegan los activos en la organización. Existen distintas formas de clasificar los activos, en este caso serán definidos por la aportación al cumplimiento de los objetivos organizacionales, de forma que los que están directamente ligados a estos serán llamados activos primarios. Estos activos son los que dan valor a la organización y ayudan directamente al logro de los objetivos organizacionales y al cumplimiento de los intereses de las partes interesadas. Comúnmente pueden ser elementos no tangibles como la información, procesos, secretos de negocio, conocimientos, etcétera, como se muestra en la ilustración Ilustración 22.

Ilustración 22. Ejemplos de activos primarios.

Los activos secundarios son aquellos que soportan a los activos primarios, ya sea como medios de almacenamiento, respaldo, transmisión, comunicación, procesamiento y hasta las instalaciones mismas donde se realizan las actividades organizacionales. Algunos ejemplos podemos encontrarlos en la ilustración Ilustración 23.

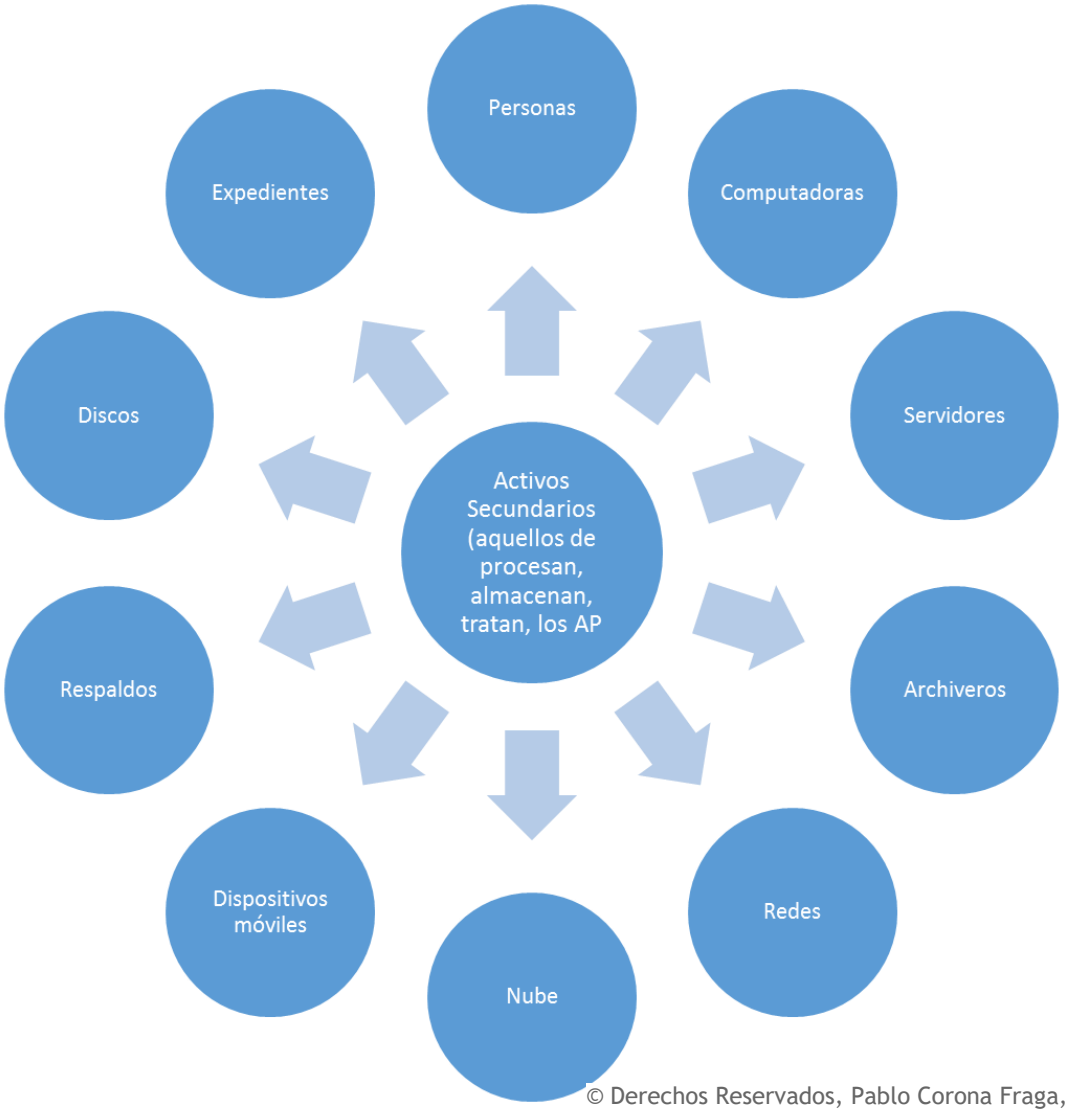


Ilustración 23. Ejemplos de activos secundarios

En la ilustración Ilustración 24podemos identificar las relaciones que existen entre un activo primario, en este caso un expediente médico, con los activos secundarios que lo soportan a lo largo de su ciclo de vida.

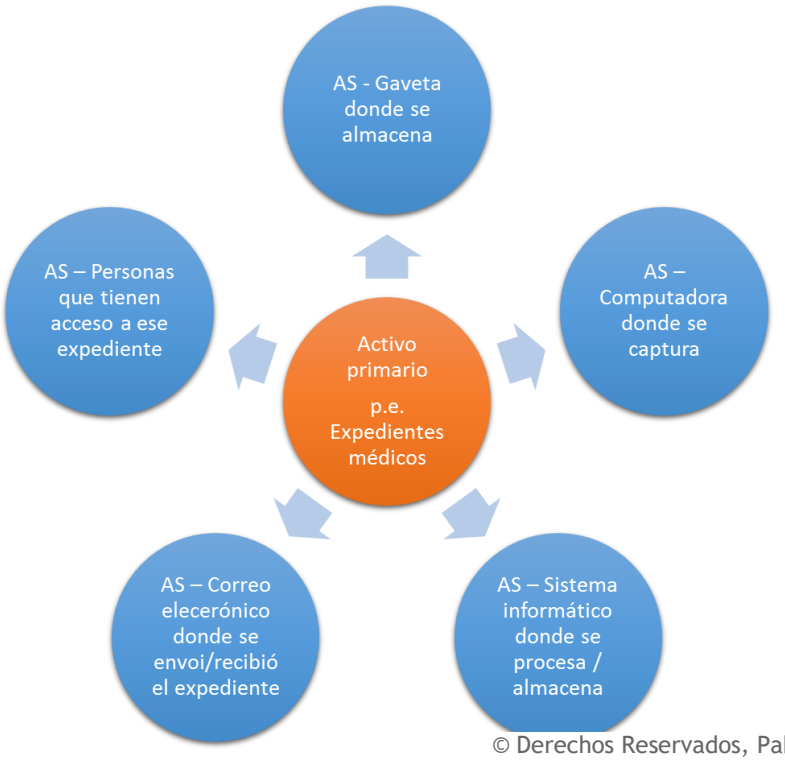


Ilustración 24. Relacion entre activos primarios y secundarios.

Para la creación de esta ontología se siguieron los pasos recomendados por (Noy & McGuinness, s.f.):

1) Determinar el dominio y el alcance de la ontología
    1. ¿Cuál es el dominio que cubrirá la ontología?
       La Gobernabilidad, Riesgos y Cumplimiento
    2. ¿Para qué vamos a usar la ontología?
       Para el diseño de un sistema de Gobernabilidad, Riesgos y Cumplimiento soportado por una Red Semántica en una plataforma web.
    3. ¿Qué tipo de respuestas debe responder la ontología?
       Qué relaciones existen entre los activos principales y secundarios de una organización. Cuál es la aportación que brinda cada activo al cumplimiento de los objetivos organizacionales. Cuáles son los riesgos asociados a los objetivos organizacionales y de qué forma son tratados mediante controles, actividades, políticas o proveedores.

4. ¿Quién va a utilizar y dar mantenimiento a la ontología?
   Deberá ser mantenida y adaptada a las necesidades de cada organización que busque implementarla.

2) Considerar la reutilización de otras ontologías
   Se reutilizaron las ontologías swb.owl y swb.owl que son la base para el *Semantic Web Builder* creado por Infosec.
3) Listar los términos importantes en la ontología
   - Esquema de cumplimiento
   - Parte interesada
   - Objetivo
   - Riesgo
   - Control
   - Actividad
   - Responsable
   - Proveedor

4) Definir las clases y la jerarquía de clases
   Ver anexo 1

Otro elemento que fue necesario definir fueron las relaciones de tipo N-arias (W3C Working Group, s.f.) dado que no todas las relaciones en la ontología eran del tipo "is-a" que se utiliza para relaciones jerárquicas. En este caso se creó una propiedad de clase llamada "isRelatedTo" para incluir distintos tipos de relaciones no jerárquicas como:

mitiga: la relación que existe entre un control y un riesgo.

esResponsable: la relación que existe entre una persona que es responsable de una actividad.

generaIncertidumbre: la relación que existe entre un riesgo y el objetivo sobre el cual genera incertidumbre.

cumpleCon: la relación que existe entre un objetivo y la aportación que da para el cumplimiento de un requisito.

Estas relaciones son importantes ya que facilitan la representación de esquemas más complejos y podrían ser complementadas con los tipos de relaciones que se adapten a las necesidades de la organización.

Douglas Hofstadter en su libro Gödel, Escher y Bach: Una eternal trenza dorada (Hofstadter, 1980) dice:

"Perhaps the most concise summary of enlightenment would be: transcending dualism. … Dualism is the conceptual division of the world into categories … human perception is by nature a dualistic phenomenon—which makes the quest for enlightenment an uphill struggle, to say the least."

Talvez la forma más concisa de resumir la iluminación (entendimiento) sería trancender el dualismo. … El dualismo es la división conceltual del mundo en categorías…la percepción humana es por naturaleza un fenómeno dualista, lo que hace la búsqueda de la iluminación una batalla de subida, por decir lo menos.

Capítulo 9: "Mumon and Gödel"

Este dualismo es el que impide que las relaciones jerárquicas describan adecuadamente la complejidad de los sistemas y elementos que utilizamos en las organizaciones actualmente.

5) Definir las propiedades de las clases
   Objetivo: nombre, fecha; isRelated: responsable, actividad(es), requisito
   Actividad: nombre, fecha inicio, fecha fin; isRelated: responsable, actividad, objetivo, recurso, control, registro.

6) Definir las limitaciones de las propiedades
   Las fechas fin de las actividades deben ser mayores que las fechas inicio

Esta ontología, incluyendo sus elementos y relaciones quedan descritas en la Ilustración 25 y definidas en el esquema en formato OWL/XML en el Anexo 1.

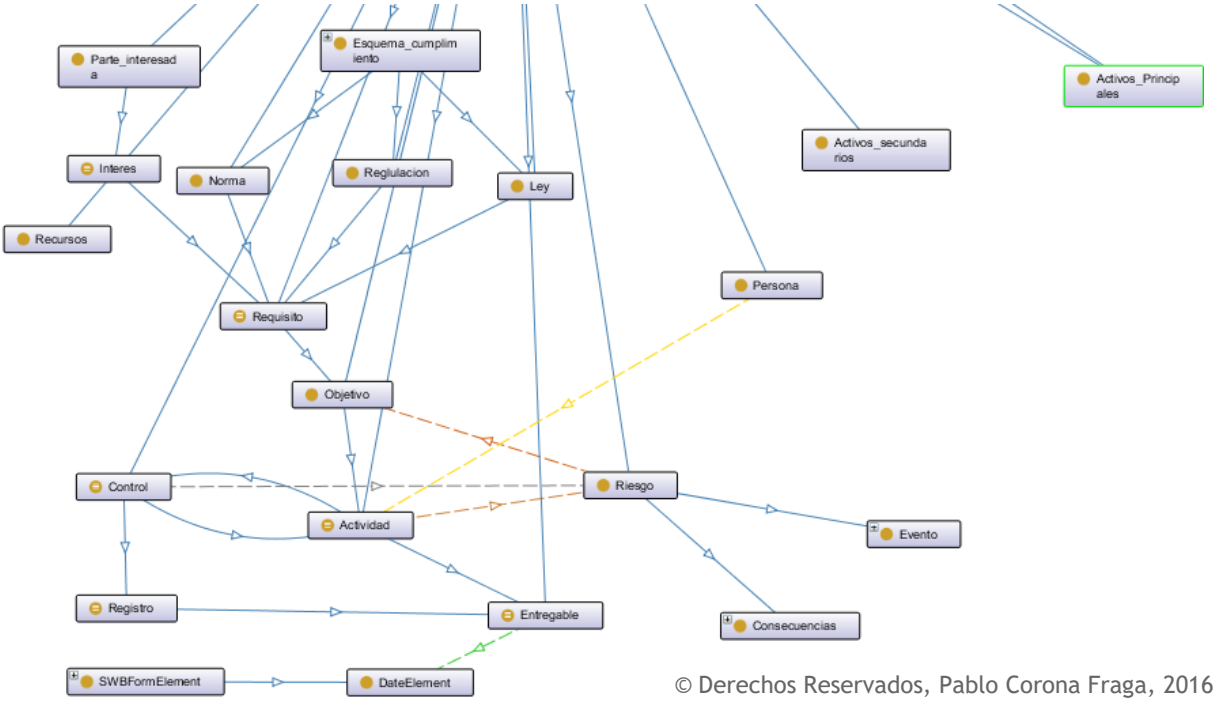


Ilustración 25. Descripción gráfica de la ontología propuesta.

CONCLUSIONES Y RECOMENDACIONES

En el mercado existen distintas herramientas que permiten definir y dar seguimiento a esquemas de GRC, sin embargo cada una tiene sus propias limitaciones, ventajas y desventajas, por lo que se decidió la creación de una ontología propia y el uso del *Semantic Web Builder* (SWB) para su uso diario.

El uso de SWB facilita la generación de una herramienta de GRC debido a que ya cuenta con un portal, una herramienta de diseño y módulos de importación y personalización que facilitan el desarrollo y mantenimiento de nuevos modelos ontológicos. Sin embargo es importante mencionar que si bien esta herramienta es más versátil y no requiere de una inversión inicial por costos de licenciamiento o pólizas de mantenimiento, es necesario que se inviertan recursos en conocer su funcionamiento, adaptarla a las necesidades organizacionales mediante la creación de nuevos modelos ontológicos, así como la definición y captura de los procesos organizacionales en la herramienta, lo que requiere de recursos, por lo que se recomienda que se analicen sus Costos totales de propiedad (PIERDANT, 2006) para asegurar su idoneidad.

La creación de una ontología adecuada a las necesidades de cada organización, que permita documentar, dar seguimiento y visualizar el esquema de Gobernabilidad, Riesgos y Cumplimiento de una organización, requiere del entendimiento de las relaciones entre los objetivos e indicadores en los distintos niveles y roles organizacionales descritos en la Ilustración 1. Intereses de las partes interesadas y su alineación a los objetivos se identifica cómo éstos se aterrrizan en actividades de los niveles inferiores de la jerarquía organizacional, así como en el sentido inverso se puede dar seguimiento al cumplimiento de dichos objetivos con base en las actividades.

Dado que el riesgo se define como “incertidumbre sobre los objetivos”, el cumplimiento de cada uno de los requisitos impuestos por los intereses de las partes interesadas, apoya en la consecución de objetivos de un nivel superior o inferior y los riesgos están relacionados con las actividades que soportan cada objetivo.

Las relaciones que rigen la interacción entre los elementos descritos no siempre pueden ser definidas por medio de relaciones jerárquicas, por lo que fue necesaria la creación de otro tipo de relaciones que dieran flexibilidad a la interacción entre elementos.

Cada organización podrá reutilizar esta ontología para definir sobre ella nuevos elementos o nuevos tipos de relaciones que permitan definir elementos particulares de su contexto organizacional.

En el anexo 2 se describen los pasos para la instalación de las herramientas utilizadas para la creación de la ontología (*Protegé*), la visualización (*NavigOWL y OWLViz*) y la generación de portal basado en una red semántica (*Semantic Web Builder*).

Futuros trabajos pueden centrarse en la integración de herramientas de medición y monitoreo automatizado, de forma que se pueda alimentar de manera sencilla la información que soporta la toma de decisiones. Por ejemplo herramientas como las propiestas por el National Isntitute for Standards and Technology (NIST) de los Estados Unidos de América, que han desarrollado el Security Content Automation Protocol (SCAP http://scap.nist.gov/revision/1.2/index.html) que es una serie

de especificaciones de interoperabilidad basada en una comunidad colaborativa abierta que ha desarrollado herramientas y listas de verificación para evaluar protocolos de seguridad informática.

No hay que olvidar que la ontología, incluyendo los elementos y los tipos de relaciones deberán ser adaptados a las necesidades de cada organización, de esta manera el sistema describirade forma precisa su realidad, los flujos de información, los roles y responsabilidades que rigen las actividades que realizan para la consecuación de sus bjetivos y a su vez el cumplimiento de las expectativas de las partes interesadas.

CAPÍTULO V: BIBLIOGRAFÍA

Referencias

AMITI, CANIETI, FMD. (2006). *Visión México 2020, Politicas Públicas en Materia de Tecnologías de Información y Comunicación para impulsar la competitividad de México.* Instituto Mexicano para la Competitividad, Select, CIDE.

Anderson, J. (1977). *Induction of augmented transition networks.* Cognitive Sciences.

Berners-Lee, T. (s.f.). *Semantic Web -XML2000 Architecture*. Obtenido de http://www.w3.org/2000/Talks/1206-xml2k-tbl/slide11-0.html

Beynon-Davies, P. (2002). *Modelo de la pirámide.*

Bobrow, D. e. (1973). *Representation and Understanding: Studies in Cognitive Science.* Academic Press.

Borkin, S. (1980). *Data models: a semantic approach for data base systems.* MIT Press.

CoDD, E. (1979). *Extending the database relational model to capture more meaning.* ACM Transaction on Database Systems vol. 4, n. 4.

Committee, C. P. (1971). *Databse Task Group Report.* ACM.

Cornella, A. (2000). *La gestión de la información en la organización.* Bilbao: Deusto.

Dahl, O. D. (1972). *Structured programming.* Academic press.

Date, C. (1981). *An introduction to data base systems.* Addison-Wesley.

Deming, W. E. (1989). Calidad, Productividad y Competitividad: la salida de la crisis. Madrid: Ediciones Díaz de Santos.

DGN. (2016). *Catálogo de normas oficiales mexicanas*. Obtenido de http://www.economia.gob.mx/

DOF. (3 de Junio de 2014). *Leyes Federales Vigentes. Últimas reformas publicadas en el Diario Oficial de la Federación el 3 de junio de 2014.* Obtenido de http://www.diputados.gob.mx/LeyesBiblio/index.htm.

Fernandez, E. S. (1981). *Database security and integrity.* Addison-Wesley.

Foro Económico Mundial. (2014). *Reporte de competitividad 2012 2013.*

Garcia Camarero, E. (1980). *Garcia Camarero, E.* INRIA.

Garcia Camarero, E. V. (1980). *Seneca: Semantic networks for conceptual analysis. Data Bases in the Humanities and Social Sciences.* North-Holland.

Gruber, T. R. (1993). *A Translation.* Knowledge Acquisition.

Gruber, T. R. (1993). *Toward Principles for.* CA: Technical Report KSL-04, Knowledge Systems Laboratory, Stanford University.

Hofstadter, D. H. (1980). *Gödel, Escher, Bach: An Eternal Golden Braid.* Penguin Books.

Imperio, M. d. (1965). *Data Structures and their Representation in Storage.* Pergamon press.

Institute for Electronics and Electrical Engineers. (1997). *Glosario estándar de la terminología de la ingeniería de software estándar 610.12-1990.*

ISO 27001. (2013). *ISO/IEC 27001 (2013), Information technology -- Security techniques -- Information security management systems – Requirements.*

ISO 31000. (2013). ISO 31000. En I. S. Organization.

ISO Survey. (2014). *Estudio ISO Survey.*

J.Anderson, M. L. (2009). A Strategic Framework for Governance, Risk, and Compliance. *Strategic Finance*, 20, 22, 61.

Keilyn Rodríguez Perojo y Rodrigo Ronda León. (November-December de 2005). Web Semántica: un nuevo enfoque para la organización y recuperación de información en la web. *ACIMED, vol. 13, núm. 6, November-December* , http://bvs.sld.cu/revistas/aci/vol13_6_05/aci030605.htm.

Knuth, D. (1968). *The Art of Computer Programming.* Addison-Wesley.

Krech, D., Crutchfied, R., & Ballachey, E. (1975). indivíduo na sociedade. D.M.

Lozada, A. (8 de Enero de 2016). *Semantic Web Builder*. Obtenido de Infotec: http://www.semanticwebbuilder.org.mx/es_mx/swb/Ontologias

Noy, N. F., & McGuinness, D. L. (s.f.). *Ontology Development 101: A Guide to Creating Your First Ontology*. Obtenido de http://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html

Objetivos SMART. (01 de 2016). Obtenido de https://en.wikipedia.org/wiki/SMART_criteria

OCDE. (1989). Principios de Gobierno Corporativo.

Pariente, S. (2013). (A. Lozada, Entrevistador)

PIERDANT, E. (2006). *¿ QUÉ ES EL COSTO TOTAL DE PROPIEDAD?*

RAE. (2001). Diccionario de la Real Academia Española. RAE.

ScHANK, R. e. (1973). *Computer Models of Thought and Language.* Freeman.

SELECT. (2013). *Fortalecimiento y desarrollo de capacidades.* Secretaria de Economía.

Shannon, C. e. (1949). *The mathematical theory of Comunication.* Universidad de Illinois.

Somerville, I. (2004). *Ingeniería de software. 7 ed.* México: Addison – Wesley.

Tarantino, A. (2008). *Governance, Risk and Compliance Handbook.* Joh Wiley & Sons, Inc.

Taylor, R. e. (1976). *CODASYL Database management systems.* ACM Computing Survey, vol. 8, n. 1.

Trost, H. e. (1981). *The Role of Roles: Some aspects of World Knowledge Representation.* IJCAI, .

W3C Working Group. (s.f.). Obtenido de Defining N-ary Relations on the Semantic Web: https://www.w3.org/TR/swbp-n-aryRelations/

Wiegers, K. (2003). *Software Requirements. 2 ed.* Washington: Microsoft Press.

Winograd, T. (1983). *Language as a Cognitive Process, Vol. I: Syntax.* Addison-Wesley.

Índice de ilustraciones

Ilustración 1. Intereses de las partes interesadas y su alineación a los objetivos 6
Ilustración 2. Modelo de la pirámide. 14
Ilustración 3. Desempeño Global de México. 17
Ilustración 4. Modelo de PHVA 19
Ilustración 5. Crecimiento Certificaciones ISO 9001 en porcentaje. 20
Ilustración 6. Gobernabilidad. 22
Ilustración 7. Partes interesadas. 23
Ilustración 8. Gestión de riesgos de cumplimiento. 25
Ilustración 9. Componentes de un control. 26
Ilustración 10. Representación del conocimiento de una red semántica. 36
Ilustración 11. Resultados obtenidos con un Sistema de búsqueda normal. 38
Ilustración 12. Resultados obtenidos con un sistema de búsqueda semántico. 39
Ilustración 13. Diseño de flujos del sistema de GRC. 40
Ilustración 14. Diseño de cumplimiento y riesgos por activo y servicios. 43
Ilustración 15. Características de los controles. 45
Ilustración 16. Niveles de madurez para la automatización de procesos. 48
Ilustración 17. Niveles de madurez para la gestión. 49
Ilustración 18. Métricas para el monitoreo del desempeño. 50
Ilustración 19. Establecimiento de acciones correctivas / preventivas. 50
Ilustración 20. Componentes de un Red Semántica. 54
Ilustración 21. Estructura del Sistema Semantic Web Builder. 56
Ilustración 22. Ejemplos de activos primarios. 59
Ilustración 23. Ejemplos de activos secundarios 60
Ilustración 24. Relacion entre activos primarios y secundarios. 61
Ilustración 25. Descripción gráfica de la ontología propuesta. 64

ANEXO 1

Esquema de la ontología definido en formato OWL/XML:

```
<?xml version="1.0"?>
<Ontology xmlns="http://www.w3.org/2002/07/owl#"
    xml:base="http://www.semanticweb.org/pcoronaf/ontologies/2016/1/ontologia-grc-pcf"
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:xml="http://www.w3.org/XML/1998/namespace"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    ontologyIRI="http://www.semanticweb.org/pcoronaf/ontologies/2016/1/ontologia-grc-pcf">
   <Prefix name="" IRI="http://www.w3.org/2002/07/owl#"/>
   <Prefix name="owl" IRI="http://www.w3.org/2002/07/owl#"/>
   <Prefix name="rdf" IRI="http://www.w3.org/1999/02/22-rdf-syntax-ns#"/>
   <Prefix name="xml" IRI="http://www.w3.org/XML/1998/namespace"/>
   <Prefix name="xsd" IRI="http://www.w3.org/2001/XMLSchema#"/>
   <Prefix name="rdfs" IRI="http://www.w3.org/2000/01/rdf-schema#"/>
   <Import>http://www.semanticwebbuilder.org/swb4/process</Import>
   <Declaration>
      <Class IRI="#Interes"/>
   </Declaration>
   <Declaration>
      <ObjectProperty IRI="#esResponsable"/>
   </Declaration>
   <Declaration>
      <Class IRI="#alteraciÃ³n_o_modificaciÃ³n_no_autorizada"/>
   </Declaration>
   <Declaration>
      <Class IRI="#pÃ©rdida_o_destrucciÃ³n_no_autorizada"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Activos_secundarios"/>
   </Declaration>
   <Declaration>
      <ObjectProperty IRI="#trata"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Entregable"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Persona"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Evento"/>
   </Declaration>
   <Declaration>
      <Class IRI="#oportunista"/>
   </Declaration>
   <Declaration>
      <Class IRI="#robo,_extravÃo"/>
   </Declaration>
   <Declaration>
      <Class IRI="#GRCElemento"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Regulacion"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Esquema_cumplimiento"/>
   </Declaration>
   <Declaration>
      <Class IRI="#Activos_Principales"/>
```

```
</Declaration>
<Declaration>
   <Class IRI="#Consecuencias"/>
</Declaration>
<Declaration>
   <ObjectProperty IRI="#incertidumbre_sobre"/>
</Declaration>
<Declaration>
   <Class IRI="#Riesgo"/>
</Declaration>
<Declaration>
   <NamedIndividual IRI="#continuidad_de_operaciones"/>
</Declaration>
<Declaration>
   <Class IRI="#intencionado"/>
</Declaration>
<Declaration>
   <ObjectProperty IRI="#isRelatedTo"/>
</Declaration>
<Declaration>
   <Class IRI="#Actividad"/>
</Declaration>
<Declaration>
   <ObjectProperty IRI="#transfiere"/>
</Declaration>
<Declaration>
   <Class IRI="#Registro"/>
</Declaration>
<Declaration>
   <Class IRI="#Parte_interesada"/>
</Declaration>
<Declaration>
   <Class IRI="#Ley"/>
</Declaration>
<Declaration>
   <Class IRI="#copia_no_autorizada"/>
</Declaration>
<Declaration>
   <NamedIndividual IRI="#Retorno_de_inversiÃ³n"/>
</Declaration>
<Declaration>
   <Class IRI="#accidental"/>
</Declaration>
<Declaration>
   <Class IRI="#Control"/>
</Declaration>
<Declaration>
   <ObjectProperty IRI="#mitiga"/>
</Declaration>
<Declaration>
   <Class IRI="#Objetivo"/>
</Declaration>
<Declaration>
   <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
</Declaration>
<Declaration>
   <Class IRI="#uso,_acceso_o_tratamiento_no_autorizado"/>
</Declaration>
<Declaration>
   <ObjectProperty IRI="#cumple_con"/>
</Declaration>
<Declaration>
   <ObjectProperty IRI="#genera"/>
</Declaration>
<Declaration>
```

```
    <Class IRI="#desastre_natural"/>
</Declaration>
<Declaration>
    <Class abbreviatedIRI="owl:Class"/>
</Declaration>
<Declaration>
    <Class IRI="#Recursos"/>
</Declaration>
<Declaration>
    <Class IRI="#Requisito"/>
</Declaration>
<Declaration>
    <ObjectProperty IRI="#dueDate"/>
</Declaration>
<Declaration>
    <Class IRI="#Norma"/>
</Declaration>
<EquivalentClasses>
    <Class IRI="#Actividad"/>
    <Class IRI="#Control"/>
</EquivalentClasses>
<EquivalentClasses>
    <Class IRI="#Entregable"/>
    <Class IRI="#Registro"/>
</EquivalentClasses>
<EquivalentClasses>
    <Class IRI="#Interes"/>
    <Class IRI="#Requisito"/>
</EquivalentClasses>
<SubClassOf>
    <Class IRI="#Actividad"/>
    <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Actividad"/>
    <Class IRI="#Objetivo"/>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Actividad"/>
    <ObjectSomeValuesFrom>
        <ObjectProperty IRI="#genera"/>
        <Class IRI="#Riesgo"/>
    </ObjectSomeValuesFrom>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Activos_Principales"/>
    <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Activos_secundarios"/>
    <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Consecuencias"/>
    <Class IRI="#Riesgo"/>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Control"/>
    <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
    <Class IRI="#Control"/>
    <ObjectSomeValuesFrom>
        <ObjectProperty IRI="#trata"/>
        <Class IRI="#Riesgo"/>
```

```
    </ObjectSomeValuesFrom>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Entregable"/>
    <Class IRI="#Actividad"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Entregable"/>
    <Class IRI="#GRCElemento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Entregable"/>
    <ObjectSomeValuesFrom>
      <ObjectProperty IRI="#isRelatedTo"/>
      <Class IRI="http://www.semanticwebbuilder.org/swb4/xforms/ontology#DateElement"/>
    </ObjectSomeValuesFrom>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Esquema_cumplimiento"/>
    <Class IRI="http://www.semanticwebbuilder.org/swb4/xforms/ontology#HerarquicalNodeable"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Esquema_cumplimiento"/>
    <Class abbreviatedIRI="owl:Class"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Evento"/>
    <Class IRI="#Riesgo"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Interes"/>
    <Class IRI="#Parte_interesada"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Ley"/>
    <Class IRI="#Esquema_cumplimiento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Ley"/>
    <Class IRI="#GRCElemento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Norma"/>
    <Class IRI="#Esquema_cumplimiento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Norma"/>
    <Class IRI="#GRCElemento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Objetivo"/>
    <Class IRI="#GRCElemento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Objetivo"/>
    <Class IRI="#Requisito"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Parte_interesada"/>
    <Class IRI="#GRCElemento"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#Persona"/>
    <Class IRI="#GRCElemento"/>
  </SubClassOf>
```

```
<SubClassOf>
   <Class IRI="#Persona"/>
   <ObjectSomeValuesFrom>
      <ObjectProperty IRI="#esResponsable"/>
      <Class IRI="#Actividad"/>
   </ObjectSomeValuesFrom>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Recursos"/>
   <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Registro"/>
   <Class IRI="#Control"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Regulacion"/>
   <Class IRI="#Esquema_cumplimiento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Regulacion"/>
   <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Requisito"/>
   <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Requisito"/>
   <Class IRI="#Ley"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Requisito"/>
   <Class IRI="#Norma"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Requisito"/>
   <Class IRI="#Regulacion"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Riesgo"/>
   <Class IRI="#GRCElemento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#Riesgo"/>
   <ObjectSomeValuesFrom>
      <ObjectProperty IRI="#incertidumbre_sobre"/>
      <Class IRI="#Objetivo"/>
   </ObjectSomeValuesFrom>
</SubClassOf>
<SubClassOf>
   <Class IRI="#accidental"/>
   <Class IRI="#Evento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#alteraciÃ³n_o_modificaciÃ³n_no_autorizada"/>
   <Class IRI="#Consecuencias"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#copia_no_autorizada"/>
   <Class IRI="#Consecuencias"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#desastre_natural"/>
   <Class IRI="#Evento"/>
```

```
</SubClassOf>
<SubClassOf>
   <Class IRI="#intencionado"/>
   <Class IRI="#Evento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#oportunista"/>
   <Class IRI="#Evento"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#pÃ©rdida_o_destrucciÃ³n_no_autorizada"/>
   <Class IRI="#Consecuencias"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#robo,_extravÃo"/>
   <Class IRI="#Consecuencias"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#uso,_acceso_o_tratamiento_no_autorizado"/>
   <Class IRI="#Consecuencias"/>
</SubClassOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#cumple_con"/>
   <ObjectProperty IRI="#isRelatedTo"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#esResponsable"/>
   <ObjectProperty IRI="#isRelatedTo"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#genera"/>
   <ObjectProperty IRI="#isRelatedTo"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#incertidumbre_sobre"/>
   <ObjectProperty IRI="#isRelatedTo"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#mitiga"/>
   <ObjectProperty IRI="#trata"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#transfiere"/>
   <ObjectProperty IRI="#trata"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
   <ObjectProperty IRI="#trata"/>
   <ObjectProperty IRI="#isRelatedTo"/>
</SubObjectPropertyOf>
<FunctionalObjectProperty>
   <ObjectProperty IRI="#cumple_con"/>
</FunctionalObjectProperty>
<FunctionalObjectProperty>
   <ObjectProperty IRI="#dueDate"/>
</FunctionalObjectProperty>
<FunctionalObjectProperty>
   <ObjectProperty IRI="#isRelatedTo"/>
</FunctionalObjectProperty>
<FunctionalObjectProperty>
   <ObjectProperty IRI="#transfiere"/>
</FunctionalObjectProperty>
<FunctionalObjectProperty>
   <ObjectProperty IRI="#trata"/>
</FunctionalObjectProperty>
<InverseFunctionalObjectProperty>
```

```
    <ObjectProperty IRI="#incertidumbre_sobre"/>
</InverseFunctionalObjectProperty>
<InverseFunctionalObjectProperty>
    <ObjectProperty IRI="#mitiga"/>
</InverseFunctionalObjectProperty>
<SymmetricObjectProperty>
    <ObjectProperty IRI="#incertidumbre_sobre"/>
</SymmetricObjectProperty>
<SymmetricObjectProperty>
    <ObjectProperty IRI="#mitiga"/>
</SymmetricObjectProperty>
<AsymmetricObjectProperty>
    <ObjectProperty IRI="#isRelatedTo"/>
</AsymmetricObjectProperty>
<TransitiveObjectProperty>
    <ObjectProperty IRI="#incertidumbre_sobre"/>
</TransitiveObjectProperty>
<TransitiveObjectProperty>
    <ObjectProperty IRI="#isRelatedTo"/>
</TransitiveObjectProperty>
<ReflexiveObjectProperty>
    <ObjectProperty IRI="#mitiga"/>
</ReflexiveObjectProperty>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#cumple_con"/>
    <Class IRI="#Actividad"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#cumple_con"/>
    <Class IRI="#Entregable"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#cumple_con"/>
    <Class IRI="#Interes"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#cumple_con"/>
    <Class IRI="#Objetivo"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Actividad"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Control"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Entregable"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#GRCElemento"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Ley"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Norma"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
```

```
    <Class IRI="#Objetivo"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Parte_interesada"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Persona"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Regulacion"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Requisito"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#isRelatedTo"/>
    <Class IRI="#Riesgo"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#mitiga"/>
    <Class IRI="#Control"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#mitiga"/>
    <Class IRI="#Riesgo"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#trata"/>
    <Class IRI="#Control"/>
</ObjectPropertyDomain>
<ObjectPropertyDomain>
    <ObjectProperty IRI="#trata"/>
    <Class IRI="#Riesgo"/>
</ObjectPropertyDomain>
<ObjectPropertyRange>
    <ObjectProperty IRI="#dueDate"/>
    <Class IRI="#Actividad"/>
</ObjectPropertyRange>
<AnnotationAssertion>
    <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
    <IRI>#Actividad</IRI>
    <IRI>#Objetivo</IRI>
</AnnotationAssertion>
<AnnotationAssertion>
    <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
    <IRI>#Objetivo</IRI>
    <IRI>#Interes</IRI>
</AnnotationAssertion>
<AnnotationAssertion>
    <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
    <IRI>#Riesgo</IRI>
    <IRI>#Objetivo</IRI>
</AnnotationAssertion>
<AnnotationAssertion>
    <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
    <IRI>#accidental</IRI>
    <IRI>#pÃ©rdida_o_destrucciÃ³n_no_autorizada</IRI>
</AnnotationAssertion>
<AnnotationAssertion>
    <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
    <IRI>#trata</IRI>
```

```
        <IRI>#Interes</IRI>
    </AnnotationAssertion>
    <AnnotationAssertion>
        <AnnotationProperty IRI="#grcrel:isRelatedTo"/>
        <AbbreviatedIRI>owl:Thing</AbbreviatedIRI>
        <IRI>#Requisito</IRI>
    </AnnotationAssertion>
</Ontology>


<!-- Generated by the OWL API (version 4.1.3.20151118-2017) https://github.com/owlcs/owlapi -->
```

ANEXO 2

Como Gestor de aplicaciones web se eligió Tomcat. Se utilizó una máquina virtual creada por Bitnami:

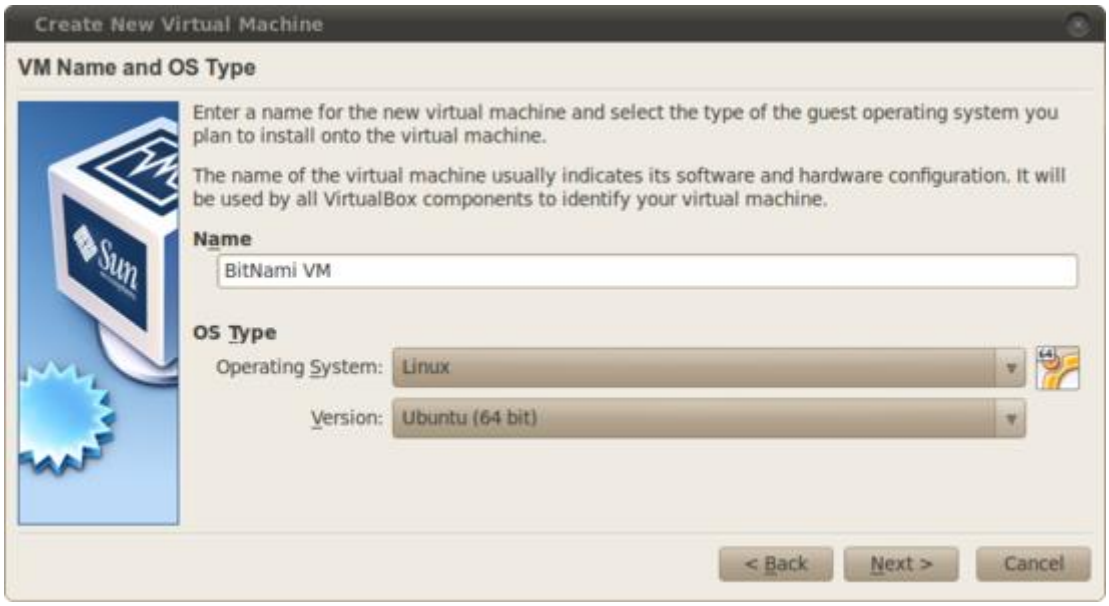
https://bitnami.com/stack/tomcat/virtual-machine

Esta máquina virtual fue montada sobre el manejador de máquinas virtuales de Oracle, Virtual Box:

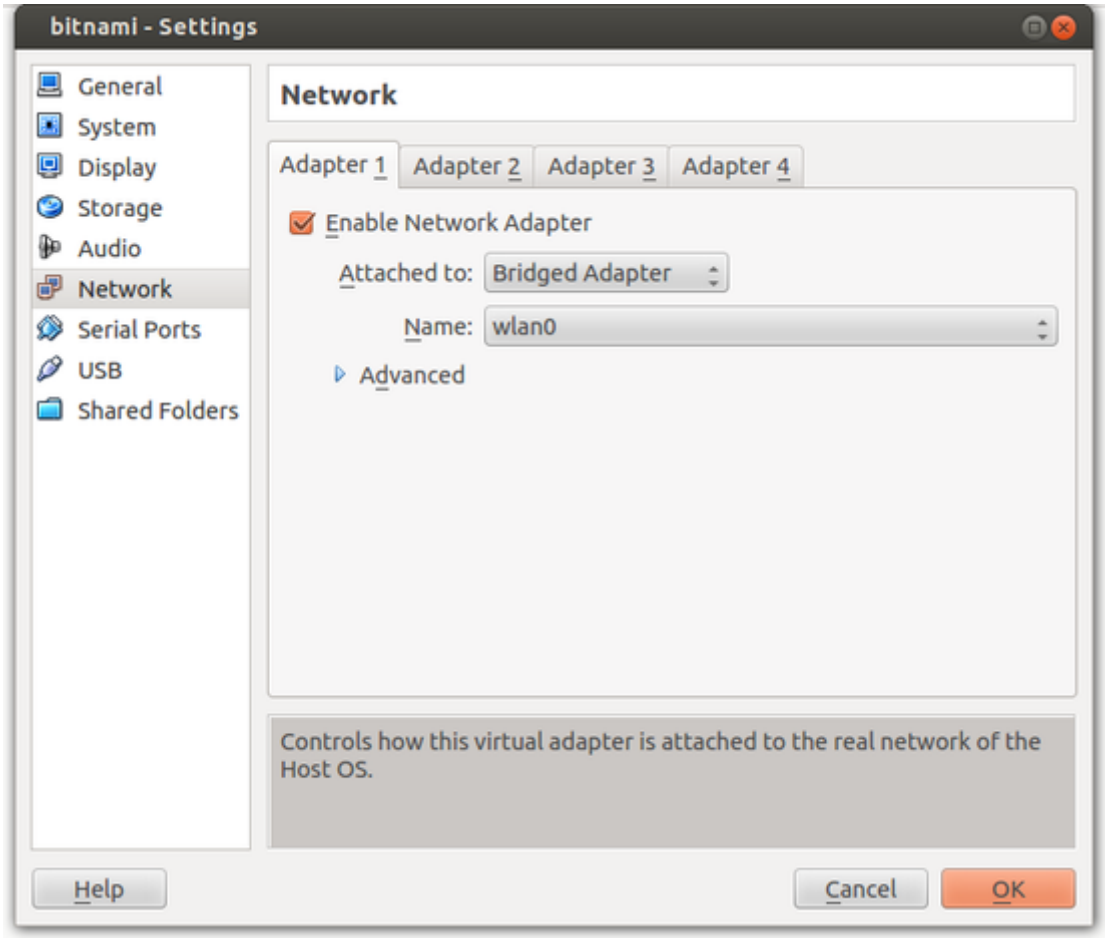
https://www.virtualbox.org/wiki/Downloads

Para instalar el "virtual appliance" se siguieron los siguientes pasos:

1. Create a new Virtual Machine and set that it is a Linux Ubuntu 64bit machine.
2. Configure RAM to 512 or higher. For Ruby-based or Java-based applications (f.e. Liferay, Alfresco, GitLab), we recommend more than 1Gb RAM.
3. Choose "existing hard disk" and select the Bitnami "vmdk" file. Be sure that you select the main one (without s00X in the file name, not any of the other vmdk files: s001.vmdk, s002.vmdk, etc).
   If you are using a previous VMware image with Ubuntu 10.10, go to Settings -> System -> Processor -> Enable PAE. For Ubuntu 12.04 images it is not necessary.
4. Check that the Network configuration is "Bridged Adapter" to have access from remote machines in your network.
5. Start your machine




Create New Virtual Machine
Virtual Hard Disk
Select a hard disk image to be used as the boot hard disk of the virtual machine. You can either create a new hard disk using the New button or select an existing hard disk image from the drop-down list or by pressing the Existing button (to invoke the Virtual Media Manager dialog).
If you need a more complicated hard disk setup, you can also skip this step and attach hard disks later using the VM Settings dialog.
The recommended size of the boot hard disk is 8192 MB.
Boot Hard Disk (Primary Master)
Create new hard disk
Use existing hard disk
bitnami-rubystack-2.0.0-0-dev-ubuntu-12.04.vmdk (Normal, 17.00 GB)
< Back
Next >
Cancel


bitnami - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
Name:
wlan0
Advanced
Controls how this virtual adapter is attached to the real network of the Host OS.
Help
Cancel
OK

Una vez instalada la máquina virtual se siquieron los siguientes pasos para iniciar el gestor de Aplicaciones web

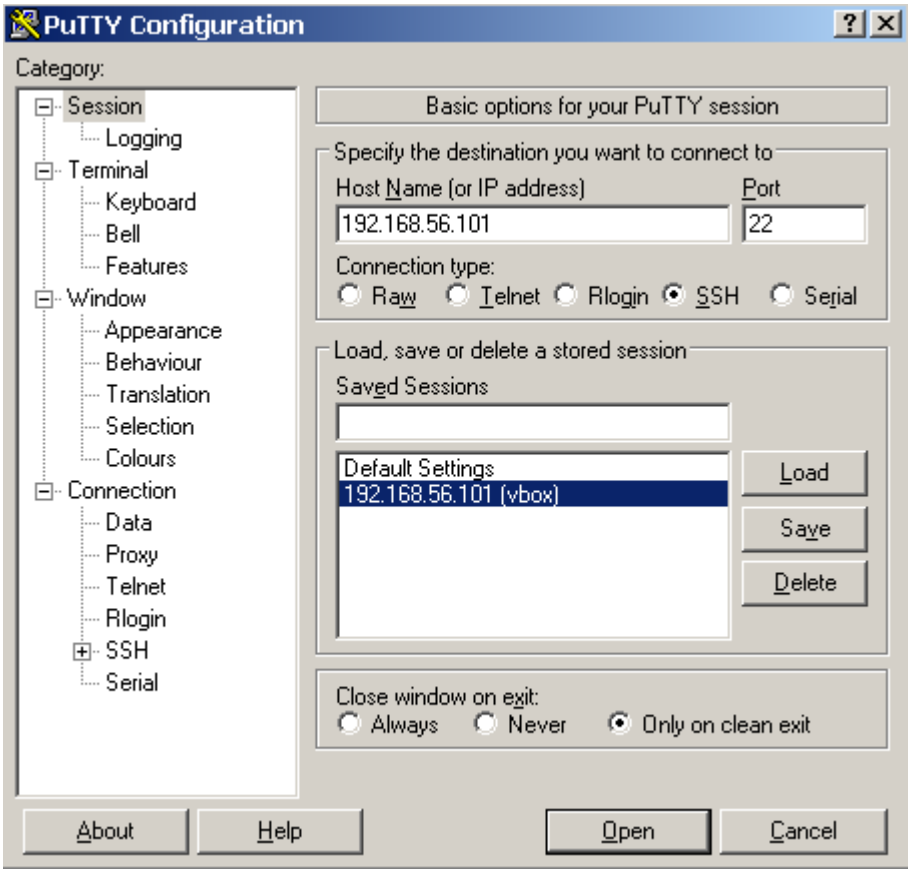
Log in at the console using the default username "bitnami" with password "bitnami". The first time you log in, the machine will request a new user password automatically. Use the "sudo" command to execute any command with root privileges.

If you would like to log in from a remote system using SSH, you must first enable SSH. Then, follow the steps below for your platform.

- Windows & PuTTY
- Linux and Mac OS X

The easiest way to log in to your virtual server remotely is with PuTTY, a free SSH client for Windows and UNIX platforms.

- Download the PuTTY ZIP archive from its website.
- Extract the contents to a folder on your desktop.
- Double-click the *putty.exe* file to bring up the PuTTY configuration window.
- Enter the network IP address of your virtual server into the "Host Name (or IP address)" field, as well as into the "Saved Sessions" field.
- Click "Save" to save the new session so you can reuse it later.



- Go back to the "Session" section and save your changes by clicking the "Save" button.

- Click the "Open" button to open an SSH session to the server.
- PuTTY will first ask you to confirm the server's host key and add it to the cache. Go ahead and click "Yes" to this request (learn more).

- Enter the default username "bitnami" and password "bitnami" when prompted.

  You should now be logged in to your virtual server.

La información para inicio de sesión por defecto es la siguiente:

Default application login information

(Please change to avoid unauthorized access.)

The default login information for Tomcat cloud images is:

> **Username:** manager
>
> **Password:** bitnami

System account:

> **Username:** bitnami

La información para el administrador general del Sistema:

It is not necessary to have a known password for the root in the Virtual Appliances. You can run any command as root user with the "sudo" command. For example to check the servers status:

```
$ sudo /opt/bitnami/ctlscript.sh status
```

You have to specify the password for the "bitnami" user. You can also change to root user in the command prompt:

```
$ sudo su

# /opt/bitnami/ctlscript.sh status
```

If you want to specify a known root password for the Virtual Appliance, you can change follow these steps:

```
$ sudo su

# passwd
```

Una vez instalado el Gestor de Aplicaciones Web se instaló el Semantic Web Builder siguiendo los siguientes pasos:

http://www.semanticwebbuilder.org.mx/en_mx/swb/SWB_Portal

Ultima versión liberada SWB 4.5.11.1 el 23 de noviembre de 2015.

Usuario: admin Contraseña: webbuilder

El siguiente usuario es usado tanto para el portal Demo como para la Administracion del SWB Process (SWB Portal):

Usuario: admin

Contraseña: webbuilder

Consola de administración

http://192.168.134.67/smbp/es/SWBAdmin/home

El editor de ontologías utilizado fue Protege:

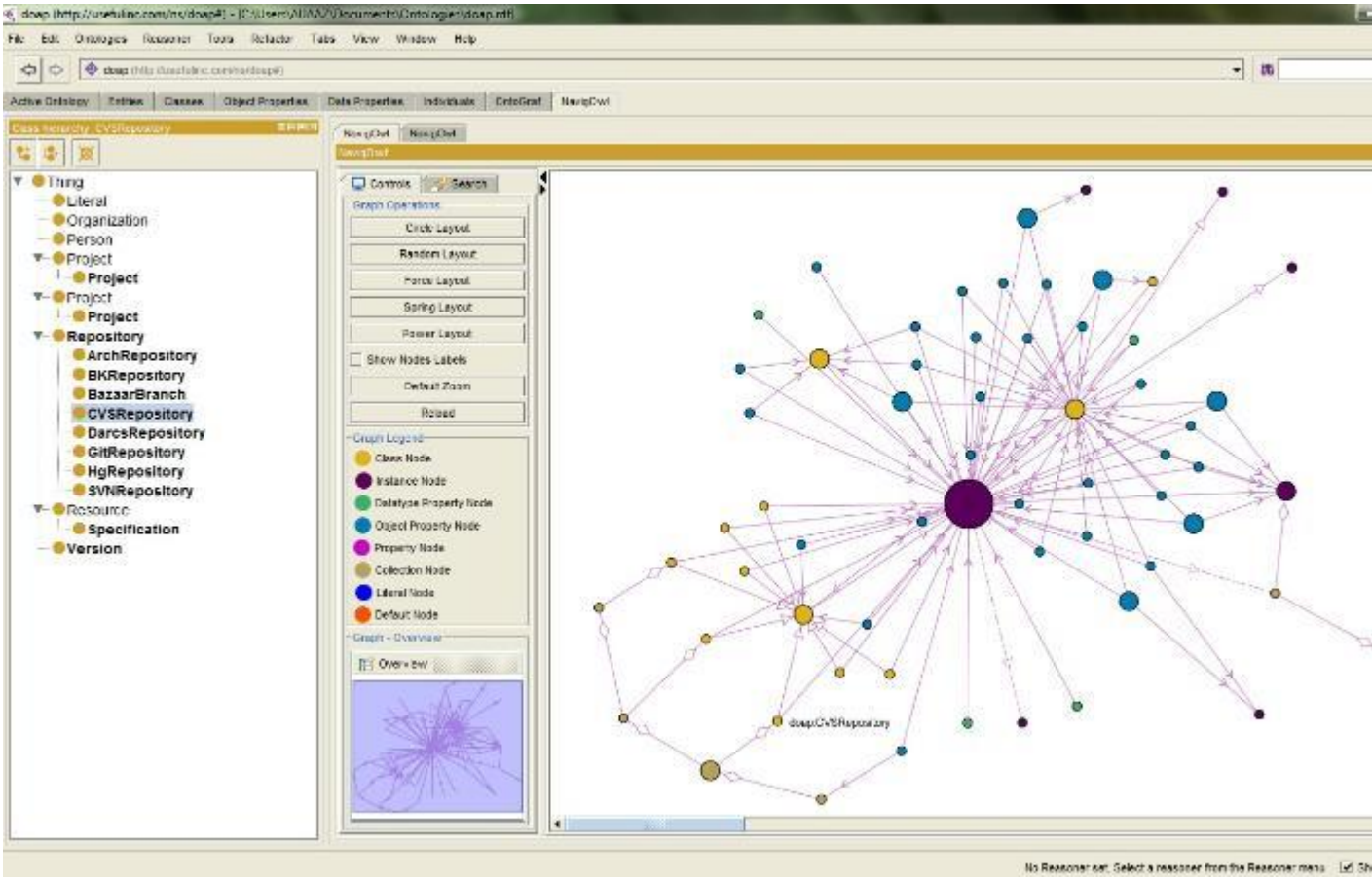
http://protege.stanford.edu/products.php#desktop-protege

A éste se le instalaron dos complementos NavigOWL y OWLViz los cuales se describen a continuación:

NavigOWL

Its an immense pleasure to share with you all, that I have developed an Ontology Visualization Tool '**NavigOWL**' along with its plugin for Protege 4.1.

NavigOWL is a visualization tool which is specially designed to explore the semantic nets a.k.a Ontologies. The Tool is enriched with appealing graph layouts that can be applied over the semantic net in order to understand the structure of ontolgies easily and it facilitates the user to build mental map in more clear and consistent view of ontology graph. The tool supports rdf and owl ontologies to visualize them.



Se pede encontrar más información en:

http://klatif.seecs.nust.edu.pk/navigowl
http://protegewiki.stanford.edu/wiki/NavigOWL

OWLViz

http://protegewiki.stanford.edu/wiki/OWLViz

OWLViz is bundled with the "full" installation of Protege. After you have installed Protege, there are two additional steps you need to perform for this plugin to work properly:

- Download and install a recent version of Graphviz, which is a free, open source graph visualization software from AT&T Research.

- Protege will make an educated guess about where to find graphviz depending on your operating system, but if it does not get it right you will need to configure this yourself:
  -
  - **Protege3.x** and **Protege4.0 (pre build 105)** on the OWLViz tab, click the Options button to bring up the Options dialog. On the Layout Options panel, specify the path to the location of the DOT executable (dot.exe). The Options dialog will look something like the following, after performing this step:
  -
  - **Protege4.x (build 105 onwards)** these settings have moved into the OWLViz preferences panel. Again, specify the path to the dot executable in the appropriate place.