CIS1010IS04

http://pegasus.javeriana.edu.co/~CIS1010IS04

PROPUESTA PARA EL CUMPLIMIENTO DE LOS CONTROLES TÉCNICOS DE LA CIRCULAR 14 BASADO EN EL MODELO PLANTEADO POR LA NORMA ISO27001, BAJO PLATAFORMA ORACLE

Javier Alejandro Losada Rivera

Marco Antonio Olivera Arboleda

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ, D.C.
2010

CIS1010IS04

PROPUESTA PARA EL CUMPLIMIENTO DE LOS CONTROLES TÉCNICOS DE LA CIRCULAR 14 BASADO EN EL MODELO PLANTEADO POR LA NORMA ISO27001, BAJO PLATAFORMA ORACLE

Autor(es):

Javier Alejandro Losada Rivera
Marco Antonio Olivera Arboleda

MEMORIA DEL TRABAJO DE GRADO REALIZADO PARA CUMPLIR UNO DE LOS REQUISITOS PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

Director

Ing. Luz Adriana Bueno Mendoza

Jurados del Trabajo de Grado

Ing. Gloria Patricia Arenas Mendoza

Ing. Norbey Mejía Chica

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS
BOGOTÁ, D.C.
Diciembre, 2010

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA DE SISTEMAS

Rector Magnífico

Joaquín Emilio Sánchez GarcíaS.J.

Decano Académico Facultad de Ingeniería

Ingeniero Francisco Javier Rebolledo Muñoz

Decano del Medio Universitario Facultad de Ingeniería

Padre Sergio Bernal Restrepo S.J.

Directora de la Carrera de Ingeniería de Sistemas

Ingeniero Luis Carlos Díaz Chaparro

Director Departamento de Ingeniería de Sistemas

Ingeniero César Julio Bustacara Medina

Artículo 23 de la Resolución No. 1 de Junio de 1946

"La Universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado. Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque no contengan ataques o polémicas puramente personales. Antes bien, que se vean en ellos el anhelo de buscar la verdad y la Justicia"

AGRADECIMIENTOS

Agradecemos a nuestra directora Luz Adriana Bueno que desde un principio nos apoyó en la realización del proyecto, sin su guía, soporte y compromiso no podría haberse logrado.

A nuestros Padres por estar siempre presentes, apoyándonos y aconsejándonos en cada paso que dimos.

A Alejandra por estar siempre de manera incondicional junto a mí.

Contenido

ABSTRACT

The following graduation paper begins by presenting an analysis of the relationship between the technological controls included in the Circular 14 of the Superintendence of Finance - 2009 and the International Standards ISO/IEC 27001 Appendix A. Subsequently, it will explore and review the Oracle tools that facilitate compliance with the previously noted controls while proposing two potential technological solutions (for medium and large size companies). These approaches are presented in 3 different sub-solutions for easy implementation. Finally, the paper analyzes how the proven model ISO 270001 is equated with Circular 14.

RESUMEN

En el presente trabajo de grado se plantea el análisis de la relación de los controles tecnológicos de la circular 014[1] del 2009 de Superintendencia Financiera de Colombia con el estándar internacional ISO/IEC 27001 Anexo A[2], una vez establecida esta relación se exploran y analizaran herramientas Oracle que apoyen el cumplimiento de dichos controles y se proponen dos soluciones tecnológicas (para mediana y gran empresa) que a su vez están divididas en 3 subsoluciones para su fácil adopción, finalmente se analiza como el modelo probado del estándar ISO 27001 se homologa con la circular 014.

[1] La circular 014 del 2009 ha sido objeto de una actualización que contiene aclaraciones de algunos de sus secciones y se conoce como Circular 038 2009.

[2] El anexo A de la ISO/IEC 27001 contiene la misma información de la ISO 27002.

RESUMEN EJECUTIVO

Las entidades reguladas por la superintendencia financiera están en la obligación de cumplir con las regulaciones que esta emite buscando que las organizaciones de este campo (financiero) definan políticas y procedimientos que faciliten la gestión y control de la información. Regulaciones como lo son la Circular 052 y Circular 014.
Del otro lado se cuenta con el modelo propuesto por la norma ISO27001, un Sistema de Gestión de la Seguridad de la Información, aspecto vital para las entidades financieras quienes manejan a diario grandes volúmenes de datos sensibles.

Las empresas se topan con estas normativas y se enfrentan ante un proceso complejo sin un procedimiento claro a seguir, de esta forma tratan de cumplir con los requerimientos de manera errónea resultando en cumplimientos parciales que resultan con sanciones para el caso de las regulaciones o una negación al proceso de certificación para el caso de la norma ISO27001.

Es importante aclarar que la propuesta puede servir para seleccionar controles a resolver tanto en una entidad financiera robusta como una pequeña, aunque consecuentemente el tiempo, el esfuerzo y el presupuesto a emplear variarán sensiblemente.

A raíz de esta problemática surge la propuesta del presente Trabajo de Grado, de esta forma las entidades contarán con un punto de arranque para el cumplimiento de la Circular 014 e ISO27001.

Bajo este ámbito, se realizaron una serie de alineaciones a nivel de objetivos control no solo de la Circular 014 e ISO27001 sino también del estándar COBIT y COSO. Los objetivos de control están agrupados en áreas de acción, estos controles son los que ayudarán a determinar el nivel de cumplimiento para las regulaciones y estándares. La idea principal fue encontrar un punto común, de homologación, en el cual pueda identificarse claramente una relación de correspondencia, permitiendo esto que un control que se ha garantizado como cumplido apoye el cumplimiento de uno o más controles similares o relacionados en otra normativa o estándar.

De esta forma se cuenta con una serie de matrices que mostrarán la relación de correspondencia principalmente entre la Circular 014 e ISO27001, y de manera secundaría con COBIT y COSO.

Como no solo basta contar con un plano general de correspondencia, se decidió proponer una serie de arquitecturas basadas en soluciones tecnológicas de Oracle, que apoyarán el cumplimiento de los controles relacionados. Para esto se identificaron y relacionaron los productos de acuerdo al área de acción en la que se encuentran agrupados los objetivos de control, para posteriormente realizar un mapeo de aquellos controles que podrían resolverse a través de estas herramientas Oracle.

El resultado provee de varios medios guía, como lo es una matriz de correspondencia, en la cual se encuentran identificados los controles y los productos Oracle que apoyarán su cumplimiento. Hay que destacar que para cada arquitectura propuesta se cuenta con dicha matriz

de correspondencia, de esta forma se observa claramente el alcance de cada una de las arquitecturas identificando los controles que cada una apoyará al proceso de cumplimiento de los objetivos de control relacionados.

Como segundo medio, se cuenta con los diagramas de arquitecturas, los cuales muestran los productos seleccionados y su interacción entre ellos. Valga la aclaración que dichas arquitecturas están acotadas en dos grupos basados en el tipo de organización, Mediana Empresa y Grandes Empresas, esto limitará el tipo y variedad de productos a implantar, entendiendo que aquellas organizaciones con mayores recursos tendrán a disposición un mayor número de productos. Pero entendiendo al mismo tiempo que existen organizaciones con presupuestos más limitados pero que de igual forma están en la obligación de cumplir con las regulaciones existentes e interesadas en aplicar al proceso de certificación ISO27001. Sin embargo contar con un recurso de inversión menor no significa un impedimento al cumplimiento y/o certificación, por el contrario se cuentan con opciones alternativas que apoyarán a un nivel conveniente el proceso de cumplimiento.

Al finalizar este proceso se observó la generalidad con la que la Circular 014 presenta sus controles permitiendo realizar diferentes interpretaciones llegando dificultar el proceso de alineamiento. Sin embargo fruto del proceso se concluyó que efectivamente existen puntos de encuentro entre la Circular 014 y la norma ISO27001. De manera adicional, se descubrió que varios de los productos Oracle propuestos están en sí mismos orientados al cumplimiento de las regulaciones.

INTRODUCCIÓN

En la actualidad es imperativo para las empresas, ya sean grandes o pequeñas el mitigar los riesgos subsecuentes de su actividad económica, porque de otra manera seria imposible sobrevivir en el ambiente competitivo del mercado actual, por ello no debe ser visto como una molestia o como un gasto innecesario, la aplicación de controles para la mitigación de riesgos es una inversión a futuro que evitara más de un dolor de cabeza y por supuesto el gasto de prevenir será poco, comparado con los gastos que genera la materialización de un riesgo.

Además muchos de ellos pueden ser sobrellevados con software y hardware que pueden reducir el error humano, automatizando procesos y realizándolos de manera eficaz y eficiente, pero definir estos controles no es fácil y mucho menos aplicarlos por ello afortunadamente en el mundo existen modelos, estándares y regulaciones que buscan dar una guía para lograr mantener protegida a las empresas contra los riesgos.

El siguiente trabajo de grado tiene como objetivo apoyar el cumplimiento de los controles tecnológicos de la circular 014 de 2009 de la Superintendencia Financiera de Colombia, para lograr esta meta, se inicia con la alineación de la circular junto con estándares y regulaciones internacionales que tienen un grado de madurez más alto debido a su trascendencia e historia, además cuentan con modelos de adopción ya probados, y debido a que la creación de estas estándares y normas fueron creados a partir de buenas prácticas es de esperar que en muchos de los controles sean comunes.

Una vez encontrada la relación de los controles entre sí, se analizaran los requerimientos tecnológicos y se definirán los tipos de programas necesarios que abarquen la mayor parte de los controles de la circular 014, ya teniendo presente las necesidades de software se procederá con el estudio de los productos Oracle, una vez seleccionados se pasa a los diseños donde vemos como los productos se distribuyen teniendo en cuenta que se proponen dos grandes arquitecturas una para gran empresa y otra para mediana empresa estas a su se dividen en tres subgrupos los cuales son monitoreo, seguridad y “Administración y Monitoreo”, esto permitirá a las empresa pensar en una adopción por etapas de los productos ORACLE.

Finalmente se propone una homologación de la circular 014 de 2009 de la Superintendencia Financiera de Colombia con el modelo propuesto por la norma ISO 27001, donde se podrá apreciar por ejemplo que el análisis y la gestión de riesgos es abordada por la ISO 27005.

I – DESCRIPCIÓN GENERAL DEL TRABAJO DE GRADO

1. Oportunidad ó Problemática

1.1. Descripción del contexto

La adopción de tecnologías que apoyen los procesos empresariales es una tendencia que se está dando desde hace varios años, esto debido a las ventajas que estas ofrecen como lo son: agilizar procesos, generar conocimientos, mejorar administración del conocimiento, romper fronteras de comunicación y producción, expansión a nuevos mercados, sustentando decisiones y generando más ganancias, Pero el uso de la tecnología por sí sola no es suficiente, a esta se le debe proveer datos obtenidos de diferentes fuentes (informes, investigaciones, estadísticas entre otras), que una vez procesados se convierten en información que debe ser almacenada y según su calidad y cantidad, se convierte junto con la tecnología en los activos más valiosos de la empresa. Pero el incremento descuidado de esta información está generando grandes riesgos que amenazan con la permanencia de las empresas en el mercado, esto es debido a la complejidad de estas tecnologías y a la falta de metodología para la integración de las mismas, esto lo único que logra es que las ventajas obtenidas se vuelvan en contra de las empresas, ya que facilita por falta de controles que empleados desleales, hackers, malware, virus, fallos en hardware o desastres naturales, generen grandes pérdidas para las empresas que en algunos casos nunca logran recuperarse, por ello es importante salvaguardar la información controlando la tecnología.

Hoy en día la batalla por la información es ahora una guerra cibernética que se da en todos los rincones del mundo. Y el listado de amenazas es creciente donde podemos encontrar desde redes zombis o botnets que realizan ataques dirigidos, PDFs maliciosos, hasta grupos de hacking donde entrenan nuevos atacantes, en su discurso dado el 29 de mayo de 2009 el presidente de los Estados Unidos Barack Obama dice: "*Se ha estimado que sólo el año pasado los ciberdelincuentes robaron la propiedad intelectual de las empresas en todo el mundo por valor de hasta 1 trillón de dólares.*"(WHITE HOUSE, 2009)[3], esta escandalosa cifra evidencia la falta de ciberseguridad en las empresas.

Para un mayor detalle remitirse a la sección 3.1 DESCRIPCIÓN DEL CONTEXTO DETALLADO.

[3] WHITE HOUSE. (29 de Mayo de 2009). *REMARKS BY THE PRESIDENT*. Recuperado el 2010 de Septiembre de 5, de whitehouse: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

1.2. Formulación

- ¿Qué relación existe entre la circular 14 de la SUPERINTENDENCIA FINANCIERA DE COLOMBIA e ISO 27001 y de qué manera se puede garantizar el cumplimiento de los controles tecnológicos de la circular 14?

2. Descripción del Proyecto

2.1. Justificación

A raíz de este contexto, nace la necesidad de generar una documentación específica que ayude a las empresas del sector financiero a encontrar una manera rápida, ágil y correcta de cumplir con la mayor cantidad de controles pertenecientes a la ISO27001 y Circular 014.Pues actualmente se exponen las normativas y sus correspondientes especificaciones, pero es la empresa quien debe decidir qué controles aplicar, que tipos de riesgo puede mitigar, cómo hacerlo y con la ayuda de algunas herramientas.

2.2. Objetivo general

Desarrollo de una propuesta para el cumplimiento de los controles tecnológicos de la circular 14 que permita mediante el uso de herramientas Oracle , agilizar la administración de la seguridad de la información acorde con los objetivos de control del Anexo A relacionados de la norma ISO 27001

2.3. Objetivos específicos

- Analizar el porcentaje de controles de la ISO 27001 que pueden ser resueltos a través de los objetivos de control tecnológicos de la circular 014 de la superintendencia financiera.
- Explorar, analizar y seleccionar las soluciones tecnológicas Oracle que apoyen el cumplimiento de los controles tecnológicos de la circular 14 así como los controles relacionados con la ISO 27001.
- Analizar, Diseñar y describir de las arquitecturas basadas soluciones tecnológicas Oracle que apoyaran el cumplimiento de los controles tecnológicos de la circular 14 así como los controles relacionados con la ISO 27001.
- Validar la propuesta y las soluciones por medio de un juicio de experto teniendo en cuenta el nivel de impacto y cumplimiento que tendría su adopción.

II -MARCO TEÓRICO

En esta sección encontraremos los concepto y teorías necesarias que se utilizarán para sustentar y justificar el problema de la investigación propuesta.

1. DESCRIPCIÓN DEL CONTEXTO DETALLADO

En una encuesta realizada por Deloitte"2010 Global Financial Services Security Survey"(Deloitte, 2010) en la cual participaron el 27% de las 100 principales instituciones financieras mundiales, 26% de los 100 principales bancos mundiales y el 28% de las 50 compañías aseguradoras mundiales las cuales se les realizaron preguntas relacionadas con la seguridad de la información, cuando se les pregunto el nivel de confianza de que la información está protegida contra ataques cuyos resultado apreciamos en la Tabla 1,la mayoría de los encuestados un 42% afirmo sentir *"Algo de Confianza"* con su protección contra un ataque interno y tan solo un 25% se sintió *"Algo de Confianza"* con su protección contra un ataque externo, tan solo el 34% afirmo estar *"Muy Confiado"* frente a un ataque interno y un 56% dijo estar *"Muy Confiado"* contra un ataque externo.

Tabla 1: CONFIANZA QUE LA INFORMACIÓN DE LA ORGANIZACIONES ES PROTEGIDA DE ATAQUES INTERNOS Y EXTERNO

	Mucha Confianza	Muy Confiado	Algo de Confianza	No muy Confiado	No Confían en Absoluto
Ataques originados internamente	5%	34%	42%	16%	2%
Ataques originados externamente	15%	56%	25%	3%	1%

Tomado y Traducido de *2010 Financial Services Global Security Study: The faceless threat*(Deloitte, 2010)[4].

[4] Deloitte. (2010). 2010 Financial Services Global Security Study: The faceless threat. Recuperado el Agosto de 29 de 2010, de Deloitte: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/Financial%20Services/dtt_fsi_2010%20Global%20FS%20Security%20Survey_20100603.pdf

Si bien los niveles de confianza más bajos *"No muy Confiado"* y *"No confían en Absoluto"* de la Tabla 1 no suman más de 18%, cuando hablamos de *"Ataques originados internamente"* y solo suman un 4% cuando hablamos de *"Ataques originados externamente"*, los ataques informáticos exitosos se presentan y peor aún estos se repiten debido a que las empresas no reaccionan de manera adecuada ante estas agresiones, entre los que más se presentan que apreciamos en la Tabla 2 están *"El software malicioso se origina fuera de la organización"* que se presenta por lo menos una vez en el 14% de las empresas y ocurre repetidas veces en un 20% de las empresas, esto evidentemente no debe suceder pero sucede y no solo con este tipo de ataques sino que con otros como lo son *"La pérdida de información procede de un ataque físico fuera de la organización"*.

Indudablemente los ataques no solo provienen desde fuera de la organización y entre las que más se presentan al interior de las organizaciones como se ve en la Tabla 3 se encuentra la *"Brecha accidental de información que proviene de dentro de la organización"* que se presenta por lo menos una vez en el 14% de la organizaciones y se repite en más del 20% de ellas.

Tabla 2: VIOLACIONES EXTERNAS EXPERIMENTADAS EN LOS ÚLTIMOS 12 MESES

	Un Incidente	Repetidos Incidentes
El software malicioso se origina fuera de la organización	14%	20%
La pérdida de información procede de un ataque físico fuera de la organización	10%	10%
Fraude financiero externo que implica sistemas de información	5%	9%
Brecha de información que proviene de fuera de la organización	7%	4%
Brecha de información que proviene de un vendedor de tercero	6%	4%
Robo de información que es resultado de espionaje estatal o industrial	2%	1%
Desfiguración del sitio web	4%	1%
Brecha de la red móvil que proviene de fuera del a organización	1%	1%
Otra forma de brecha externa	5%	4%

Tomado y Traducido de *2010 Financial Services Global Security Study: The faceless threat*(Deloitte, 2010).[5]

Tabla 3: VIOLACIONES INTERNAS EN LOS ÚLTIMOS 12 MESES

	Un Incidente	Repetidos Incidentes
Brecha accidental de información que proviene de dentro de la organización	8%	11%
Software malévolo que proviene de dentro de la organización	9%	10%
Brecha de información que proviene de dentro de la organización conducida por un empleado	11%	8%
Fraude interno financiero que implica sistemas de información	7%	4%
Brecha de información que proviene de dentro de la organización conducida por un no empleado	3%	2%
Brecha de información que proviene de un vendedor de tercero	3%	2%
Brecha de red móvil que proviene de dentro de la organización	1%	1%
Información privilegiada y comerciante bribón	2%	0%
Otra forma de brecha interna	3%	3%

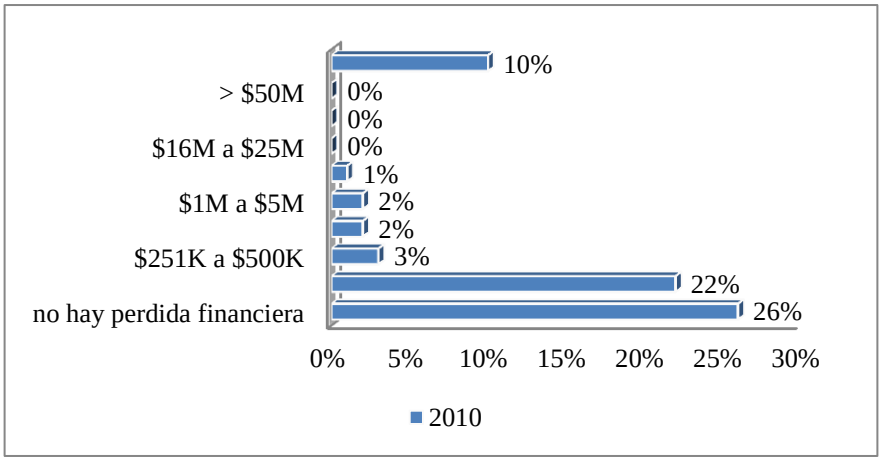
Tomado y Traducido de *2010 Financial Services Global Security Study: The faceless threat*(Deloitte, 2010)[6].

[5] Ibíd., p. 5.

[6] Ibíd., p. 5.

Sin lugar a dudas estos ataques no solo generan perdida de información y de imagen ante los clientes, también generan grandes pérdidas que en algunos casos ni siquiera puede ser estimada por las empresas, como se puede contemplar en la Tabla 4 que solo el 26% dice *"no hay perdida financiera"*, mientras que el restante presentan perdidas que van de desde los 250.000 dólares hasta 10 millones de dólares y en algunos casos 10% dice que esta *"no medido"*, debemos tener en cuenta que en más de la mitad de los casos las empresas no tiene registro de estar perdidas con lo cual se aumenta la probabilidad que los errores se presenten nuevamente.

Tabla 4: DAÑOS Y PERJUICIOS ESTIMADOS TOTALES MONETARIOS QUE SON RESULTADO DE VIOLACIONES DURANTE LOS 12 MESES PASADOS



Tomado y Traducido de *2010 Financial Services Global Security Study: The faceless threat*(Deloitte, 2010)[7].

Por estas razones "*La creciente adopción de mejores prácticas de TI ha sido impulsada por una exigencia de la industria de TI para gestionar mejor la calidad y fiabilidad de las TI en los negocios y responder a un número cada vez mayor de las disposiciones normativas y contractuales*"(ITGI, 2005)[8] que buscan permitirles un mayor control en la administración de la información por medio de políticas y procedimientos de control interno, desarrollando sus

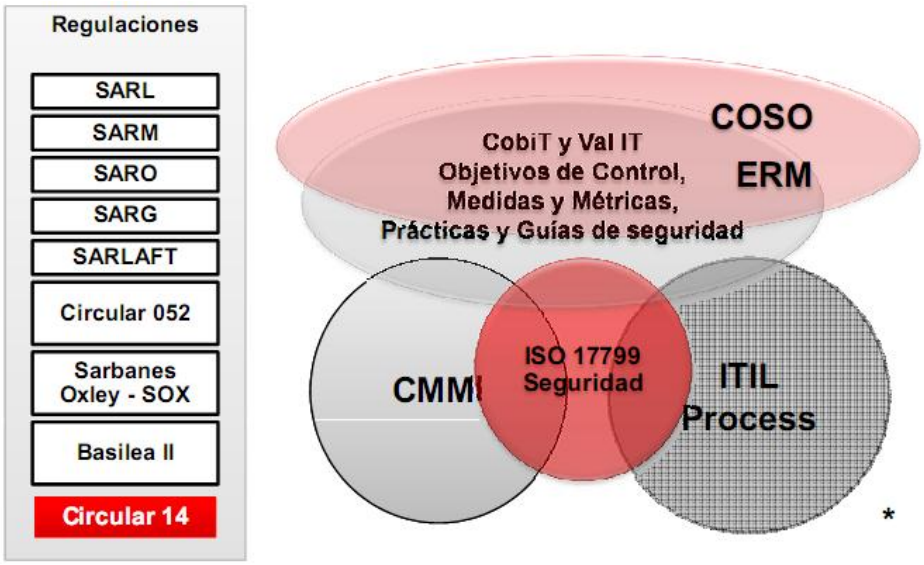
[7] Ibíd., p. 5.

[8] ITGI. (2005). itgovernance. Recuperado el 15 de Agosto de 2010, de http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf

objetivos "*en el ámbito de la seguridad, transparencia y eficiencia*". (Superintendencia Financiera de Colombia, 2009)[9].

Con relación a la gestión del riesgo, seguridad de la información, continuidad del negocio y elementos relacionados se observan en la Ilustración 1, se dispone de estándares internacionales como lo son COSO, Cobit, Val IT, CMMI, ISO 17799 (más conocido actualmente como ISO 27001 anexo A ó ISO 27002) y ITIL; y en lo referente a las Regulaciones encontramos a SARL, SARM, SARO, SARG, SARLAFT, CIRCULAR 052 BASILEA II y CIRCULAR 014.

Ilustración 1: Estándares y Regulaciones.



Tomado de ISACA.org

Estándares internacionales para la Gestión de la Seguridad de la Información, como lo es la ISO27001 anteriormente ISO 17799, la cual "*busca proponer un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información*"(ISO, 2005)[10], junto con ITIL y Cobit 4.1 1 "*son el estándar y las*

[9] Superintendencia Financiera de Colombia. (19 de Mayo de 2009). Normativa. Recuperado el 16 de Agosto de 2010, de Superintendencia Financiera de Colombia: http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ance014_09.doc

[10] ISO. (2005). International Standards for Business. Recuperado el 16 de Agosto de 2010, de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

buenas prácticas que están en las áreas de seguridad de la información o en los departamentos de tecnologías de información"(ACIS, 2010)[11].

Regulaciones Colombianas como lo es la Circular 052 y la Circular 014 también conocida como Circular 038 la cual contiene modificaciones para la circular 014 son emitidas por la Superintendencia Financiera de Colombia, cabe recalcar que la "*Circular 052 y Circular 014 son las normativas actuales a cumplir, sin embargo la Circular038 del 2009 es las más reciente y activa*"(Bueno, 2010)[12]. Estas circulares consideran que "Corresponde a los administradores de las entidades **vigiladas o sometidas al control exclusivo** de esta Superintendencia" cumplir con dichas circulares, entre las entidades vigiladas encontramos las del sector de servicios de banca y financieros, en la actualidad estas empresas se están definiendo los planes de adopción e implementación de las mismas debido a que las fechas paras las cuales ellos deben demostrar cumplimiento se acercan. Estas regulaciones definen que es lo que desean pero en ningún momento especifican como lograr esto, por ello las empresas sin tener un punto de arranque ejecutan de manera inadecuada o parcialmente los controles que establecen las regulaciones, otros deciden no cumplirlos con las consecuencias que esto conlleva, "*Existe el peligro, que la aplicación de estas mejores prácticas potencialmente útiles será costosa y fuera de foco si se les trata como una orientación puramente técnica*"(ITGI, 2005)[13], para que estas buenas prácticas logren de manera efectiva sus objetivos se deben aplicar en el contexto del negocio y en la medida de lo posible que estas logren el mayor beneficio para la organización. "*La alta dirección, administración de empresas, auditores, oficiales de cumplimiento y los administradores de TI deben trabajar juntos para asegurar que las mejores prácticas de conducir a la relación coste-efectiva y bien controlados de TI de entrega.*"(ITGI, 2005)[14]

Es importante aclarar que la propuesta puede servir para seleccionar controles a resolver tanto en una entidad financiera robusta como una pequeña, aunque el tiempo, el esfuerzo y el presupuesto a emplear variarán sensiblemente. A continuación serán explicados de manera un poco más detalladas algunos de los marcos de referencia nombrados anterior mente así mismo se aclarara la relación entre ellos.

III – PROCESO

En este capítulo se presenta la metodología que enmarco las actividades del presente proyecto, dividida en fases con sus respectivos entregables.

[11] Superintendencia Financiera de Colombia, op. cit., p.8.

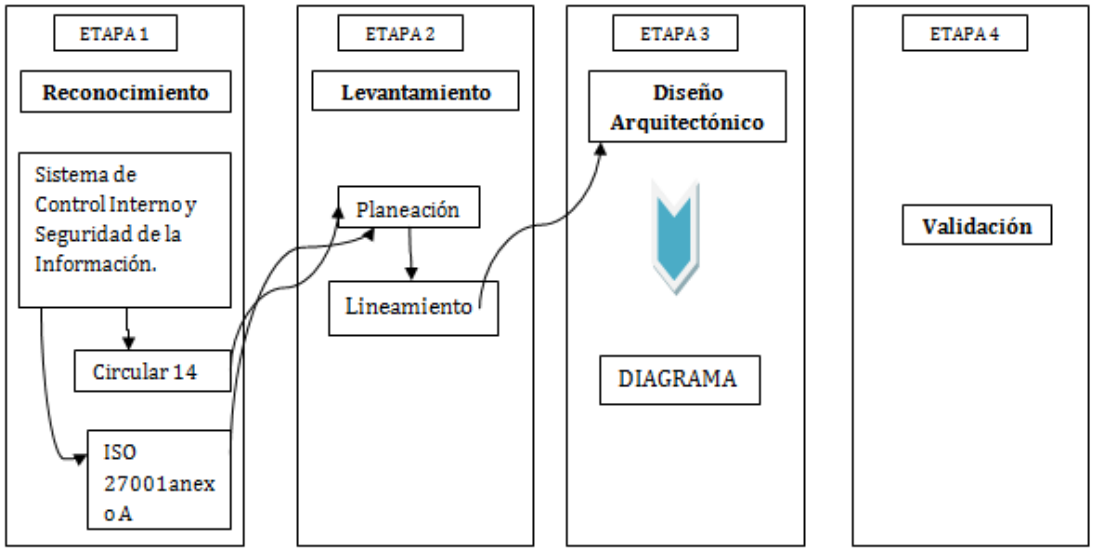
[12] Bueno, L. A. (2010).

[13] ITGI, op. cit., p.8.

[14] ITGI, op. cit., p.8.

1. Metodología Propuesta

La metodología que será empleada para el desarrollo de este proyecto consiste en una serie de etapas interconectadas que servirán de base sólida para el resultado final de la investigación.



De esta forma la primera etapa de esta metodología se basó en el estudió y entendimiento de los conceptos de Sistema de Control Interno y Sistema de seguridad de la información, sus componentes y fases para finalmente abordar la Circular 014 y la norma ISO27001. El estudio de esta regulación y estándar respectivamente hizo posible conocer y entender sus objetivos, estructura y enfoque.

La segunda etapa consistió en realizar la planeación previa a la realización de los alineamientos, la cual consiste en entender la forma en la que se abordaría el proceso de cruce de controles entre la regulación y los estándares.

Posterior a la etapa dos, se encuentra el diseño de las arquitecturas basadas en soluciones Oracle que apoyarán al cumplimiento de los controles seleccionados. La cuarta etapa es el proceso de validación de la propuesta por medio de un juicio de un experto.

IV - RESULTADOS Y RECOMENDACIONES

Antes de abordar en detalle la Circular 014 es importante conocer cuáles fueron los lineamientos que influenciaron su creación y porque la Superintendencia financiera decidió oficializar y exigir el cumplimiento de una regulación basada en estándares internacionales que enmarca los objetivos del negocio dentro del concepto del Control Interno.

1. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO)

COSO, se constituyó en 1985 con el fin ofrecer patrocinio a la Comisión Nacional De Información Financiera Fraudulenta, cuyo propósito es estudiar aquellos factores que dan evidencia a la emisión de información financiera de carácter fraudulento.

COSO es una organización sin ánimo de lucro cuya función es emitir lineamientos a la administración ejecutiva y a diversas entidades con el fin de establecer procesos de negocio basados en la ética, en la eficiencia y eficacia. Es por esto que dicho lineamiento toma la forma de frameworks y guías basados en buenas prácticas fruto de investigaciones, y análisis hechos a profundidad.

1.1. Marco de Control (Informe COSO)

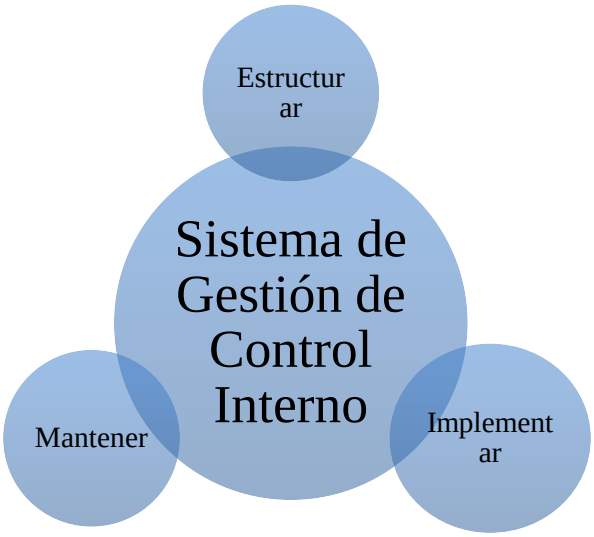
El informe COSO tiene por objetivos(Bae, 2003)[15]:

- Establecer un Marco de Referencia común de Control Interno.
- Dicho Marco debe ser susceptible de evaluación por parte de cualquier organización con el fin de evaluar su Sistema de Control y encontrar la manera de mejorarlo.
- Apoyar a las Directivas de las empresas a optimizar el proceso de control de actividades.

El control interno es un proceso o ciclo (*Ver Ilustración 2*) efectuado por las Directivas, la Gerencia y el personal, con el fin de aportar un nivel aceptable de seguridad en el logro de los objetivos. Esto para garantizar que las operaciones hechas en la organización sean eficientes y eficaces. Para que la información financiera sea correcta y confiable y para garantizar el cumplimiento de leyes y normas pertinentes.

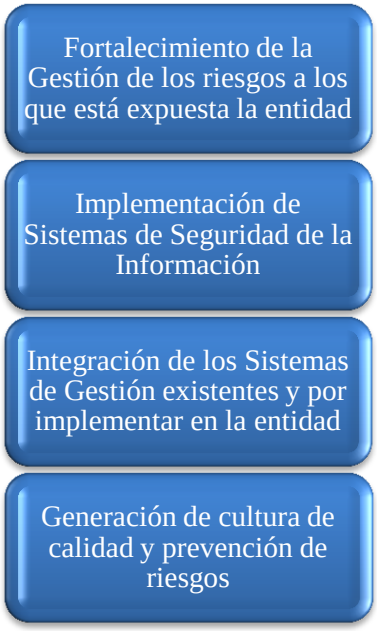
[15] Bae, B. (2003). Internal Control Issues: The Case of Changes to Information Processes.

Ilustración 2: Ciclo del SCI



En la ilustración 2 se observa el ciclo que debe llevarse a cabo para el desarrollo de un Sistema de Control Interno como el que propone COSO. Este sistema surge entonces como solución o instrumento para lograr los objetivos propuestos por la organización y busca esto a través de:

Ilustración 3: Medios para el SCI



Como beneficios la entidad adquiere:

- Incrementar la productividad y competitividad de la entidad.
- Generar confianza e incrementar el reconocimiento de la entidad por parte de sus grupos de interés.
- Fortalecer el proceso de toma de decisiones, fundamentando su gestión en la identificación, prevención y gestión de riesgos y en la mejora continua.
- Clarificar los roles de las diferentes áreas de dirección de los órganos de control involucrados en el Sistema de Control Interno.
- Dar mayor relevancia al rol que desempeña el proceso contable y tecnológico para el soporte de los procesos misionales de la entidad.
- Mayor compromiso por parte de todos los funcionarios de la entidad en el cumplimiento de los objetivos institucionales. Esto es que cada funcionario entienda la importancia de cumplir debidamente con su trabajo para lograr los objetivos de negocio propuestos por las directivas.

COSO no es un proceso secuencial, por el contrario es interoperable, reiterativo y constante.

Como se muestra en la Ilustración 8, COSO cuenta con cinco componentes principales relacionados entre sí como respuesta a la administración adecuada del negocio. Dichos componentes están interconectados con los procesos administrativos formando *"un sistema integrado que reacciona dinámicamente a las condiciones cambiantes."*[Control Interno y Control de Gestión] del entorno que rodean a las organizaciones.

Los componentes son:

Ilustración 4: Componentes del SCI

La descripción detallada de cada uno los componentes se encuentra en el documento llamado "TG_DocumentoFinal.doc" Sección 1.2.1 Marco de Control (Informe COSO).

1.1.1. SOX y El Control Interno

SOX es una ley de los Estados Unidos que surgió debido a una serie de sucesos en el 2001 relacionados con quiebras, fraudes y anomalías en la administración corporativa que puso en duda la veracidad de la información financiera emitida por las empresas. En el 2002 la ley Sarbanes-Oxley fue aprobada con el fin de fortalecer los mecanismos de control de las empresas y retomar la confianza en el proceso de emisión de información financiera.

Para lo anterior busca crear Transparencia en las operaciones, generar controles que aseguren el manejo legal y minimizar riesgos para la alta gerencia. Adicionalmente, busca que las entidades produzcan requerimientos relacionados con la confiabilidad y veracidad de la información financiera así como la calidad de los procesos de emisión de la información y sus controles internos.

Como Funciona SOX.

De SOX se abstraen una serie de interrogantes interrelacionados que buscan generar procedimientos de valoración y mejora del sistema de control, dichos pasos son los siguientes:

Luego de estos pasos se debe llevar a cabo la Implementación de nuevos controles y la actualización y mejora de los existentes para así garantizar un nivel aceptable de confiabilidad, exactitud y disponibilidad en el proceso de emisión de la información financiera.

Ilustración 5: Ventajas de SOX

Y es de esa forma que SOX se convierte en un sistema de Implementación del control interno para verificar y analizar los procedimientos de funcionamiento, garantizar la confiabilidad de la información y la gestión pertinente obteniendo como resultado los aspectos que se muestran en la Ilustración 5.

*"Si bien COSO identifica cinco componentes de control interno, que deberán estar integrados para alcanzar los objetivos de reporte financiero y divulgación, CobiT (*CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY*) proporciona una guía detallada similar pero para TI"*(BDO, 2010)[16]

2. CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (CobiT)

Para el proceso de apoyo al cumplimiento de los controles de la Circular 014 se hará uso de herramientas tecnológicas por lo tanto es necesario abordar el estándar COBIT, el cual apunta hacia el control sobre la inversión en TI, velando por el uso responsable de los recursos tecnológicos, entendiendo, planeando y gestionando los riesgos asociados a esta, y realizando mediciones sobre el despeño con el fin de asegurar que la inversión en TI genere beneficios para la organización.

El gobierno de las TI busca la integración e institucionalización de las buenas prácticas, para lograr sacar el máximo provecho a la información que tienen las empresas, para así maximizar los beneficios obtenidos.

CobiT no expide un certificado que avale el uso de las prácticas indicadas, pero ISACA si brinda un título personal como lo es "Certified Information Systems Auditor" (CISA), "Certi-

[16] BDO. (2010). Adoptando los Modelos de Control Interno COSO y COBIT.

fied Information Security Manager" (CISM) y "Certified in the Governance of Enterprise IT" CGEIT.

Para mayor información remitirse al documento llamado "TG_DocumentoFinal.doc" Sección 1.3 CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)

2.1. Áreas de Enfoque del Gobierno de las TI.

COBIT ofrece un modelo de procesos genéricos que representan los procesos que se encuentran en las funciones de TI, esto ofrece un modelo de referencia común para los gerentes operativos de TI y del negocio, de esta manera se establece un puente entre lo que los gerentes operativos deben realizar y lo que los ejecutivos desean gobernar.

Los objetivos definen las áreas de enfoque que vemos en la ilustración 9.

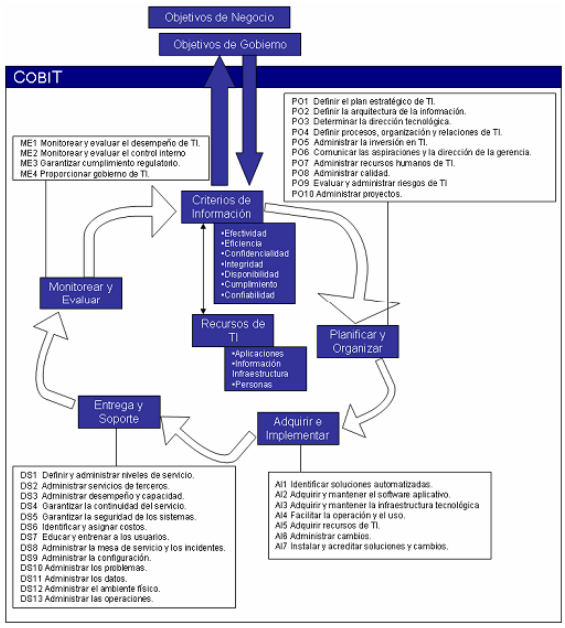
Ilustración 6: Áreas de enfoque del gobierno de las TI.(IT Governance Institute, 2007)[17]

[17] IT Governance Institute. (2007). cobiT4.1. Recuperado el 12 de Septiembre de 2010, de isaca: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

La descripción detallada de cada una de las áreas de enfoque del gobierno de las TI se encuentra en el documento llamado "TG_DocumentoFinal.doc" Sección 1.3.1 Áreas de Enfoque del Gobierno de las TI.

2.2. Marco de Trabajo.

Ilustración 7: Marco de Trabajo completo de CobiT



Tomado de CobiT 4.1 Spanish.(IT Governance Institute, 2007)[18]

CobiT es un marco relacionado con ISO 27001 anexo A y Coso, ya que incorpora aspectos elementales de otros estándares relacionados, debido a esto las empresas que se hayan desa-

[18] Ibíd., p. 16.

rrollado según las prácticas de CobiT están más cerca de adaptarse y lograr la certificación de ISO 27001 (López Neira, Otros Estandares)[19].

3. ISO 27001 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Cuando se habla del Sistema de Control Interno, este no solo incluye aspectos de gestión de riesgos, integración de sistemas y cultura de calidad, sino que además sugiere la idea de implantar un sistema de gestión de seguridad de la información es por esto que a continuación se aborda la norma ISO 27001 la cual se remite directamente a la implantación de un SGSI.

3.1. Seguridad de la Información.

La información es uno de los activos más importantes de una empresa, y es posible que a veces no se lleven a cabo medidas para protegerla y alguna contingencia puede llevar a perderla para siempre.

La tecnología hoy en día juega un papel importante en la operación y vida de una organización, casi todos los procesos en el ámbito de las comunicaciones, producción y gestión de la información dependen en gran medida de ella. Los riesgos a los que la información se enfrenta van desde los daños físicos como desastres naturales o daños humanos hasta los causados por virus, ataques informáticos y daños en infraestructura tecnológica. Y es por esto que las amenazas a las que actualmente están expuestas las organizaciones son cada vez mayores.

"Contar con un sistema 100% seguro es prácticamente imposible, siempre hay cabida a una pequeña posibilidad de que alguien logre hacer más de lo que los administradores de sistemas de cómputo le permitan hacer."(Colombiahosting.com, 2010)[20]

He aquí unas estadísticas relacionadas con la seguridad de la información hoy en día:

- 45% de los empleados se llevan consigo información de la empresa cuando cambia de empleo.(Machines, 2002)[21]
- 97% de los entrevistados se muestra preocupado sobre brechas en la protección de la información.(Institute, 2009)[22]

---

[19] López Neira, A. (s.f.). Otros Estandares. Recuperado el 14 de Septiembre de 2010, de iso27000.es: http://www.iso27000.es/download/doc_otros_estandar_all.pdf

[20] Colombiahosting.com. (2010). La Seguridad de la Información.

[21] Machines, L. (2002). Information Security Survey on Internal Threats.

- 80% de los entrevistados considera que la mayor amenaza humana para la seguridad de la información son personas internas. (Institute, 2009)[23]

Los siguientes porcentajes fueron obtenidos del documento *Seguridad de la Información en Latinoamérica, Tendencias 2009. Jeimy Cano*

- Virus 71%
- Software No Autorizado 61%
- Troyanos 33%
- Acceso No Autorizados 31%
- Manipulación de Aplicaciones 22%

(Cano, 2009)[24]

Las anteriores estadísticas nos muestran que *la Seguridad de la información no es un mito, tampoco moda, es una realidad*.(Deloitte, 2010)[25]. Y es que actualmente el mismo mercado lleva a las organizaciones a contemplar constantemente la protección de la información para sus negocios, la globalización, la tecnología como producto de consumo masivo, etc.

[22] Institute, M. T. (2009). CISO Information Security Survey.

[23] Ibíd., p. 20.

[24] Cano, J. (2009). Seguridad de la Información en Latinoamerica Tendencias.

[25] Deloitte. (2010). Alineando Procesos de Negocio con la ISO27001.

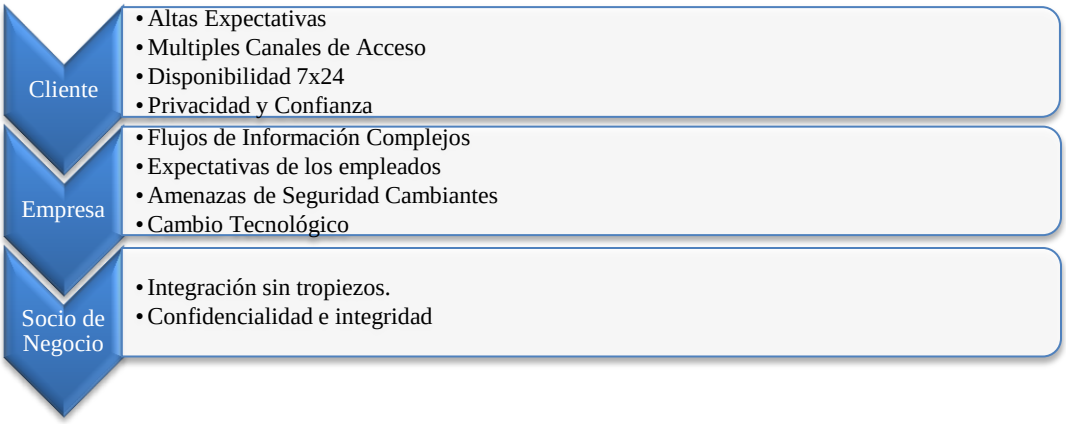


Ilustración 8 Protección de la Información(Deloitte, 2010)[26]

Adicional a las condiciones de mercado, uno de los problemas más significativos *"es que la mayoría de los "especialistas en seguridad" basan sus conocimientos y experticia solamente en el aspecto técnico tradicional de la seguridad, es decir del área IT."* (Meyer, 2010)[27]

Pero obteniéndose un enfoque puramente técnico, lo único que se manejaría serían vulnerabilidades bajo ciertos tipos de plataformas siendo insuficiente para el gran número de riesgos asociados a ellas.

El mejor proceso es llevar a cabo un análisis de riesgos, donde se realiza una valoración de los activos en la organización, una identificación de amenazas relacionadas con las vulnerabilidades de cada uno de los activos. A partir de este proceso es posible iniciar con la identificación de los riesgos. Posteriormente es necesario conocer la manera en la que los riesgos se asumirán, generalmente se busca mitigarlos para lograr un nivel aceptable de funcionamiento, pero que para lo cual se deberán generar e implantar un serie de disposiciones de seguridad.

El proceso sigue realizando un análisis de los riesgos identificados contra un estándar técnico como lo es la ISO27001 (como se verá más adelante), para así poder establecer una serie de controles a implantar de acuerdo a un nivel de implementación definido para reducir dichos riesgos a estados aceptables. Para esto se propone un Sistema de Gestión de la Seguridad de la Información.

[26] Ibíd., p. 21.

[27] Meyer, C. O. (2010). Seguridad Informatica vs Seguridad de la Información.

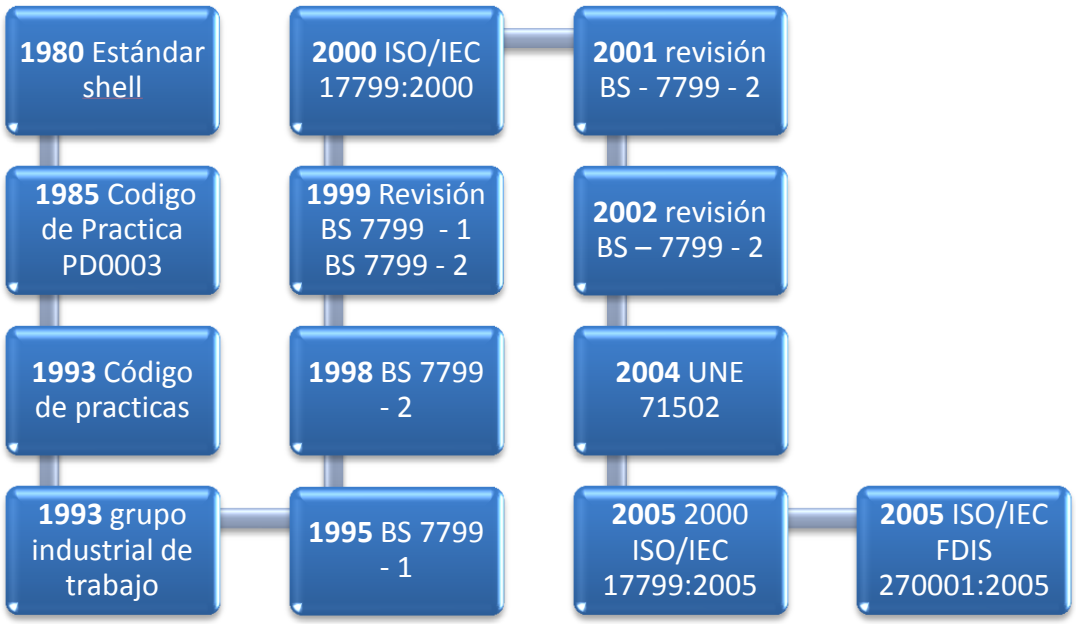
3.2. ISO 27001 y el sistema de gestión de la seguridad de la información.

"*El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías."*(López Neira, iso27000.es el Portal de ISO 27001 en español, 2005) [28]Siguiendo la meta del SGSI podremos garantizar que habrá protección de la confidencialidad, integridad y disponibilidad de la información.

Este estándar fue aprobado y publicado en el año 2005 por ISO, esto con el fin de crear una certificación que se enfocara exclusivamente en la seguridad informática, en el anexo A se encuentran los objetivos de control y controles necesarios para lograr el SGSI (Sistema de gestión de seguridad de la información) el cual es la base sobre la cual se construye la certificación, para llegar finalmente a la ISO 27001 se vivió un proceso de muchos años de evolución y crecimiento de la importancia que llega a tener la seguridad informática en las empresas, en el siguiente grafico podemos observas los elementos que dejaron huella en la creación de la certificación.

Ilustración 9. Evolución de ISO 27001

[28] López Neira, A. (2005). iso27000.es el Portal de ISO 27001 en español. Recuperado el 16 de Agosto de 2010, de http://www.iso27000.es/sgsi.html



Con el apropiado uso de la certificación se logra:

- ✓ reducir o prevenir los riegos relacionados con la información, esto mediante la implantación de controles adecuados, consiguiendo que la empresa esté preparada ante la materialización de una amenaza con lo cual se garantice la continuidad del negocio.
- ✓ Crear un instrumento para la creación del SGSI que considere la estructura organizativa, los recursos, los procedimientos y la política de la empresa.
- ✓ Gestión de la integridad, disponibilidad y confidencialidad.
- ✓ Concientización del personal de la empresa en lo relacionado con la seguridad de la informática más específicamente en la seguridad de la información.

En general "*con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente*"(López Neira, iso27000.es el Portal de ISO 27001 en español, 2005)[29]. Es importante que la seguridad haga parte del diario vivir de la empresa y que se tenga en cuenta desde el cargo más bajo como el más alto de la organización. Adicionalmente si una empresa logra la certificación le será de gran utilidad ya que con ella puede demostrar no solo a nivel nacional sino a nivel internacio-

[29] Ibíd., p. 22.

nal, que cuenta con un sistema de gestión en el campo de seguridad informática, lo cual nos facilitara el hacer negocios con multinacionales ya que algunas de ellas exigen esta certificación para lograr tener una relación comercial.

3.3. Establecimiento del SGSI.

El establecimiento del SGSI consta de las siguientes fases:

3.3.1. Identificación de los Activos de la Información.

Como se vio anteriormente, la estrategia de seguridad busca identificar un nivel aceptable de seguridad acorde con los objetivos de negocio de la organización, sin embargo para establecer dicho nivel es necesario identificar qué activos de la empresa serán objeto de control y verificación, es decir, establecer qué activos se van a asegurar.

Para esto se debe identificar los flujos de información y los datos que pasan a través de ellos, esto se hace en cada uno de los procesos críticos que se hayan seleccionado y a partir de este mecanismo se identifican los activos de información de dichos procesos que serán tratados por el análisis de riesgos.

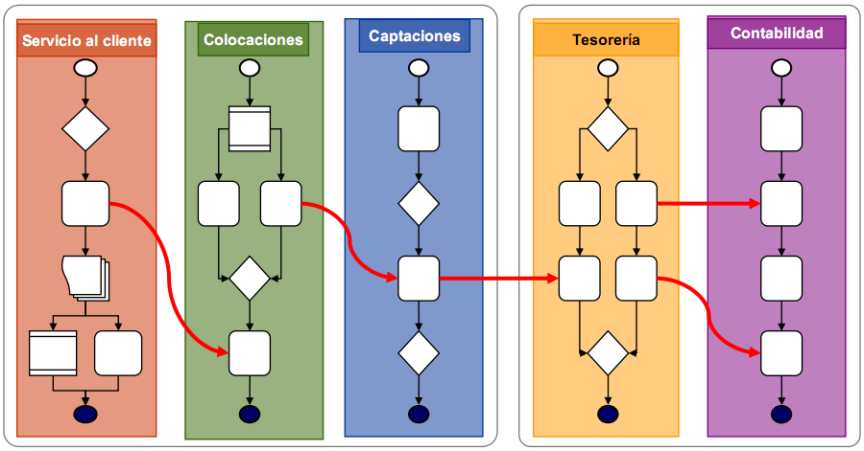


Ilustración 10 Ejemplo Activos de La Información(Deloitte, 2010)[30]

[30] Deloitte. (2010). Alineando Procesos de Negocio con la ISO27001.

Como se muestra en la imagen de arriba, es un ejemplo de algunos procesos de negocio en una organización, allí deben analizarse los flujos de información que atraviesan el proceso en cuestión, validar con el dueño del proceso e identificar los activos asociados a dichos procesos, para su posterior clasificación.

3.3.2. Clasificación de Activos de Información.

Para realizar una clasificación de los activos de información se requiere haber identificado como se explicó anteriormente unos procesos, para cada proceso una serie de activos. Posteriormente se establecen atributos agrupados en categorías que ayudarán a establecer el impacto del activo frente a una característica de la información. En estas categorías se encuentras ejemplos como **C**onfidencialidad, **I**ntegridad y **D**isponibilidad. Cada atributo tendrá un puntaje de acuerdo al impacto en la característica. Totalizando de acuerdo a cada categoría como lo indica la gráfica, quedan agrupados los puntajes de los atributos de acuerdo a **C**onfidencialidad, **I**ntegridad y **D**isponibilidad, para luego establecer un promedio obteniendo como resultado la columna llamada **Valor del Activo,** que contendrá un puntaje que indicará el impacto del activo en el negocio, siendo los puntajes más altos los que obtendrán mayor prioridad.

Proceso	Activo de Información	Atributos									Atributos			Valor del activo
		C			I			D						
		Atributo 1	Atributo 2	Atributo 3	Atributo 1	Atributo 2	Atributo 3	Atributo 1	Atributo 2	Atributo 3	C	I	D	
Proceso 1	Activo 1	5	3	1	3	4	2	3	1	4	3.0	3.0	2.7	2.89
	Activo 2	4	5	4	3	4	3	5	5	4	4.3	3.3	4.7	4.11
	Activo 3	2	3	1	5	3	3	5	3	3	2.0	3.7	3.7	3.11
	Activo 4	3	1	3	1	3	2	3	2	5	2.3	2.0	3.3	2.56
	Activo 5	3	2	1	3	1	3	4	3	4	2.0	2.3	3.7	2.67
	Activo 6	3	3	3	3	3	3	3	3	3	3.0	3.0	3.0	3.00
	Activo 7	1	5	5	3	4	4	5	1	3	3.7	3.7	3.0	3.44

Clasificación según el impacto en cada característica de la información

Clasificación según el impacto del activo al negocio

Ilustración 11 Clasificación Activos(Deloitte, 2010)

3.3.3. Análisis de la Situación Actual.

Actualmente las empresas deben lidiar con diversos aspectos coyunturales, por un lado disponen ellas mismas de una Estrategia de negocio que establece planes y programas de acción, definiendo prioridades y recursos para lograr los objetivos de negocio. Por otro lado se encuentra con la estructura organizacional que define una división del trabajo en la organización alineado con los objetivos de negocio pero limitado por mecanismos de coordinación para ajustar, estandarizar, supervisar y valorar las actividades pertenecientes a las labores operacionales. Y por último se encuentran con un entorno que establece una serie de procesos bajo un marco normativo. Estos tres elementos deben integrarse y alinearse con el fin de trabajar juntos en contexto con la norma ISO27001.

Ilustración 12 Integración del Negocio, Funcionario, Normatividad e ISO27001(Deloitte, 2010)[31]

3.3.4. Análisis de Riesgos y Vulnerabilidades.

Establecer un inventario de activos críticos por proceso no es suficiente para realizar un mecanismo de protección y aseguramiento, también es necesario e indispensable identificar los riesgos asociados a dichos activos, sus vulnerabilidades y las probabilidades de que estos se presenten.

Como se muestra en la siguiente gráfica, con anterioridad ya se cuentan con los procesos y los activos asociados a ellos, lo siguiente a identificar son la vulnerabilidades para cada uno de los activos agrupadas según categorías, pare el caso **C**onfidencialidad, **I**ntegridad y **D**isponibilidad, luego de identificar las amenazas asociadas a los activos y se determina la probabilidad de que una amenaza suceda y explote la vulnerabilidad tratada.

[31] Deloitte. (2010). Alineando Procesos de Negocio con la ISO27001.

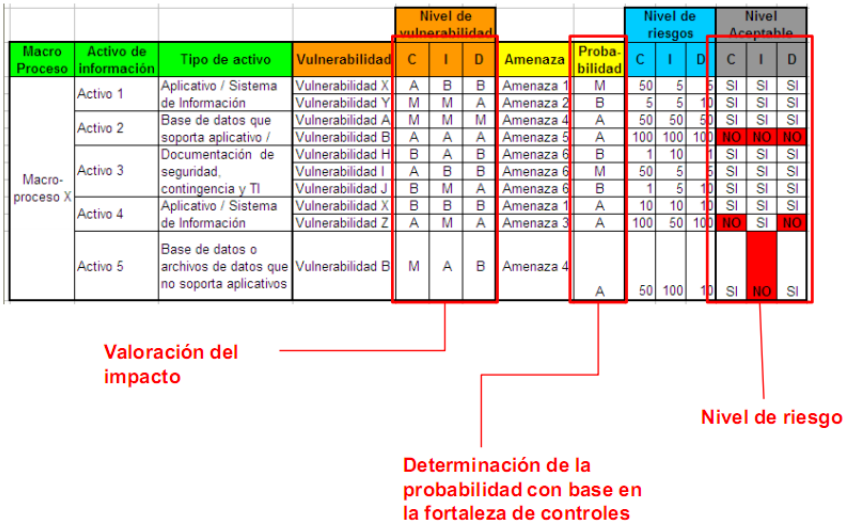


Ilustración 13 Riesgos vs Vulnerabilidades(Deloitte, 2010)[32]

3.3.5. Opciones del Tratamiento del Riesgo.

Las siguientes son las cuatro opciones que propone Deloitte para tratar los posibles riesgos que se presenten(Deloitte, 2010):

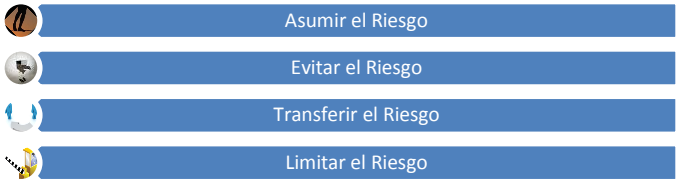


Ilustración 14 Tratamiento del Riesgo(Deloitte, 2010)[33]

- **Asumir el Riesgo**
  "Asumir el riesgo es la opción más arriesgada, es aceptar el riesgo y continuar operando tal como se ha estado haciendo"(Deloitte, 2010)[34]

[32] Ibíd., p. 27.

[33] Ibíd., p. 27.

[34] Ibíd., p. 27.

- **Evitar el Riesgo**
  Una de las más complicadas, "*Eliminar la causa de éste (ej. sacar de producción un activo)"*(Deloitte, 2010)[35]

- **Transferir el Riesgo**
  Va desde transferir la operación y responsabilidad a un tercero o *"Usar opciones que compensen la pérdida (ej. Adquirir seguros o pólizas)"*(Deloitte, 2010)[36] con los costos que esto acarrea.
- **Limitar el Riesgo**
  La más adecuada de todas y la base del modelo ISO27001 que es *"Implementar controles que reduzcan la probabilidad de la amenaza"*(Deloitte, 2010)[37]

3.4. Requisitos de Documentación.

El ISO 27001 especifica que debe contar un mínimo de documentos en cualquier formato (Digital o impreso).

Para conocer cada uno de los documentos deberá remitirse al documento llamado "TG_DocumentoFinal.doc" Sección 1.4.4 Requisitos de Documentación.

Los documentos deben contar con un proceso de verificación y validación para asegurar la calidad de los mismos ya que estos deben ser conocidos por todos los involucrados en el SGSI, que son los miembros de las áreas sometidas al SGSI.

Para lograr la implementación este estándar internacional adopta el modelo PDCA "por sus siglas en ingles Plan-Do-Check-Act", en español seria Planificar-Hacer-Verificar-Actuar.

3.4.1. Ciclo de Vida de la Información.

Con el aumento dramático de la información y la consecuente complejidad en su administración da una idea del porqué *"los sistemas y las soluciones de almacenamiento se desplazan hacia el centro de la infraestructura tecnológica."*(Solla, 2009)[38] . La TI busca ahora generar

[35] Ibíd., p. 27.

[36] Ibíd., p. 27.

[37] Ibíd., p. 27.

[38] Solla, J. L. (2009). Gestión del Ciclo de Vida de la Información.

conciencia del valor actual de la información, su organización y clasificación según importancia y prioridad. De esta forma así como otros procesos de negocio cuentan con un ciclo de vida, la información también lo tiene, donde su valor constantemente cambia desde su creación hasta su fin.

El valor de la información no es constante, este varía de acuerdo a los estados en las operaciones de la organización como por ejemplo:

- Horas o días en las transacciones que generan las ventas.(Solla, 2009)[39]
- Mensuales en el tratamiento de nóminas.(Solla, 2009)[40]
- Anuales en los cierres de ejercicio.(Solla, 2009)[41]

Esto significa que las organizaciones cada vez producen y usan en mayor nivel grande s volúmenes de información, que constantemente modifican, actualizan y mantienen como acción natural al crecimiento del negocio. Adicionalmente se vinculan normativas que obligan a *"establecer un el plazo que hay que mantener salvaguardados los correos y otras informaciones en formato electrónico, así como el tiempo máximo para su recuperación y puesta a disposición del organismo solicitante"*(Solla, 2009)[42]

Entonces a medida que la información crece es necesario establecer un ciclo apropiado que apoyará los cambios de estado y de valor que en ella se presentan y para esto se establece un ciclo de 6 fases como lo muestra la siguiente imagen:

[39] Ibíd., p. 29.

[40] Ibíd., p. 29.

[41] Ibíd., p. 29.

[42] Ibíd., p. 29.

Ilustración 15 Ciclo de Vida de la Información(Deloitte, 2010)[43]

Este ciclo permitirá asociar un estado en el que se encuentra la información con unos procedimientos para tratarla en dicho estado. Estos procedimientos son libremente establecidos por la organización y dependen en gran medida del volumen, tipo y tiempos de vida de la información a tratar.

El punto de partida radica que dentro de la organización se comprenda que la gestión del ciclo de vida la información puede implementarse por etapas, cada una ofreciendo un valor específico, la construcción de esta implementación es secuencial y dependerá del alcance fijado por la organización así como de las arquitecturas tecnológicas existentes. De esta forma como bien la norma ISO27001 requiere que todo proceso se encuentre debidamente documentado, es necesario establecer un ciclo de vida válido y acorde con los requerimientos para toda documentación generada fruto del establecimiento de nuevos procedimientos en la organización.

3.5. Alineamiento Estratégico.

Ya conociendo la estructura formal de la norma ISO 27001, es evidente que se necesita identificar una estrategia de seguridad en las organizaciones para esto es necesario contemplar los

[43] Deloitte. (2010). Alineando Procesos de Negocio con la ISO27001.

diferentes aspectos que la alimentan. Por un lado es necesario establecer los Objetivos de Negocio, que estén debidamente formulados y clarificados, posteriormente se formularán los objetivos de seguridad que estarán alineados con los de negocio, para consecuentemente emitir Políticas corporativas que deberán ser divulgadas en todas la organización.

Para mayor información deberá remitirse al documento llamado "TG_DocumentoFinal.doc" Sección 1.4.5 Alineamiento Estratégico.

Ilustración 16 Estrategia de Seguridad(Deloitte, 2010)[44]

Ya entendiendo el concepto del Sistema de Control interno y su relación con el Sistema de Gestión de Seguridad de la información, a continuación se abordará en detalle la Circular 014, sus objetivos, estructura y controles.

4. Circular Externa 014 del 2009 de la Superintendencia Financiera de Colombia

La superintendencia Financiera controla y supervisa la gestión de las entidades detalladas en los artículos 72 y 73 del Decreto 4327 de 2006 y bajo este contexto emitió la Circular Externa 14 el 19 de Mayo de 2009, titulándola *"Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno"* realizando un recalcando la importancia del papel que tiene el Sistema de Control Interno (SCI) como instrumento fundamental del gobierno corporativo de las entidades. La exigencia de su adopción inició el 30 de septiembre de 2009.

[44] Deloitte. (2010). Alineando Procesos de Negocio con la ISO27001.

La emisión de la circular busca presentar un conjunto de requerimientos y recomendaciones técnicas y metodológicas con el fin de hacer cumplir un modelo de gestión relacionado con las actividades a desarrollar propias del control interno de las entidades.

La circular 14 hereda aspectos fundamentales del Modelo Estándar de Control Interno (MECI) establecido en el Decreto 1599 de 2005 y aplicabilidad en el sector público. Su alcance es bastante grande incluyendo:

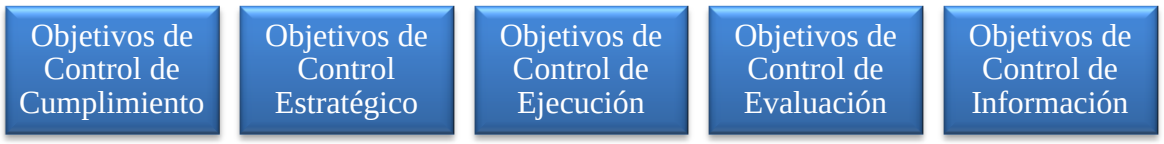
- Tareas
- Funciones
- Responsabilidades

Todas ellas propias de los Directivos, Auditores Internos, Departamento de Tecnología, Administración del Riesgo. De esta forma MECI propone una estructura para realizar control en la gestión, en la estrategia y valoración de las entidades esto con el fin de orientarse hacia el cumplimiento de los objetivos de la institución.

El Modelo MECI se formuló con el propósito de que las entidades pudieran mejorar su desempeño día a día fortaleciendo los procesos control y evaluación. Para esto (similar a la Circular 014) las entidades deben llevar a cabo una valoración que arrojará un nivel de efectividad de los elementos de control con los que cuenta, con el fin de realizar una etapa de diseño, desarrollo o incluso de ajuste para su implementación o mejora según sea el caso.

Sin embargo, es importante aclarar los objetivos fundamentales del Modelo Estándar de Control Interno (MECI), estos se agrupan en 5 Grandes Áreas u Objetivos de Control:

Ilustración 17: Objetivos de Control MECI



La descripción detallada de cada uno los objetivos de control MECI se encuentra en el documento llamado "TG_DocumentoFinal.doc" Sección 1.5 Circular Externa 014 del 2009 de la Superintendencia Financiera de Colombia

Bajo este marco de control que aporta MECI es en el cual *en parte* se basa la Superintendencia Financiera para emitir circular 14 donde evaluará el cumplimiento de las exigencias que en ella se nombran pero de acuerdo a su propio modelo de supervisión.

En dicha Circular se establece de manera obligatoria la realización de informes periódicos en cada etapa de cierre e informes de avance sobre cada temática. De esta manera la Superintendencia Financiera busca constatar la existencia de documentación formal como Políticas, procedimientos y normas. Así como la implementación real en los sectores relacionados. Para tal fin la Superintendencia Financiera cuenta con un documento mayor que evaluará a manera de CheckList los aspectos a revisar durante su visita.

La circular externa 014 busca no solo los administradores de las entidades vigiladas o sometidas al control exclusivo de la Superintendencia Financiera de Colombia cumplan con un sistema de control interno, sino que las entidades Financieras también lo hagan llevando a cabo una serie de procedimientos, normas, políticas y mecanismos que entregarán un nivel de seguridad adecuado para la organización y para aquellas entidades que interactúen con ella.

Dentro de la circular 14 se establece:

- Ámbito de Aplicación
- Objetivos
- Elementos del Sistema de Control.
- Procedimientos para la gestión de riesgos.
- Órganos responsables de verificar la implementación y cumplimiento del SCI.
- Mecanismos y procesos de seguimiento.

Adicionalmente afirma que son los representantes legales de la organización tienen a cargo establecer y mantener los sistemas de revelación, los de control y además el proceso de diseño y operación de los controles internos.

El cumplimiento de la circular 14 es posible solo con la implantación de un SCIF (Sistema de Control Interno Efectivo) el cual permitiría la detección y remedio de los vacíos que existen entre los riesgos que la compañía afronta y los controles establecidos para prevenir o mitigar esos riesgos.

Este sistema busca contribuir al logro de los objetivos empresariales y fortalecer la administración de los riesgos a los que las empresas están expuestas a diario en sus actividades ofreciendo entornos de seguridad y eficiencia.

Los registros de fracasos y crisis en el sector empresarial han mostrado que la gerencia toma riesgos sin los controles correspondientes. Es por esto que con un nuevo enfoque del control interno se puede corregir esta falla llevando a cabo controles en cada uno de los procesos administrativos y estableciendo un Ambiente de Control que incentive los principios y buenas conductas orientadas al control.

En este caso las directivas juegan un papel crucial para transferir liderazgo y compromiso haciendo hincapié en la gran importancia de los controles internos y las responsabilidades que deben ser asumidas por cada uno de los funcionarios de acuerdo al sistema de control interno. Por lo tanto se habla de un control preventivo donde se reúnen aspectos fundamenta-

les de la organización como la estrategia, reglamentos, información para tomar decisiones, etc. De esta manera las directivas, jefes y empleados tendrán la capacidad para administrar los riesgos de la empresa, estableciendo con antelación un Sistema de Control Interno.

Claro está que el Sistema de Control Interno se basa en que cada uno de los funcionarios de la empresa control su trabajo con el fin de detectar fallas para después ejecutar acciones correctivas en sus funciones y proporcionar mejoras a las operaciones.

Bajo este contexto los auditores juegan dos papeles importantes para el mantenimiento del Sistema de Control interno. Por una parte, la auditoría interna es un aspecto fundamental para el mejoramiento del sistema, detectando irregularidades, gestionando riesgos, amenazas y proporcionando un monitoreo constante de los procesos internos. La auditoría externa ofrece un nivel adecuado de seguridad a terceros referente a la confiabilidad de la certificación que tiene la empresa para comprobar la efectividad de su Sistema de control Interno.

4.1. Elementos y Estructura de la Circular 14.

Como ya se ha explicado con anterioridad, todas las entidades supervisadas, deberán implementar un Sistema de Control Interno de nivel aceptable que la circular establece en sus capítulos. Y se espera que dicho sistema sea acorde con el tamaño de la empresa es decir que se deberá tener en cuenta el número de empleados, activos e ingresos, número de sucursales, etc. (Superintendencia Financiera de Colombia, 2009)[45].

La Circula Externa 014 en su sección 7.4 explica lo que para la Superintendencia Financiera son los principios del Sistema de Control Interno, siendo tres como se muestra a continuación:

Para obtener un mayor detalle de cada uno de los tres principios, debe remitirse al documento llamado "TG_DocumentoFinal.doc" Sección 1.5.1 Elementos y Estructura de la Circular 14

1) Autocontrol

El autocontrol va directamente relacionado a que cada empleado en la organización pueda *"evaluar y controlar su trabajo"*(Superintendencia Financiera de Colombia, 2009)[46], y si

[45] Superintendencia Financiera de Colombia. (19 de Mayo de 2009). Normativa. Recuperado el 16 de Agosto de 2010, de Superintendencia Financiera de Colombia: http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ance014_09.doc

[46] Ibíd., p. 35.

detectará un error pueda efectuar una actividad de corrección en sus funciones, a esto se le agrega también, la capacidad de optimizar tareas y responsabilidades asignadas.

2) **Autorregulación**

Hace referencia a que la organización debe estar en capacidad de generar lineamientos, normas e instructivos que permitan que el Sistema de Control Interno pueda ser desarrollado, implementado o mejorado según sea el caso.

3) **Autogestión**

La autogestión hace referencia a que la organización este en capacidad de *"interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento."*(Superintendencia Financiera de Colombia, 2009)[47].

Para que haya un cumplimiento efectivo de los principios mencionados anteriormente así como los objetivos del SCI tratados, las organizaciones tendrán que crear una *"estructura de control interno"*(Superintendencia Financiera de Colombia, 2009)[48] que esté basado en los elementos del SCI propuesto por el Modelo COSO, ya explicados en secciones anteriores, sin embargo señálemelos desde la perspectiva de la Circula 014:

- **Ambiente de Control**

  La Circular 14 se refiere a este como *"políticas y procedimientos que deben seguirse para lograr que las instrucciones de la administración con relación a sus riesgos y controles se cumplan. Las actividades de control se distribuyen a lo largo y a lo ancho de la organización, en todos los niveles y funciones."*(Superintendencia Financiera de Colombia, 2009)[49]

- **Análisis de Riesgo:**

  Este componente comprende una etapa de identificación y otra de análisis de los riesgos más importantes a los que se verían comprometidos los objetivos de negocio de la organización y que servirá como base para conocer la manera en la que esos riesgos serán manejados.

[47] Ibíd., p. 35.

[48] Ibíd., p. 35.

[49] Ibíd., p. 35.

- **Actividades de Control:**

  La Circular 014 afirma que *"las actividades de control son las políticas y los procedimientos que deben seguirse para lograr que las instrucciones de la administración con relación a sus riesgos y controles se cumplan."*(Superintendencia Financiera de Colombia, 2009)[50].

  Las actividades de control que sean consideradas cumplirán una relación costo/beneficio y estarán apoyadas en políticas que enseñaran qué hay que hacer y cómo hacerlo.

- **Información y Comunicación:**

  La Circular 014 expresa que es indispensable *"identificar, capturar e intercambiar información en una forma y período de tiempo que permita al personal cumplir con sus responsabilidades."*(Superintendencia Financiera de Colombia, 2009)

  Información
  El sistema de información debe suministrar información suficiente para poder controlar los objetivos de negocio establecidos, la Circular 014 propone las siguientes:

  Comunicación:
  La organización debe garantizar un nivel de comunicación bastante alto para que esta se propague en todas las áreas de la organización.
  De esta forma, cada empleado deber saber exactamente qué rol desempeña dentro del Sistema de Control Interno y ser consciente que las actividades que realiza dependen de las de otros y viceversa.

- **Monitoreo:**

  La Circula 014 define a este componente como *"el proceso que se lleva a cabo para verificar la calidad de desempeño del control interno a través del tiempo"*(Superintendencia Financiera de Colombia, 2009)[51]. Lo anterior se logra con un proceso de valoración continua en cada una de las áreas o procesos liderados por cada uno de los jefes responsables. La circular externa hace hincapié en que el SCI debe ser dinámico para que siempre pueda adaptarse a las condiciones de la empresa

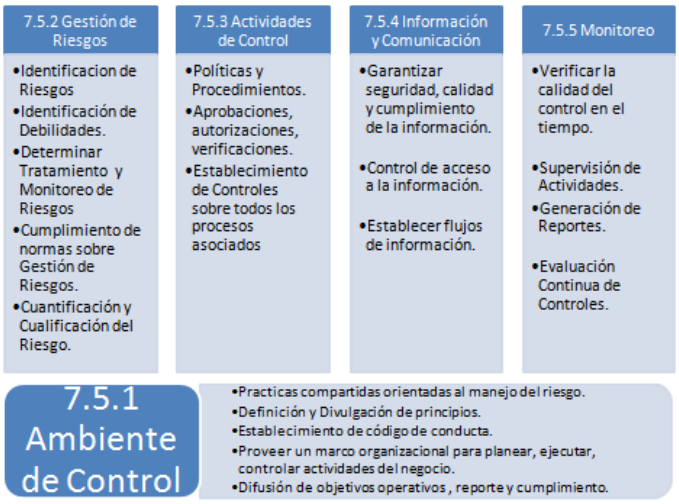
[50] Ibíd., p. 35.

[51] Ibíd., p. 35.

y al entorno en el que opera. Lo cual implica una evaluación de calidad y desempeño del sistema con sus correcciones pertinentes.

La siguiente Ilustración muestra un resumen los elementos del SCI propuesto por la Circular 014.

Ilustración 18: Elementos del SCI en la Circular 14 (Oracle, 2009)



4.2. COSO y la Circular 014.

Con el paso de los años se ha presentado un interés sobre la importancia del control interno como elemento fundamental de las grandes organizaciones y así mismo se han generado una serie de herramientas que ayudan a las directivas de las entidades a ejercer dicha función de una manera más fácil y efectiva. Es por esto que existe una estructura bien conceptualizada sobre el control interno junto con varios enfoques teóricos disponibles.

"Desde septiembre de 1992 el control interno ha constituido un fenómeno mundial y su aceptación ha ido creciendo en todos los sectores vinculados con los negocios."(Grupo Inversión, financiación y control Universidad Icesi, 2010)[52]

Con la emisión de la ley Sravane-Oxley de 2001, las grandes organizaciones y entidades auditoras adoptaron el enfoque propuesto por el modelo COSO para así cumplir con esta regulación y es a partir de esta donde se generan herramientas orientadas para su implantación.

[52] Grupo Inversión, financiación y control Universidad Icesi. (Enero de 2010). Universidad ICESI. Recuperado el 15 de Agosto de 2010, de http://www.icesi.edu.co/departamentos/finanzas_contabilidad/images/proyectos/control_interno.pdf

Gracias a esto, los empresarios se vieron en la necesidad de establecer ciertos elementos que garantizarán un mínimo de control dentro de la organización.

De esta forma, debieron transcurrir casi 20 años para que la Superintendencia Financiera de Colombia tuviera en consideración aquellos estándares de carácter internacional referentes al control interno como un requisito indispensable de cumplimiento de las organizaciones que están bajo su supervisión y control.

Y para mayo de 2009, se promulga la Circular Externa 014 de 2009, circular que hace alusión al compromiso en el que se encuentran las organizaciones que están supeditadas al control y vigilancia de la Superintendencia Financiera. Dicho compromiso se entiende como la especificación de políticas y diseño de una serie de procedimientos de control interno que deberán ser implementados dentro de la entidad, esto con el fin de permitir, mejorar y garantizar el cumplimiento de sus objetivos de negocio. En esta circular se "*compila toda la normatividad dispersa sobre control interno y estructura un documento formal y completo sobre el tema de aplicación forzosa en Colombia para empresas emisoras de títulos valores."*(Grupo Inversión, financiación y control Universidad Icesi, 2010)[53]

El hecho de haberse emitido la Circular Externa, indica que se ha iniciado un proceso de verificación, estandarización y encuentro de los modelos de control interno, y es la Superintendencia Financiera quien sugiere la utilización de la guía de COSO*(Committe Sponsoring Organization of the Treadway)* como apoyo a dicho proceso de implantación. A continuación se explicará el porqué de la Circular Externa 014, sus antecedentes y la importancia de esta más allá del entorno regulatorio que la rodea.

4.3. ISO 27001 y la Circular 014.

Tanto en la Circular 014 como en la norma ISO27001, la palabra *control* se refiere a una serie de acciones, a documentación, adopción de medidas, procedimientos y técnicas de medición. Tanto para Circular 014 como para la ISO27001 un control *"es lo que permite garantizar que cada aspecto que se valoró con un cierto riesgo, queda cubierto y auditable"*(Estrada, 2006)[54]

En este sentido la Circular 014 y la ISO 27001 buscan establecer *una "definición común del control interno"*(Mantilla, 2005)[55], es decir que ambas proponen un marco de referencia con el fin de proporcionar un cierto grado de seguridad para la consecución de objetivos.

[53] Ibíd., p. 38.

[54] Estrada, A. (2006). ISO27001: Los Controles.

[55] Mantilla, S. A. (2005). Auditoría del control interno.

Así que sobre un Activo de Información previamente identificado fruto de los lineamientos de la ISO27001 se llevará a cabo la aplicación de los cinco componentes básicos del sistema de control interno en el que se basa la Circular 014 (Explicados con anterioridad):

Ilustración 19SCI y los Activos de la Información

De manera análoga *"Se trata de ejercer el control interno sobre nuestros principales activos mediante un ciclo de mejora continua"*(Security, 2010)[56] como se muestra a continuación:

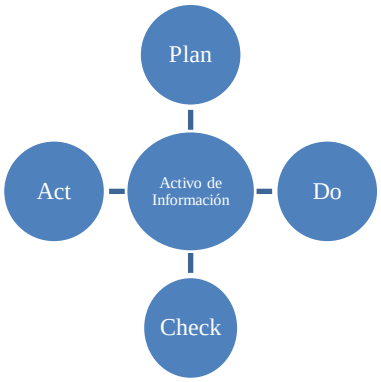


Ilustración 20 Ciclo de Mejora Continua - Activos de Información

[56] Security, E. (2010). ISO 27001 • Certificación de la Gestión de la Seguridad de la Información • Implantación SGSI.

Plan: Definir la política de seguridad basada en los activos identificados, definir el alcance del Sistema de Gestión de la Seguridad, realizar el análisis de riesgos correspondiente para los activos identificados, selección de controles para la mitigación de los riesgos identificados.

Do: Implantación del Plan de Gestión de Riesgos .Implantación de controles.

Check: Revisión interna del Sistema de Gestión de Seguridad por medio de auditorías.

Act: Aplicación de las Acciones Correctivas y Preventivas.

De esta forma se observa la relación que tiene el SCI propuesto en la Circular 14 junto con el proceso de mejora continua que se llevaría cabo por la ISO 27001 contra los activos de la información identificados en la organización.

4.4. Circular 014 y los Controles Tecnológicos.

Para conocer los controles tecnológicos que propone la circular 014 debe remitirse a la sección 7.6.2 de la misma.

5. Alineación Circular 014 de 2009, ISO 27001:2005 Anexo A, Cobit y COSO.

La siguiente tabla ilustra la alineación correspondiente entre la Circular 014, la norma ISO27001 Anexo A, Cobit y COSO. Para acceder a la totalidad de la alineación debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 1.6 *"Alineación Circular 014 de 2009, ISO 27001:2005 Anexo A, Cobit y COSO".*

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A	CobiT	COSO
7.6.2	Normas de Control Interno para la gestión de la Tecnología			
I	**Plan estratégico de tecnología.**			
	i. Análisis de cómo soporta la tecnología los objetivos del negocio.	• A.7.1.1 Inventario de Activos • A.10.5.1 Back-up o respaldo de la información • A.10.6.1 Controles de red • A.10.6.2 Seguridad de servicios de red • A.10.7.1 Gestión de Medio removibles. • A.10.7.4 Seguridad de Documentación del Sistema • A.10.8.3 Medio Físicos en Tránsito • A.10.8.4 Mensajes electrónicos. • A.10.9.1 Comercio Electrónico. • A.10.9.2 Transacciones en línea. • A.10.9.3 Información Disponible Públicamente • A.11.4.2 Autenticación de usuario para conexiones externas • A.11.4.6 Control conexión de redes. • A.11.4.7 Control de Routing de redes.	• PO1 Definir un Plan Estratégico de TI. • PO2 Definir la Arquitectura de la Información. • PO3 Determinar la Dirección Tecnológica. • PO4 Definir los Procesos, Organización y Relaciones de TI. • PO5 Administrar la Inversión TI. • PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia.	• A.7.1.1 Inventario de Activos

6. Soluciones Tecnológicas

En la presente sección se expondrá los requerimientos que deberían cumplir aquellas herramientas tecnológicas que puedan apoyar el proceso de cumplimiento de los objetivos de control analizados con anterioridad, pertenecientes a la Circular 014 y al Anexo A de la norma ISO 27001. Para este capítulo se busca ser lo más genérico posible, para evaluar de manera imparcial las necesidades que deberán suplir las soluciones tecnológicas a elegir.

6.1. NECESIDADES TÉCNICAS GENERALES A CUMPLIR EN LA CIRCULAR 14 SECCIÓN 7.6

Para entender en mayor medida las necesidades técnicas debe referirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 2.1 NECESIDADES TÉCNICAS GENERALES A CUMPLIR EN LA CIRCULAR 14 SECCIÓN 7.6

6.1.1. Cifrado y Enmascaramiento.

A nivel mundial existen una serie de requerimientos de seguridad que se aplican en diferentes países como lo son PCI-DSS, HIPAA y la ley 201 CMR 17.00 orientados a la protección de la información sensible. Y debido a esto es necesario contar con soluciones que permitan realizar cifrado en los datos de las Bases de Datos con las que cuentan las organizaciones, para que de esta forma se controle y proteja el acceso a ellos a través del sistema operativo o a través de los backups.

6.1.2. Control de Acceso.

El control de acceso además de ser implementado a nivel de aplicación debe serlo a nivel de capa de datos, esto debido a que las *"organizaciones se mueven hacia la consolidación de datos, la tercerización y la computación en la nube"*(ORACLE, 2010)[57] y porque las regulaciones y leyes de privacidad así lo requieren. Siguiendo esta visión, con una protección a nivel de datos provee una seguridad adicional cuando existe un uso inadecuado de los privilegios o cuando estos han sido obtenidos por individuos ajenos a la organización.

[57] ORACLE. (2010). Conceptos de Seguridad.

6.1.3. Monitoreo y Auditoría.

La dinámica y movimiento en el que las empresas se encuentran inmersas hoy en día, como resultado de la competencia que se hace cada vez mayor, debido a los procesos de globalización derivan en una mayor exigencia de control y calidad de las tecnologías que intervienen en los sistemas productivos de la empresa, en consecuencia es necesario la captación, almacenamiento y comunicación de los cambios en el entorno, que permitirán aplicar las estrategias correctivas para cada caso.

6.1.4. Continuidad del negocio.

Los sistemas de información en las empresas día a día se convierten en un elemento críticos, debido a la necesidad de acceso a sus datos desde cualquier lugar y en cualquier momento, lo que hace que sea indispensable que exista un servicio ininterrumpido de los mismos para el mantenimiento de las actividades del negocio sin ningún tipo de perdida.

6.1.5. Gestión Documental.

Contar con un buen sistema de gestión documental que permita la recepción, distribución, consulta, organización, y recuperación de los documentos es de vital importancia para las empresas, ya que dinamizan los procesos informativos, la toma de decisiones basadas en antecedentes, por otra parte la regulación Colombiana exige la gestión documental como lo dicta "La Ley 594 de 2000 - Ley General de Archivos, reguló en su Título V: Gestión de documentos, la obligación que tienen las entidades públicas y privadas que cumplen funciones públicas, en elaborar programas de gestión de documentos, independientemente del soporte en que produzcan la información para el cumplimiento de su cometido estatal, o del objeto social para el que fueron creadas"(Archivo General de la Nacion, 2010)[58]

6.2. COMPONENTES ORACLE

Ya entendiendo las necesidades tecnológicas que apoyarán el cumplimiento de controles, se muestra en este capítulo el mapeo de dichas necesidades a soluciones bajo plataforma ORACLE.

A continuación se listan los productos Oracle con los cuales se trabajaron para construir las arquitecturas propuestas. Para conocer la descripción del producto debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc" Sección 2.2 *"Componentes Oracle"*.

[58] Archivo General de la Nacion. (29 de 10 de 2010). Programa de Gestión Documental (PGD). Recuperado el 30 de Octubre de 2010, de Archivo General de la Nacion: http://www.archivogeneral.gov.co/index.php?idcategoria=1232

6.2.1. Cifrado y Enmascaramiento.

Oracle Data Masking Pack.

Las Organizaciones precisan compartir datos de producción con usuarios internos y externos con diferentes propósitos, como el de realizar pruebas a las aplicaciones, en muchos casos estos datos contienen información sensible que queda expuesta y pude ser usado con fines maliciosos. Con Oracle Data Masking es posible suplir esta necesidad de compartir estos datos con entidades internas y externas pero garantizando que los datos no sean revelados, pero que de igual manera sean válidos para las pruebas y otros usos que se le den.

Oracle Advanced Security Option.

Oracle Advanced Security ofrece una solución completa y fácil de implementar para la protección de las comunicaciones hacia y desde la base de datos.

6.2.2. Control de Acceso.

Oracle DatabaseVault.

Con DatabaseVault se protege la información sensible para que no sea vista por el administrador de la base de datos. Información sensible como datos relacionados con los ciudadanos, socios, empleados y clientes.

Oracle Identity Management.

Identity Management permite a las empresas administrar el ciclo de vida de la identidad de los usuarios a través de todos los recursos de la empresa dentro y más allá de los firewall. De esta forma puede hacerse un deploy de aplicaciones rápido y posteriormente aplicar una protección granular a los recursos.

6.2.3. Monitoreo y Auditoría.

Oracle Enterprise Manager y Oracle Enterprise Manager Grid Control.

Oracle Enterprise Manager es una solución para mantener una configuración segura en instalaciones Oracle y escaneos periódicos para configuraciones relacionadas con seguridad. Provee así una gestión de la configuración y una automatización de los procesos de TI de manera centralizada.

Oracle AuditVault.

Audit Vault es un motor de auditoría que busca detectar, monitorear, consolidar y generar alertas y reportes de los datos de auditoría de todos los sistemas con los que se cuente incluso si no son productos Oracle.

Database Firewall.

Con Database Firewall es la primeria línea de defensa, el cual provee un monitoreo en tiempo real de la actividad de la base de datos en la red. Con este firewall es posible bloquear transacciones no autorizadas ayudando a prevenir ataques internos y externos, antes de que alcancen la base de datos.

Oracle Diagnostic Pack.

Oracle Diagnostic Pack es un motor de diagnóstico automático dentro de la base de datos. Este producto permite analizar problemas de desempeño en la base de datos liberando de trabajo adicional a los administradores.

6.2.4. Continuidad del Negocio.

Oracle Real Application Clusters (RAC).

Oracle Real Application Clusters permite que varias terminales puedan ejecutar software de una base de datos Oracle mientras se accede a una base de datos individual, esto es conocido como una base de datos en clúster. Permitiendo que dos o más computadores accedan de forma concurrente a una base de datos individual, permitiendo que un usuario e incluso una aplicación se conecte a alguno de esos computadores y obtenga acceso a los mismos datos.

Oracle Data Guard (DG) y Oracle Active Data Guard (ADG).

Con Oracle Data Guard se asegura alta disponibilidad, protección de datos y recuperación del desastre para los datos de las empresas. Data Guard provee un conjunto de servicios para crear,

mantener, administrar y monitorear una o más bases de datos para soportar desastres y corrupción de datos.

Oracle Golden Gate.

Oracle Golden Gate fue diseñada para proveer soluciones de integración de datos en tiempo real con una sobrecarga mínima de la infraestructura de TI, una de sus características más notables es su capacidad de configuración, la cual le permite realizar integraciones heterogéneas entre diferentes bases de datos, sistemas operativos y servidores de manera bidireccional.

6.2.5. Gestión Documental.

Oracle Enterprise Content Management (ECM).

Oracle Content Management provee una solución para todos los tipos de contenido que la administración necesita. Desde un servidor de archivos hasta la administración de contenido web

Oracle Information Rights Management (IRM).

Oracle IRM permite implantar Políticas Corporativas de Seguridad Documental.

6.2.6. Alineación de la Circular 014 de 2009 de la Superintendencia Financiera y las ISO27001 con los productos ORACLE seleccionados.

El propósito de esta sección es presentar de manera lógica y ordenada los controles tecnológicos de la Circular 014 de la Superintendencia Financiera y los objetivos de control relacionado del Anexo A de la norma ISO 27001, sumándole a esto se sugiere un producto Oracle que apoyará el cumplimiento de los controles respectivos.

La tabla está organizada de la siguiente manera:

La primera columna contiene los controles tecnológicos de la Circular 014, la segunda columna contiene los objetivos de control del Anexo A de la norma ISO 27001 que están relacionados con la Circular 014, y la tercer y última columna presenta el producto que apoyara el cumplimiento de los controles analizados en la fila de consulta.

Para acceder a la totalidad de la alineación debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 2.3 *"Alineación de la Circular 014 de 2009 de la Superintendencia Financiera y las ISO27001 con los productos ORACLE seleccionados".*

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A	Soluciones Oracle
7.6.2	Normas de Control Interno para la gestión de la Tecnología		
I	**Plan estratégico de tecnología.**		
	i. Análisis de cómo soporta la tecnología los objetivos del negocio.	• A.7.1.1 Inventario de Activos • A.10.5.1 Back-up o respaldo de la información • A.10.6.1 Controles de red • A.10.6.2 Seguridad de servicios de red • A.10.7.1 Gestión de Medio removibles. • A.10.7.4 Seguridad de Documentación del Sistema • A.10.8.3 Medio Físicos en Tránsito • A.10.8.4 Mensajes electrónicos. • A.10.9.1 Comercio Electrónico. • A.10.9.2 Transacciones en línea. • A.10.9.3 Información Disponible Públicamente • A.11.4.2 Autenticación de usuario para conexiones externas • A.11.4.6 Control conexión de redes. • A.11.4.7 Control de Routing de redes.	

7. ARQUITECTURAS PROPUESTAS

Esta sección presenta una descripción de varias arquitecturas genéricas para medianas y grandes empresas con el objetivo de transmitir una visión global de un conjunto de ambientes y soluciones de software de la manera más estructurada posible que buscan acercar a las empresas al cumplimiento de los requerimientos tecnológicos de la Circular 014 de 2009 de la Superintendencia Financiera de Colombia y los objetivos de control del Anexo A de la norma ISO27001.

Con las arquitecturas propuestas las empresas lograrán automatizar muchos de los procesos que en el mejor de los casos se hace manualmente, como copias de seguridad y conservación de la información, procesos que son vitales para la continuidad del negocio.

Al establecer diferentes niveles de seguridad como la protección de acceso, cifrado de datos, gestión de identidad y gestión documental, se mitigarán los riesgos de un fallo total del sistema.

"Para ampliar el alcance de las arquitecturas se decidió diseñarlas y agruparlas de acuerdo al tamaño de las empresas objetivo, es decir para medias y grandes empresas. Partiendo de que "las medianas empresas tienen la misma necesidad de proteger sus datos tanto como las grandes; la única diferencia es que cuentan con menos recursos para hacerlo", afirma Mike Karp, analista jefe de Ptak, Noel & Associates. En cualquier empresa, si los datos están comprometidos o son inaccesibles por alguna razón, su actividad se detendrá en poco tiempo. "El interrogante es cuánto tiempo puede funcionar sin tener acceso a los datos" y de esto dependerá el tipo de arquitectura a elegir."(Alan, 2010)[59]

De manera adicional, se cuentan con algunos consolidados orientados a ofrecer una mayor información respecto al alcance de cada una de las arquitecturas. Es por esto que se incluye:

- **Tabla de apoyo al cumplimiento:** Muestra cada uno de los controles de la Circular 014 y del Anexo A de la ISO27001 que la arquitectura propuesta apoyará para el proceso de su cumplimiento (los controles).

- **Cifras de apoyo al cumplimiento:** Por cada arquitectura se presentan dos tipos de gráficos que muestran en términos porcentuales la capacidad con la que cuenta la arquitectura en el proceso de apoyo del cumplimento de los controles tecnológicos de la Circular 014 y del Anexo A de la norma ISO27001.

[59] Alan, R. (2010). Guía paso a paso: protección de datos. Recuperado el 20 de 11 de 2010, de http://i.dell.com/sites/content/business/smb/sb360/es/Documents/0910-mx-catalyst-4.pdf

7.1. Arquitecturas Para Mediana Empresa

La adopción de tecnologías por parte de la pequeñas y medianas empresas para lograr el cumplimiento de la leyes Colombianas esta dictaminada por muchos factores, entre ellos está la viabilidad económica, que en algunos casos por buscar un ahorro puede llevar a la adopción de tecnologías riesgosas (no probadas o con muy poco tiempo en el mercado) o poco efectiva o eficiente que implican una mayor probabilidad de fallo.

Teniendo en cuenta esto las arquitecturas propuestas para la mediana empresa cuenta con soluciones inteligentes y asequibles de Oracle, que poseen la misma funcionalidad, rendimiento y seguridad de sistemas de mayor magnitud, cuenta con tecnologías innovadoras, las mejores prácticas de la industria y la suficiente madurez y confiabilidad en el mercado, adicionalmente estudios realizados mundialmente como vemos en la siguiente tabla indican que Oracle es el líder mundial desde el 2006 en RDBMS con una cuota del mercado en el 2009 de 48%, lo cual nos indica que un enorme porcentaje del as empresa que aplicaran la circular 014 contaran con las Bases de datos ORACLE, las cuales son la base de las arquitecturas propuestas.

Tabla 5: Reporte de cuota del mercado de RDBMS a nivel mundial

Año	Cuota del Mercado
2006	47.1%
2007	48.6%
2008	48.9%
2009*	48.0%

Tomado de Busika.com (ThanosTP, 2009)

*Tomado de (Oracle, 2010)[60]

[60] Oracle. (2010). Oracle is #1 in the RDBMS market for 2009. Recuperado el 20 de 11 de 2010, de Oracle: http://www.oracle.com/us/products/database/number-one-database-069037.html

7.1.1. ARQUITECTURA ORIENTADA A LA CONTINUIDAD DEL NEGOCIO

La arquitectura de continuidad de negocio está dirigida a pequeñas y medianas empresas que cuentas o planean adquirir las versiones más básicas de aplicaciones Oracle, partiendo de las base de datos Standard Edition. Con esta arquitectura se busca mantener la funcionalidad de la organización en un nivel mínimo considerable, contando con medidas preventivas y de recuperación ante los posibles riesgos a los que la compañía este expuesta.

De esta forma se incluye Real Application Cluster (RAC) para ejecutarse una única base de datos en varios servidores proporcionando tolerancia a fallos y mejorando el rendimiento y la capacidad de escalabilidad. Se incluye Golden Gate para realizar integraciones heterogéneas entre diferentes bases de datos, ya sean SQL Server, Informix, FileSystem y sistemas operativos y servidores. Y adicionalmente se propone el uso de herramientas de gestión documental como Oracle Enterprise Content Management (ECM) y Oracle Information Rights Management (IRM) para la administración de documentos e imágenes y procesos y también para el establecimiento de permisos de acceso, lectura, impresión, etc., respectivamente. Obteniéndose alta disponibilidad, replicación con sitio alterno.

Tabla de Apoyo al Cumplimiento

La aplicación de la arquitectura base para la continuidad de negocio apoya al cumplimiento del siguiente listado de controles de la circular 014 de 2009 y de la ISO 27001:2005.

Para acceder a la totalidad de la tabla de apoyo al cumplimiento debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 3.1.1 *"Arquitectura orientada a la continuidad del negocio".*

Tabla 6: controles apoyados con la arquitectura básica de continuidad

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
7.6.2	Normas de Control Interno para la gestión de la Tecnología	
III	**Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.**	• A.15.1.1 Identificación de legislación aplicable. • A.15.1.2 Derechos de propiedad intelectual. • A.15.1.3 Protección de los registros organizacionales. • A.15.1.4 Protección de data y privacidad de información personal. • A.15.1.6 Regulación de controles criptográficos.

Teniendo en cuenta la anterior tabla podemos extrapolar las siguientes cifras, de las cuales obtenemos a nivel porcentual los controles que la arquitectura *básica orientada a la continuidad del negocio* apoyará a cumplir (los controles). Divididas en el porcentaje de apoyo al cumplimiento de los controles tecnológicos de la Circular 014 y los objetivos de control de la norma ISO27001. Junto con el porcentaje de aquellos controles que la arquitectura actual por su diseño no apoyará su cumplimiento.

Ilustración 21: Circular 14 arquitectura Base Controles apoyados versus no apoyados

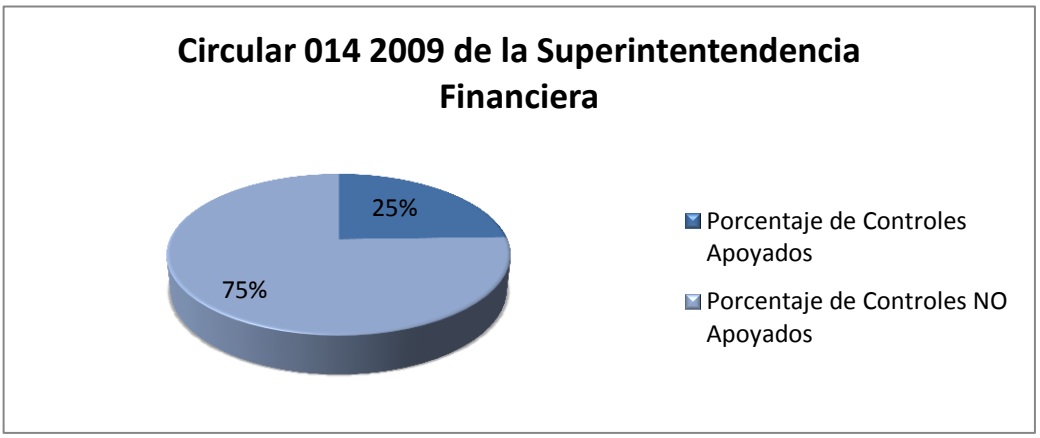
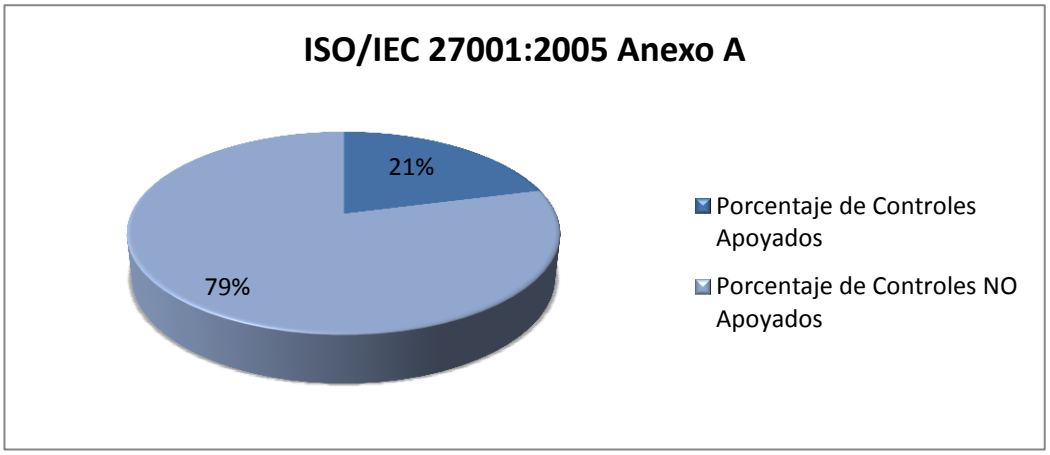


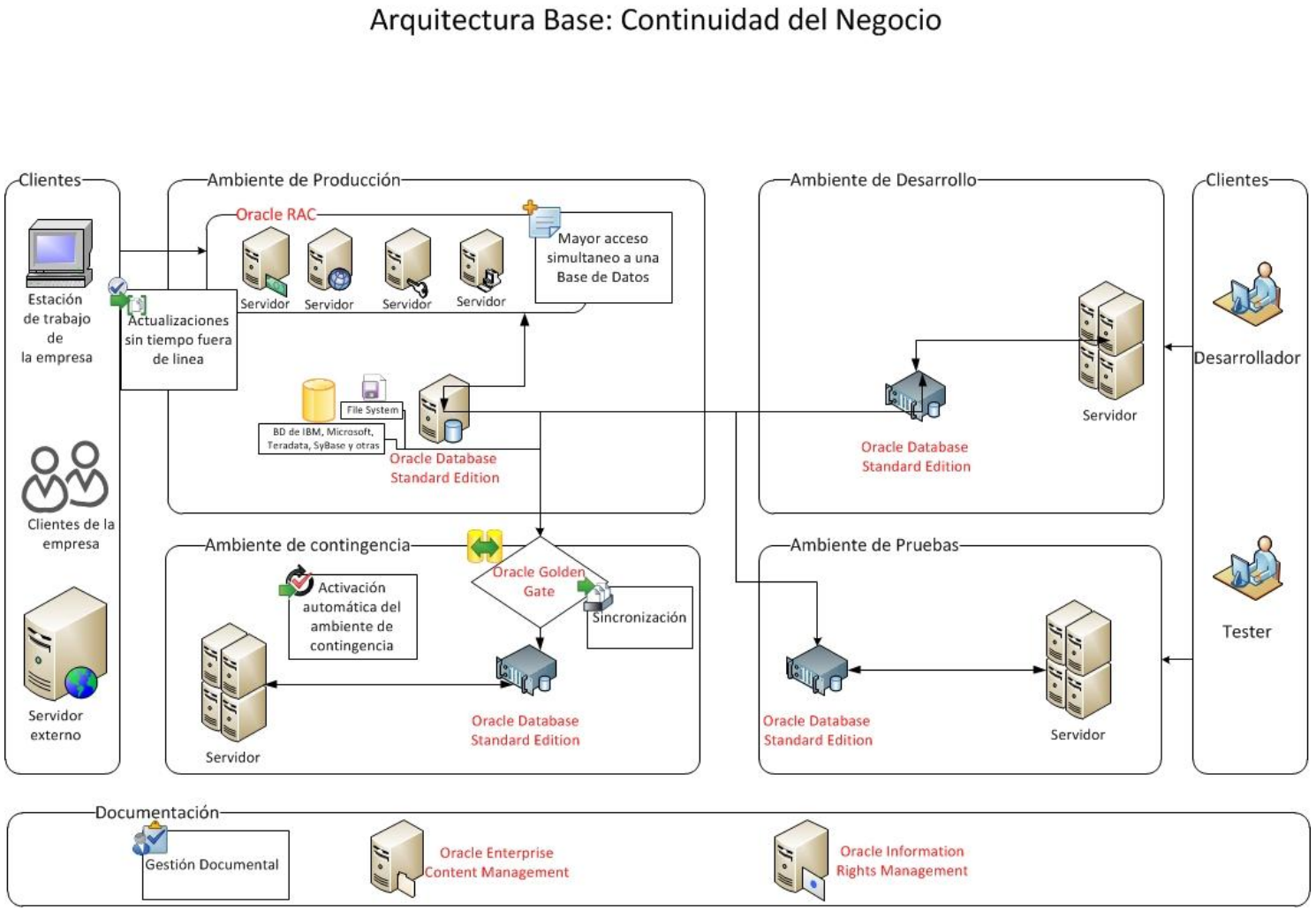
Ilustración 22: ISO 27001 arquitectura Base Controles apoyados versus no apoyados



Lista de productos asociados a la arquitectura

- Oracle Database Enterprise Edition
- Oracle Enterprise Content Management (ECM)
- Oracle Golden Gate (GG)
- Oracle Information Rights Management (IRM).
- Oracle Real Application Clusters (RAC)

Ilustración de la arquitectura Base continuidad del negocio



7.1.2. ARQUITECTURA ORIENTADA A LA SEGURIDAD

Con la arquitectura orientada a seguridad se busca enfrentar y reducir riesgos provenientes de agentes internos y externos, ya sean fallos en el paso de información a través de la red, pérdida o robo de datos, robo o pérdida de infraestructura tecnológica. Pero con la arquitectura orientada a seguridad no solo se busca apoyar este procedo sino también agilizar su ejecución y manejo.

En esta arquitectura se continúa partiendo de la base de datos Oracle Standard Edition, la cual incluye internamente opciones de seguridad que pueden habilitarse, entre ellos un paquete de cifrado de datos y de auditoría. Aquí se incluye protección perimetral a través de DataBase Firewall y AuditVault para monitorear la información que cruza por la red y monitorear bases de datos Oracle y de otros fabricantes y logs de bases de datos respectivamente, bloqueando sentencias SQL e incluso reemplazándolas. El monitoreo llegar incluso a ser directamente sobre los servidores. Agregándole Oracle Identity Management para la gestión adecuada de identidad.

Tabla de Apoyo al Cumplimiento

La aplicación de la arquitectura base para la continuidad de negocio apoya el cumplimiento del siguiente listado de controles de la circular 014 de 2009 y de la ISO 27001:2005.

Para acceder a la totalidad de la tabla de apoyo al cumplimiento debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 3.1.2 *"Arquitectura orientada a la seguridad".*

Tabla 7: controles apoyados con la arquitectura básica de seguridad

Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
7.6.2 Normas de Control Interno para la gestión de la Tecnología	

Circular 014 2009 de la Superintendencia Financiera		ISO/IEC 27001:2005 Anexo A
II	**Infraestructura de tecnología.**	• A.7.1.1 Inventarios de Activos. • A.9.1.1 Perímetro de Seguridad Física. • A.9.1.2 Controles de entrada físicos. • A.9.1.3 Seguridad de oficinas, habitaciones y medios. • A.9.1.4 Protección contra amenazas externas y ambientales. • A.9.1.5 Trabajo en áreas seguras. • A.9.2.1 Ubicación y protección del equipo. • A.9.2.2 Servicios Públicos. • A.9.2.3 Seguridad en el cableado.

Teniendo en cuenta la anterior tabla podemos extrapolar las siguientes cifras, de las cuales obtenemos a nivel porcentual los controles que la arquitectura *básica orientada a la seguridad* apoyará a cumplir (los controles). Divididas en el porcentaje de apoyo al cumplimiento de los controles tecnológicos de la Circular 014 y los objetivos de control de la norma ISO27001. Junto con el porcentaje de aquellos controles que la arquitectura actual por su diseño no apoyará su cumplimiento.

Ilustración 23: CIRCULAR 14 ARQUITECTURA BASE CONTROLES APOYADOS VERSUS NO APOYADOS

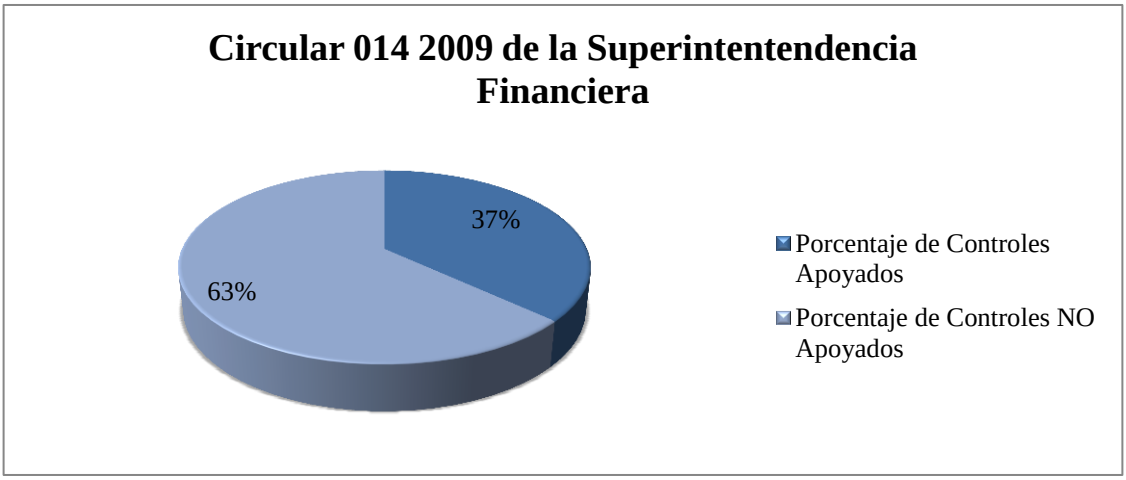
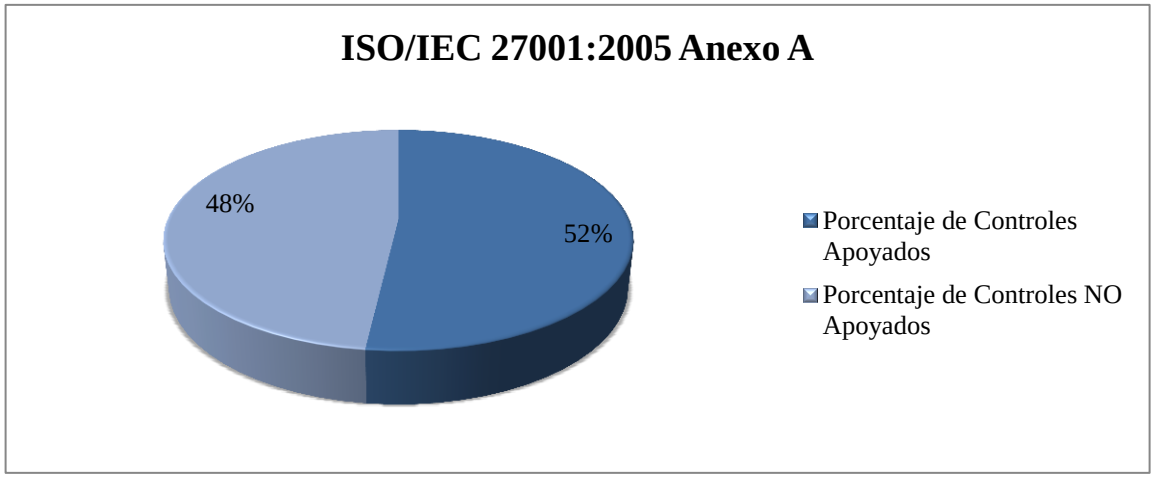


Ilustración 24: ISO 27001 ARQUITECTURA BASE CONTROLES APOYADOS VERSUS NO APOYADOS

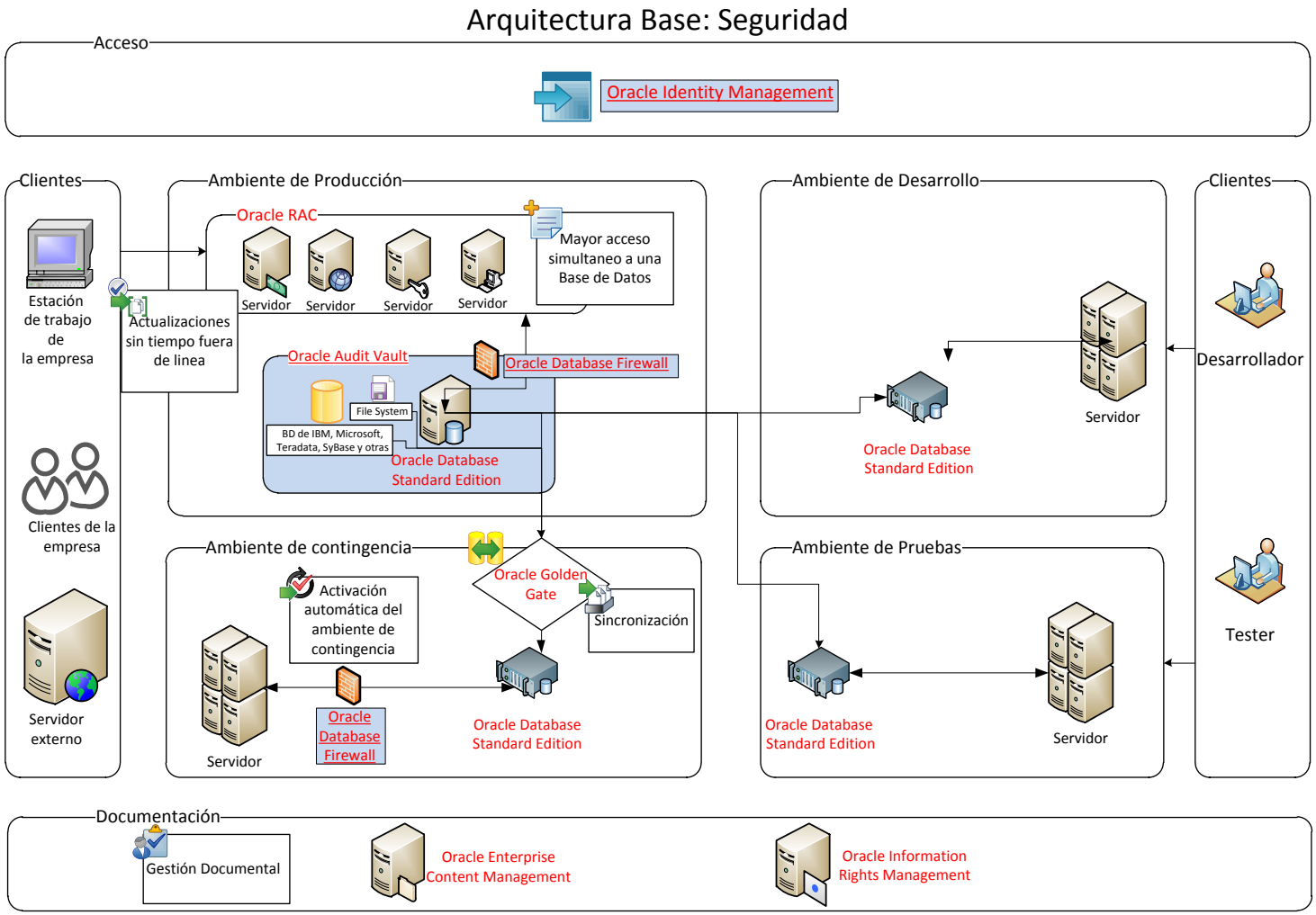


Lista de productos asociados a la arquitectura

Los productos de la siguiente lista son los asociados a la arquitectura, los que se encuentran subrayados son adicionales a la arquitectura anterior.

- Oracle Database Enterprise Edition
- Oracle Audit Vault (AV).
- Oracle Database Firewall (DF).
- Oracle Enterprise Content Management (ECM)
- Oracle Golden Gate (GG)
- Oracle Identity Management (IDM).
- Oracle Information Rights Management (IRM)
- Oracle Real Application Clusters (RAC)

Ilustración de la arquitectura base Seguridad



7.1.3. ARQUITECTURA ORIENTADA A LA ADMINISTRACIÓN Y MONITOREO

Esta arquitectura completa incluye la integración de continuidad de negocio y seguridad, sin embargo se busca darle un mayor alcance, permitiendo realizar tareas de administración y monitoreo de los recursos TI con los que cuenta las compañías, de esta forma se incluye el complemento de Oracle Enterprise Manager Grid Control el cual permitirá monitorear y administrar el ciclo de vida de la infraestructura TI de Oracle como por ejemplo las bases de datos y servidores de aplicaciones con que se cuenten.

Tabla de Apoyo al Cumplimiento

La aplicación de la arquitectura base para la continuidad de negocio apoya el cumplimiento del siguiente listado de controles de la circular 014 de 2009 y de la ISO 27001:2005.

Para acceder a la totalidad de la tabla de apoyo al cumplimiento debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 3.1.3 *"Arquitectura orientada a la administración y monitoreo".*

Ilustración 25: Controles apoyados con la arquitectura básica de continuidad

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
7.6.2	Normas de Control Interno para la gestión de la Tecnología	
IX	**Administración de cambios.**	
	i. Identificación clara del cambio a realizar en la infraestructura.	• A.10.1.2 Gestión de Cambio. • A.10.2.3 Manejar los cambios en los servicios de terceros. • A.12.5.1 Procedimientos de control de cambio.

Teniendo en cuenta la anterior tabla podemos extrapolar las siguientes cifras, de las cuales obtenemos a nivel porcentual los controles que la arquitectura *básica orientada a la administración y monitoreo* apoyará a cumplir (los controles). Divididas en el porcentaje de apoyo al cumplimiento de los controles tecnológicos de la Circular 014 y los objetivos de control de la norma ISO27001. Jun-

to con el porcentaje de aquellos controles que la arquitectura actual por su diseño no apoyará su cumplimiento.

Ilustración 26: Circular 14 arquitectura base: controles apoyados versus no apoyados

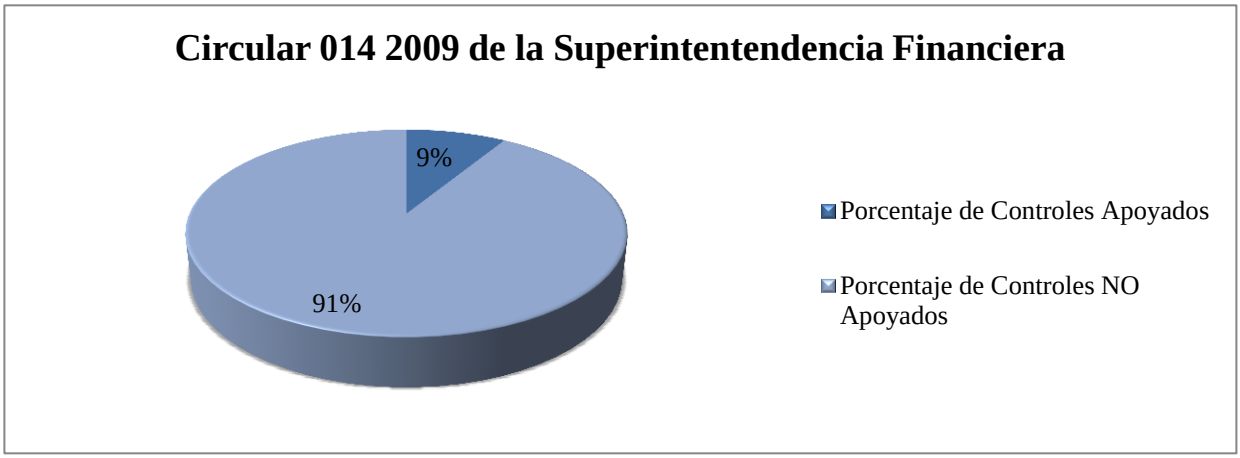
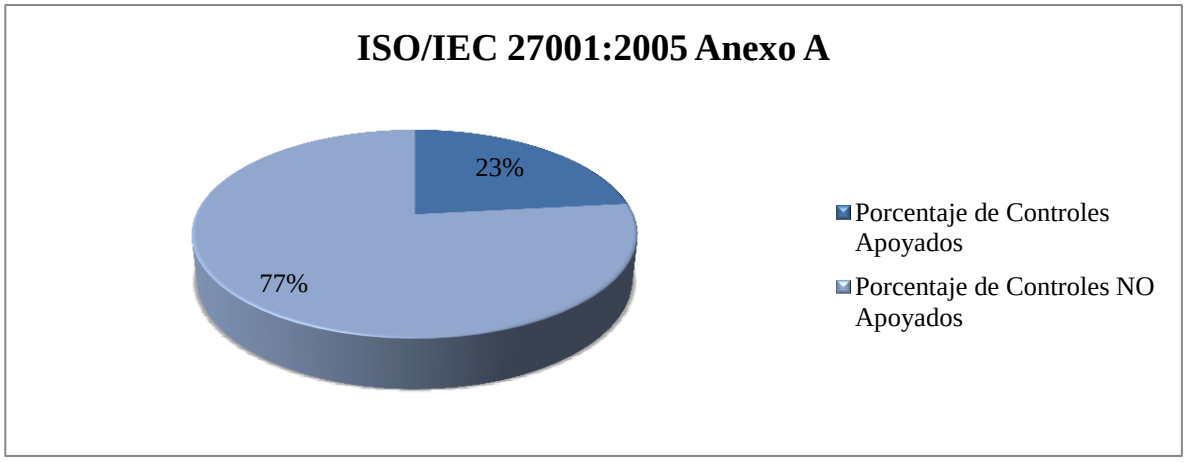


Ilustración 27: Iso 27001 arquitectura base: controles apoyados versus no apoyados

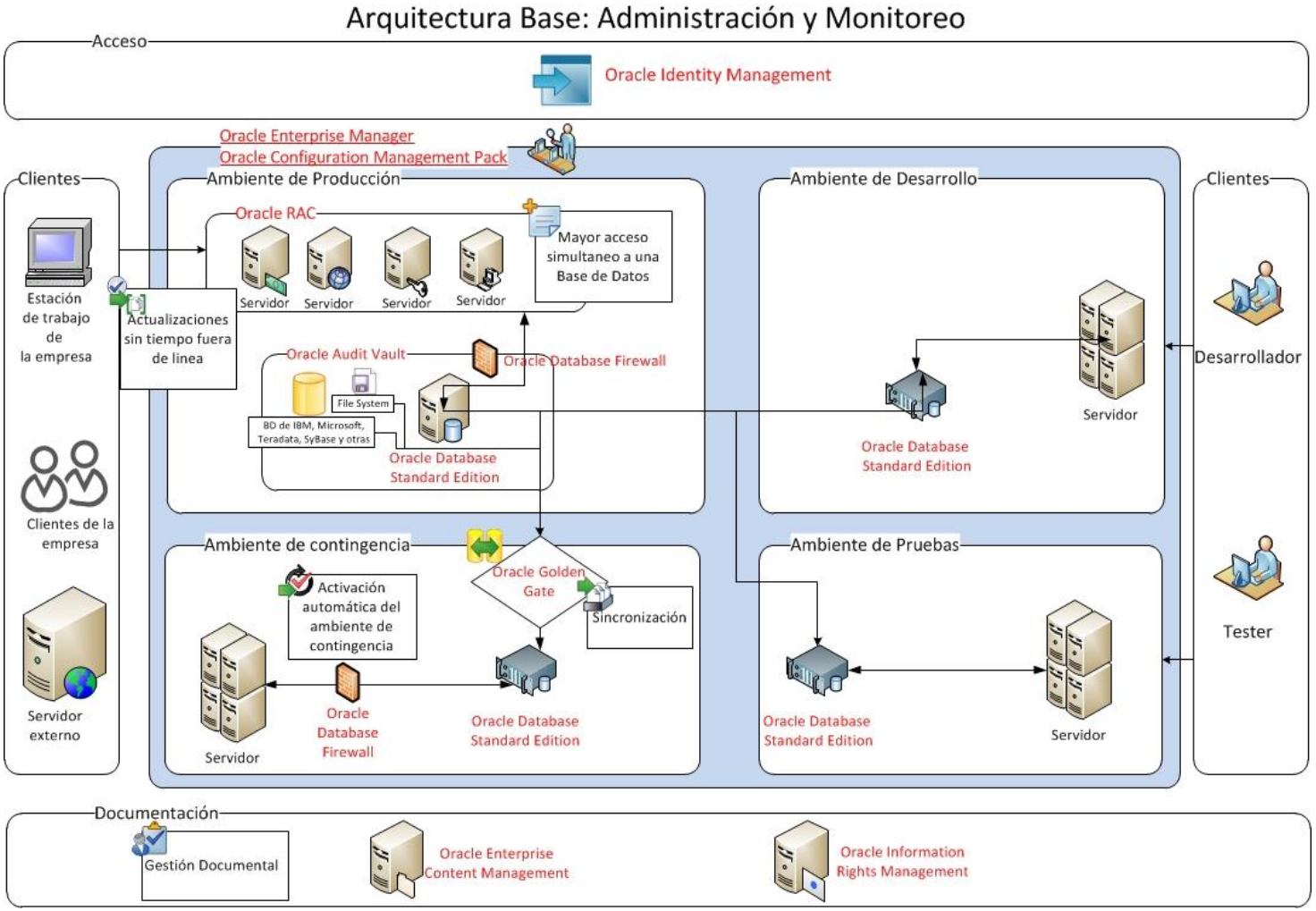


Lista de productos asociados a la arquitectura

Los productos de la siguiente lista son los asociados a la arquitectura, los que se encuentran subrayados son adicionales a la arquitectura anterior.

- Oracle Database Enterprise Edition
- Oracle Audit Vault (AV).
- Oracle Configuration Management Pack (CMP).
- Oracle Enterprise Manager (EM).
- Oracle Database Firewall (DF).
- Oracle Enterprise Content Management (ECM)
- Oracle Golden Gate (GG)
- Oracle Identity Management (IDM).
- Oracle Information Rights Management (IRM)
- Oracle Real Application Clusters (RAC)

Ilustración de la arquitectura base Administración y monitoreo



7.2. Arquitecturas Para Grandes Empresas

Las arquitecturas para grandes empresas están pensadas para organizaciones que requieren un nivel de protección y seguridad mayor, una arquitectura más robusta de continuidad del negocio y menores tiempos de caída del sistema. Dichas arquitecturas al ser más completas y avanzadas cuentan con las soluciones Oracle más complejas y efectivas a nivel empresarial contemplando escalabilidad, seguridad, confiabilidad y ofreciendo diversas características para gestionar los ambientes más demandantes.

7.2.1. ARQUITECTURA AVANZADA ORIENTADA A LA CONTINUIDAD

Con la arquitectura avanzada de continuidad de negocio, se busca garantizar un mayor tiempo de funcionamiento de la infraestructura contemplando las posibles contingencias, reduciendo tiempos de caída del sistema.

A diferencia de la básica, se parte a través de la base de datos Oracle Enterprise Edition. Con esta versión de base de datos la integración con otros productos de Oracle tendrá mayores opciones y complementos que harán a la arquitectura más compleja y variada. Se integra nuevamente con Oracle RAC para proveer de alta disponibilidad con la diferencia de que ahora esta versión soportará un número ilimitado de máquinas con distribución de ambientes, dando una mayor flexibilidad.

La replicación se realizará con Data Guard de esta forma se asegura alta disponibilidad y protección de datos y ofreciendo servicios para crear, mantener, administrar y monitorear bases de datos.

Directamente sobre el sitio alterno se establecerá Active Data Guard, permitiendo que las bases de datos replicadas seas copias de la de producción, permitiendo esto en caso de falla, usar una de las réplicas de forma automática, minimizando el tiempo de baja del servicio. Lo anterior permitirá que desde los sitios alternos puedan realizarse backups, se ejecuten reportes y se hagan pruebas de carga.

También se incluye un sitio alterno basado en otros productos como SQL Server, Informix, FileSystem pero administrado y monitoreado a través de Oracle Golden Gate.

Tabla de Apoyo al Cumplimiento

La aplicación de la arquitectura base para la continuidad de negocio apoya el cumplimiento del siguiente listado de controles de la circular 014 de 2009 y de la ISO 27001:2005.

Para acceder a la totalidad de la tabla de apoyo al cumplimiento debe remitirse al documento principal del trabajo de grado llamado “TG_DocumentoFinal.doc”. Sección 3.2.1 *“Arquitectura avanzada orientada a la continuidad del negocio”.*

Tabla 8: Controles apoyados con la arquitectura avanzada de continuidad

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
7.6.2	Normas de Control Interno para la gestión de la Tecnología	
III	**Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.**	• A.15.1.1 Identificación de legislación aplicable. • A.15.1.2 Derechos de propiedad intelectual. • A.15.1.3 Protección de los registros organizacionales. • A.15.1.4 Protección de data y privacidad de información personal. • A.15.1.6 Regulación de controles criptográficos.
V	**Administración de la calidad,**	

Teniendo en cuenta la anterior tabla podemos extrapolar las siguientes cifras, de las cuales obtenemos a nivel porcentual los controles que la arquitectura *avanzada orientada a la continuidad* apoyará a cumplir (los controles). Divididas en el porcentaje de apoyo al cumplimiento de los controles tecnológicos de la Circular 014 y los objetivos de control de la norma ISO27001. Junto con el porcentaje de aquellos controles que la arquitectura actual por su diseño no apoyará su cumplimiento.

Ilustración 28: Circular 14 arquitectura avanzada continuidad: controles apoyados versus no apoyados

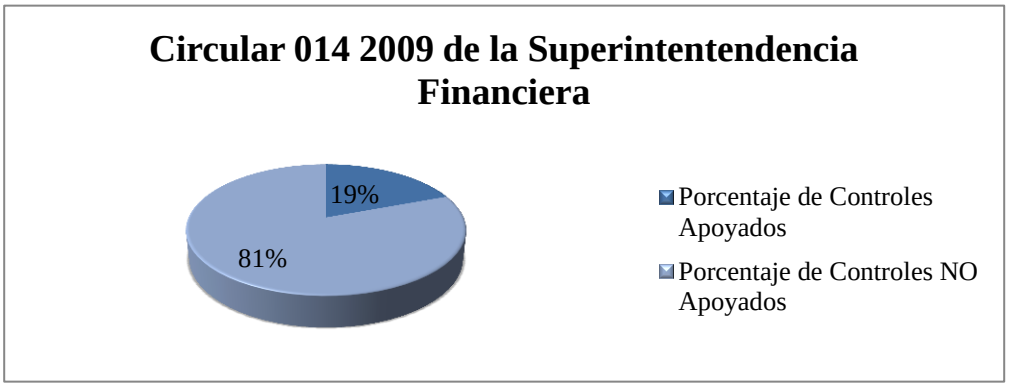
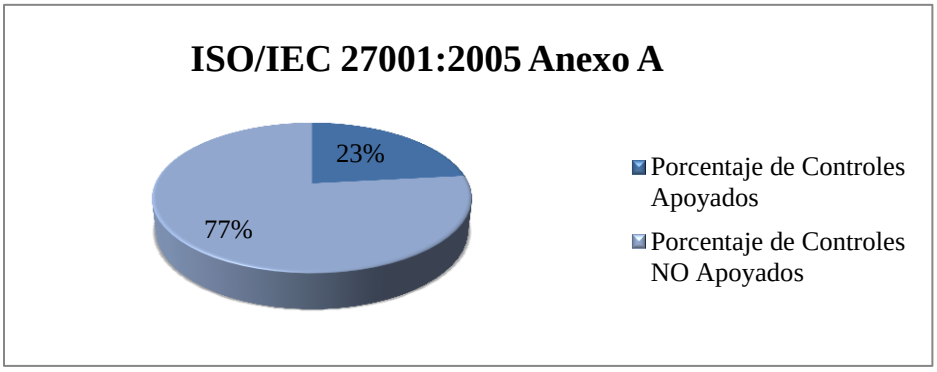


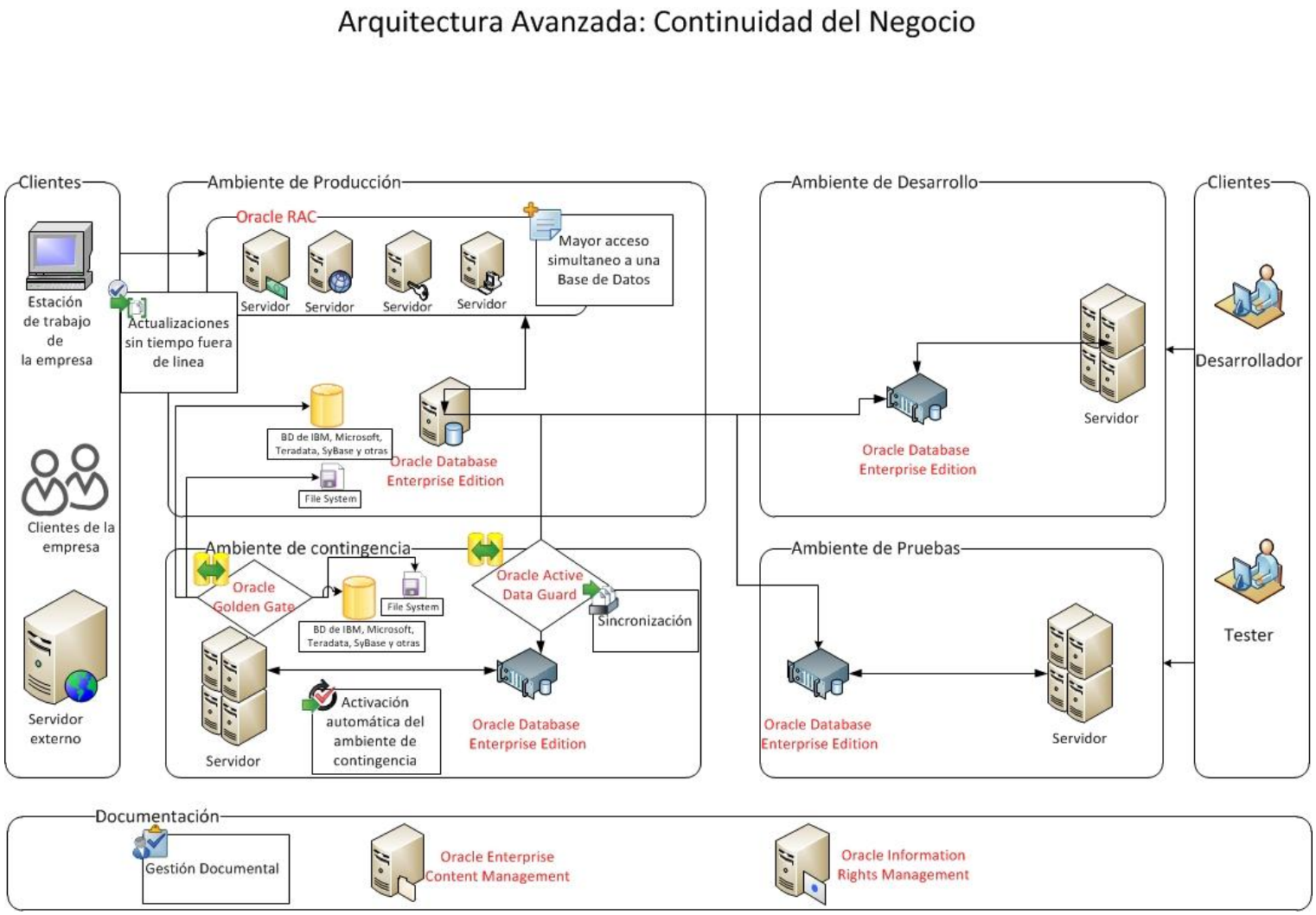
Ilustración 29: Iso 27001 arquitectura avanzada Continuidad: controles apoyados versus no apoyados



Lista de productos asociados a la arquitectura

- Oracle Database Enterprise Edition
- Oracle Data Guard (DG) y Oracle Active Data Guard (ADG)
- Oracle Enterprise Content Management (ECM)
- Oracle Golden Gate (GG)
- Oracle Information Rights Management (IRM)
- Oracle Real Application Clusters (RAC)

Ilustración de la arquitectura avanzada Continuidad del negocio



7.2.2. ARQUITECTURA AVANZADA ORIENTADA A LA SEGURIDAD

Con la arquitectura orientada a seguridad se busca enfrentar y reducir riesgos provenientes de agentes internos y externos, ya sean fallos en el paso de información a través de la red, pérdida o robo de datos, robo o pérdida de infraestructura tecnológica.

Esta arquitectura se basa en la arquitectura de continuidad pero se le incluye un fuerte aspecto de seguridad con herramientas de integración que ahora son posibles incluirlas gracias al uso de las base de datos Oracle Enterprise Edition. Se agrega Oracle Data Vault con el fin de impedir que los DBA accedan a aplicaciones y tareas que están fuera de sus responsabilidades y se asignar permisos de acuerdo a roles establecidos. La arquitectura cuenta también con el apoyo de Oracle Advanced security ofreciendo criptografía en la base de datos y en la red, de esta forma se protege toda comunicación hacia y desde la base de datos.

Se provee de un ambiente de desarrollo especializado a través de Oracle Data Masking el cual permitirá sustituir datos de producción con valores similares y válidos para trabajar con ellos en este ambiente.

Los clientes antes de ingresar al sistema tendrán que pasar a través de Oracle Database Firewall para el monitoreo en tiempo real de la actividad de la base de datos en la red, esto con el apoyo de Oracle Identity Management para la gestión de usuarios.

Tabla de Apoyo al Cumplimiento

La aplicación de la arquitectura base para la continuidad de negocio cumple con el siguiente listado de controles de la circular 014 de 2009 y de la ISO 27001:2005.

Para acceder a la totalidad de la tabla de apoyo al cumplimiento debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 3.2.2 *"Arquitectura avanzada orientada a la seguridad".*

Tabla 9: Controles apoyados con la arquitectura avanzada de Seguridad

Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
7.6.2 Normas de Control Interno para la gestión de la Tecnología	

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
II	**Infraestructura de tecnología.**	• A.7.1.1 Inventarios de Activos. • A.9.1.1 Perímetro de Seguridad Física. • A.9.1.2 Controles de entrada físicos. • A.9.1.3 Seguridad de oficinas, habitaciones y medios. • A.9.1.4 Protección contra amenazas externas y ambientales. • A.9.1.5 Trabajo en áreas seguras. • A.9.2.1 Ubicación y protección del equipo. • A.9.2.2 Servicios Públicos. • A.9.2.3 Seguridad en el cableado.

Teniendo en cuenta la anterior tabla podemos extrapolar las siguientes cifras, de las cuales obtenemos a nivel porcentual los controles que la arquitectura *avanzada orientada a la seguridad* apoyará a cumplir (los controles). Divididas en el porcentaje de apoyo al cumplimiento de los controles tecnológicos de la Circular 014 y los objetivos de control de la norma ISO27001. Junto con el porcentaje de aquellos controles que la arquitectura actual por su diseño no apoyará su cumplimiento.

Ilustración 30: Circular 14 arquitectura avanzada Seguridad: controles apoyados versus no apoyados

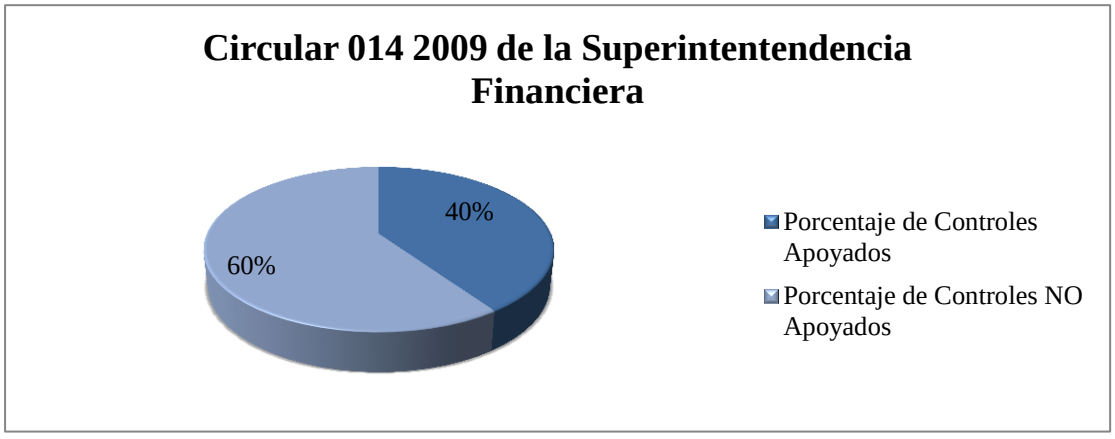
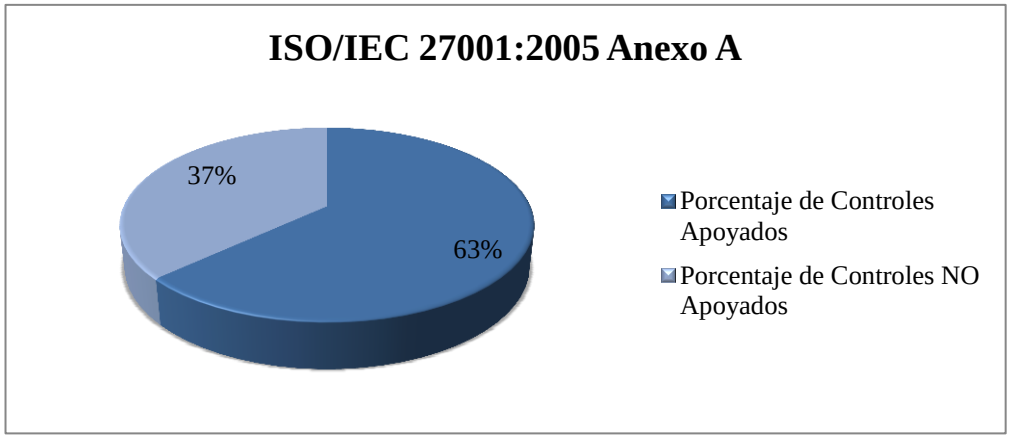


Ilustración 31: Iso 27001 arquitectura avanzada Seguridad: controles apoyados versus no apoyados

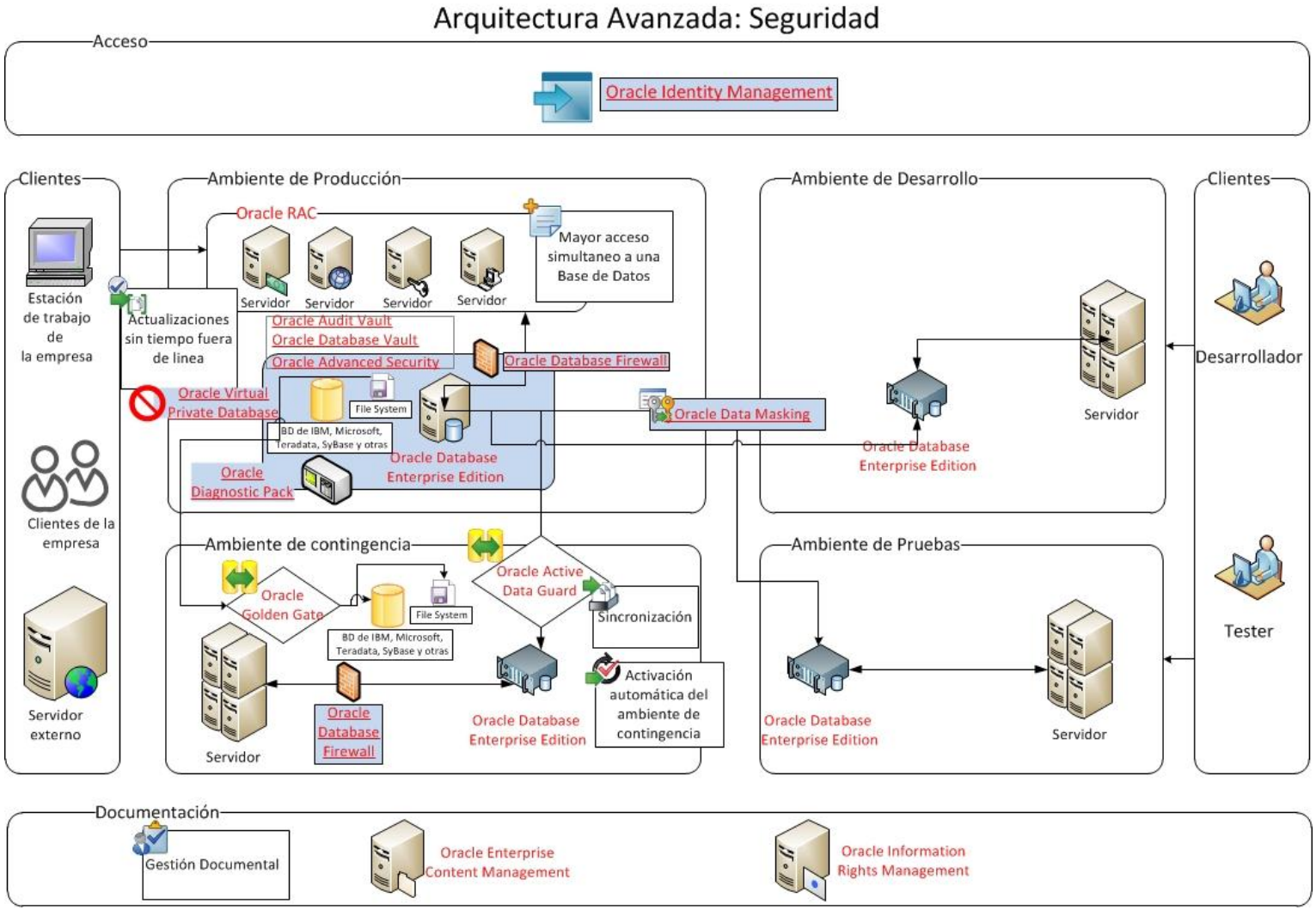


Lista de productos asociados a la arquitectura

Los productos de la siguiente lista son los asociados a la arquitectura, los que se encuentran subrayados son adicionales a la arquitectura anterior.

- Oracle Database Enterprise Edition
- Oracle Advanced Security (AS).
- Oracle Audit Vault (AV).
- Oracle Data Guard (DG) y Oracle Active Data Guard (ADG)
- Oracle Data Masking Pack (DMP).
- Oracle Database Firewall (DF).
- Oracle Database Vault (DV).
- Oracle Diagnostic Pack (DP).
- Oracle Enterprise Content Management (ECM)
- Oracle Golden Gate (GG)
- Oracle Identity Management (IDM).
- Oracle Information Rights Management (IRM)
- Oracle Real Application Clusters (RAC)
- Oracle Virtual Private Database (VD).

Ilustración de la arquitectura avanzada seguridad



7.2.3. ARQUITECTURA AVANZADA ORIENTADA A LA ADMINISTRACIÓN Y MONITOREO

Esta arquitectura incluye la integración de continuidad de negocio avanzada y seguridad avanzada, pero se busca darle un componente adicional con el fin de ejercer un mayor control sobre la infraestructura dándole un mayor poder a través de herramientas de Administración y Monitoreo. Es por esto que se incluye Oracle Diagnostic Pack el cual hará labores de diagnóstico en busca de problemas de rendimiento, métricas, notificación de eventos e historial de carga.

Tabla de Apoyo al Cumplimiento

La aplicación de la arquitectura base para la continuidad de negocio apoya el cumplimiento del siguiente listado de controles de la circular 014 de 2009 y de la ISO 27001:2005.

Para acceder a la totalidad de la tabla de apoyo al cumplimiento debe remitirse al documento principal del trabajo de grado llamado "TG_DocumentoFinal.doc". Sección 3.2.3 *"Arquitectura avanzada orientada a la administración y monitoreo".*

Tabla 10: Controles apoyados con la arquitectura avanzada de Administración y Monitoreo

	Circular 014 2009 de la Superintendencia Financiera	ISO/IEC 27001:2005 Anexo A
7.6.2	Normas de Control Interno para la gestión de la Tecnología	
I	**Plan estratégico de tecnología.**	
	ii. Evaluación de la tecnología actual.	• A.7.1.1 Inventario de Activos.

Teniendo en cuenta la anterior tabla podemos extrapolar las siguientes cifras, de las cuales obtenemos a nivel porcentual los controles que la arquitectura *avanzada orientada a la administración y monitoreo* apoyará a cumplir (los controles). Divididas en el porcentaje de apoyo al cumplimiento de los controles tecnológicos de la Circular 014 y los objetivos de control de la norma ISO27001. Junto con el porcentaje de aquellos controles que la arquitectura actual por su diseño no apoyará su cumplimiento.

Ilustración 32: Circular 14 arquitectura avanzada Administración y Monitoreo: controles apoyados versus no apoyados

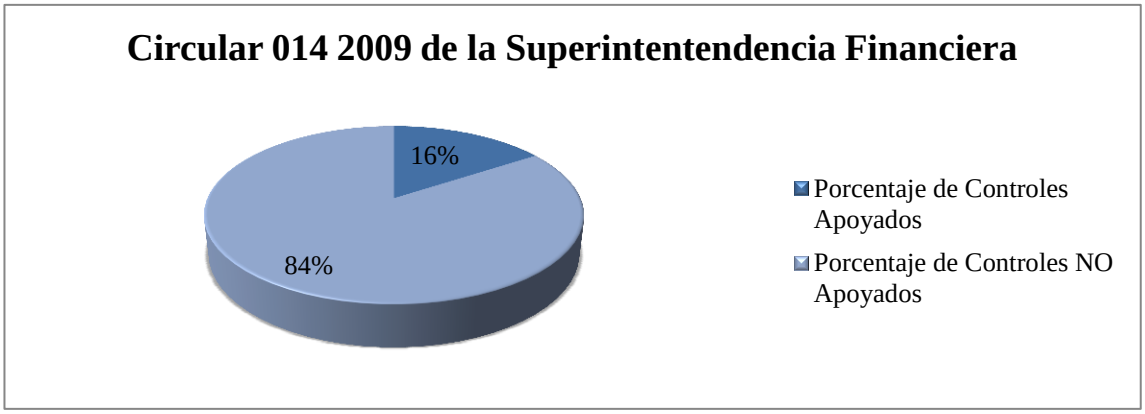
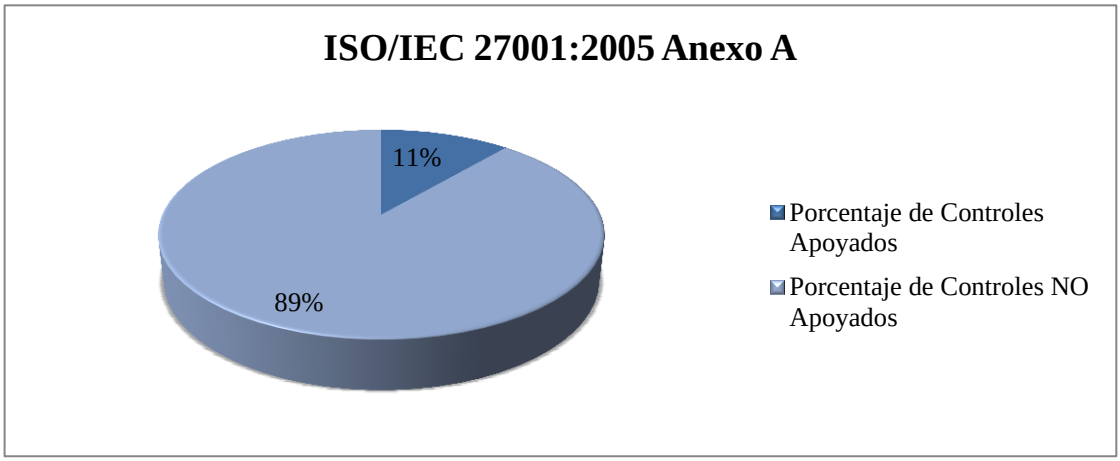


Ilustración 33: Iso 27001 arquitectura avanzada administración y Monitoreo: controles apoyados versus no apoyados

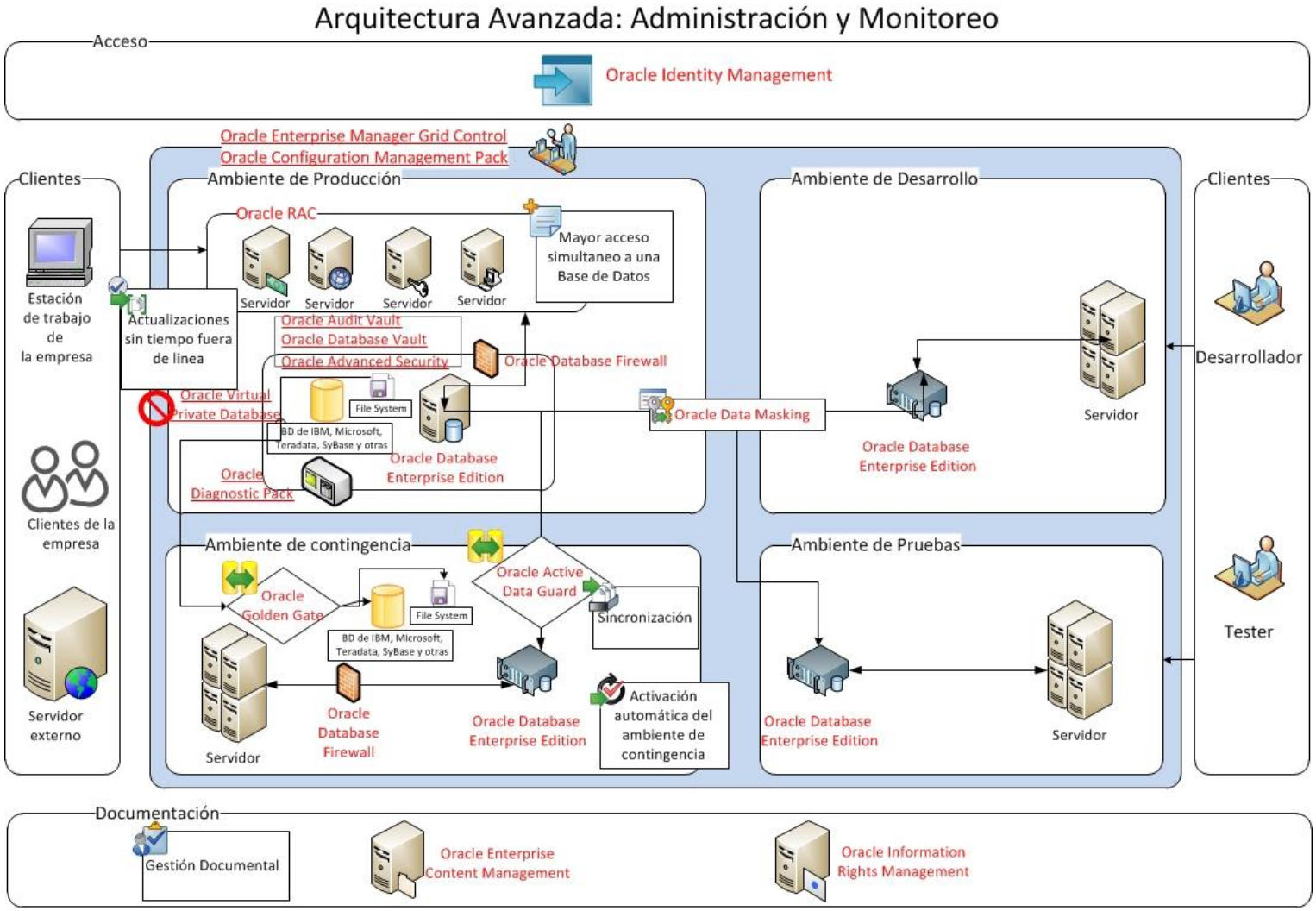


Lista de productos asociados a la arquitectura

Los productos de la siguiente lista son los asociados a la arquitectura, los que se encuentran subrayados son adicionales a la arquitectura anterior.

- Oracle Database Enterprise Edition
- Oracle Advanced Security (AS).
- Oracle Audit Vault (AV).
- Oracle Configuration Management Pack (CMP).
- Oracle Data Guard (DG) y Oracle Active Data Guard (ADG)
- Oracle Data Masking Pack (DMP).
- Oracle Database Firewall (DF).
- Oracle Database Vault (DV).
- Oracle Diagnostic Pack (DP).
- Oracle Enterprise Content Management (ECM)
- Oracle Enterprise Manager Grid Control (EMGC)
- Oracle Golden Gate (GG)
- Oracle Identity Management (IDM).
- Oracle Information Rights Management (IRM)
- Oracle Real Application Clusters (RAC)
- Oracle Virtual Private Database (VD).

Ilustración de la arquitectura avanzada administración y monitoreo



7.3. Estadísticas de Cumplimiento

Las arquitecturas propuestas tienen como meta el cumplimiento de los controles tecnológicos de la Circular 014 de 2009 y de la norma ISO 27001:2005 anexo A, para lograr cubrir la mayor cantidad de estos controles tanto la mediana y gran empresa debe de aplicar la arquitectura orientada de Administración y monitoreo la cual recoge los productos y los controles cumplidos de seguridad y continuidad de negocio, también debemos tener en cuenta que las soluciones Oracle cuenta con tecnologías y aplicaciones escalables, por lo cual es posible arrancar con una solución muy reducida e ir agregando componentes cuando la empresa lo considere necesario.

En los siguientes gráficos circulares podemos observar el aporte para el cumplimiento que da cada una de las arquitecturas, se puede afirmar que el grado de cumplimiento de la arquitectura básica con relación a los controles tecnológicos de la circular 014 de 2009 de la Superintendencia Financiera alcanza un 70.18% de cumplimiento, y la ISO 27001:2005 logra un 96.17%.

Ilustración 34: Porcentajes de apoyo en la circular 014 con la arquitectura básica

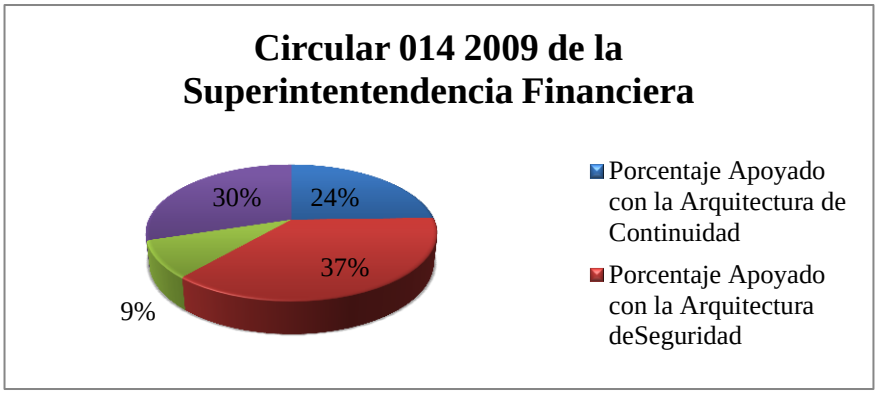
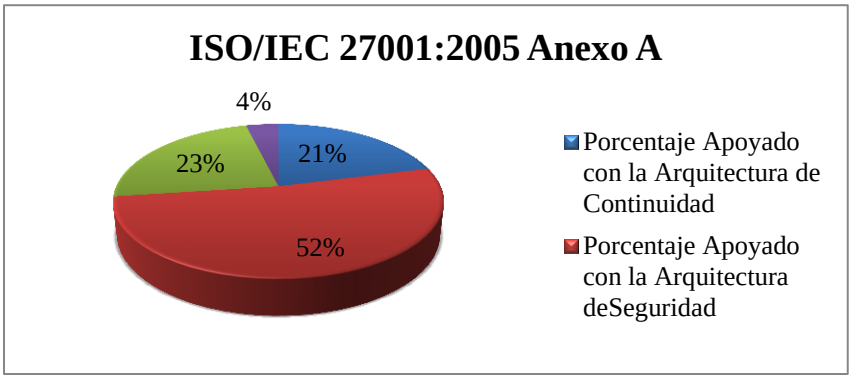


Ilustración 35: Porcentajes de controles apoyados de la ISO 27001 con la arquitectura básica



Por otra parte la Arquitectura avanzada logra mejores cifras como se puede observar en las siguientes gráficas, en el caso del cumplimiento de la circular 014 de la Superintendencia Financiera se logra un nivel de cumplimiento de 75.44% y con la ISO 27001:2005 Anexo A es de 97.72%, también podemos observar que la arquitectura que más aporta es la de seguridad con un ostentoso 37% y 52% en la Circular 014 y la ISO 27001:2005 Anexo A respectivamente.

Ilustración 36: Porcentajes de controles apoyados de la circular 014 con la arquitectura Avanzada

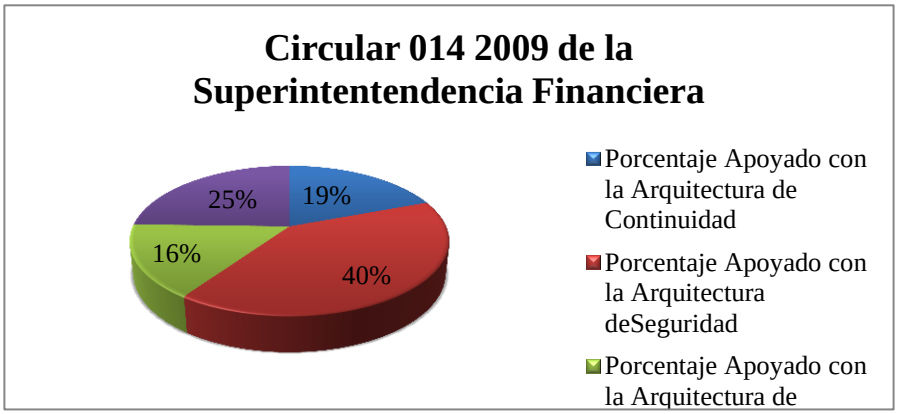
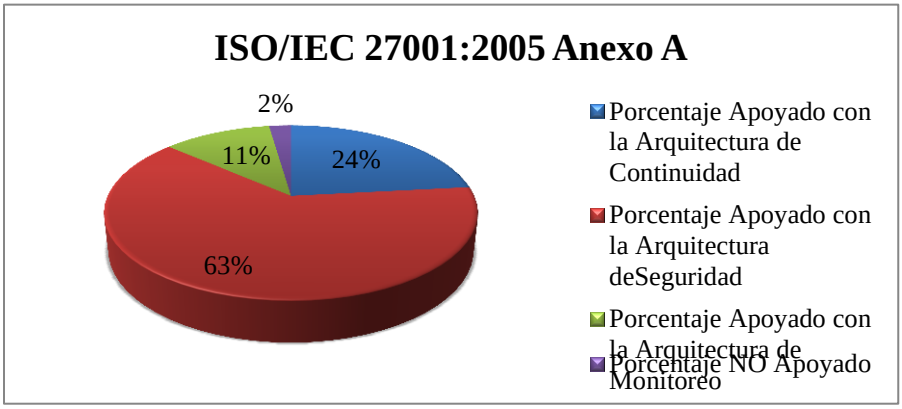


Ilustración 37: Porcentajes de controles apoyados de la Iso 27001 con la arquitectura avanzada

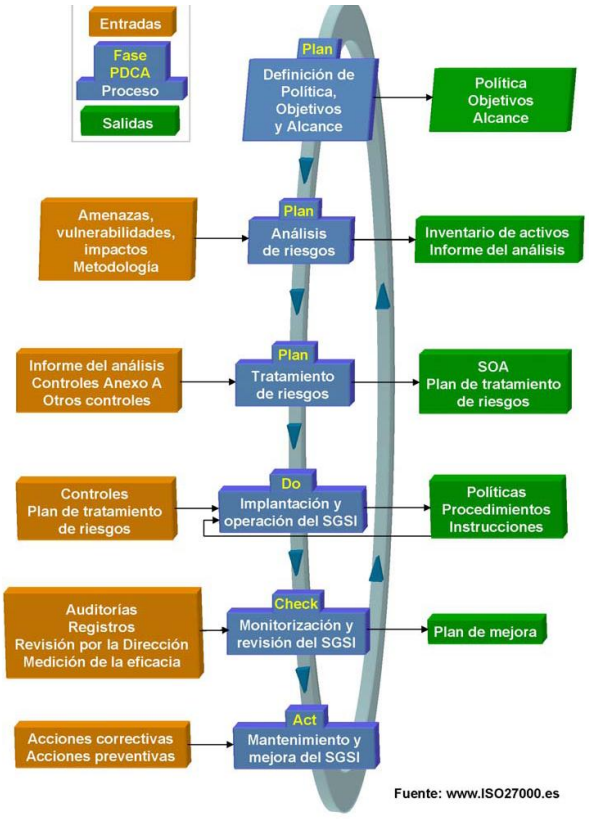


8. LA CIRCULAR 014 ENMARCADA BAJO EL MODELO PROPUESTO DE LA NORMA ISO27001

El ejercicio desarrollado busca facilitar a las organizaciones el abordar procesos de Gobierno, riesgo y cumplimiento unificados, de manera que la implementación de cada nueva regulación, framework, o cualquier tipo de medición sobre la efectividad de operación del negocio, pueda ser visualizado de manera centralizada. A continuación se plantea la manera en que es posible aprovechar la implementación de la Circular 14, para agilizar y facilitar la implementación de la ISO 27001, centralizando tareas, reutilizando controles y consolidando los documentos y diferentes entregables exigidos, buscando la implementación de un programa integrado de GRC (Gobierno, Riesgo y Cumplimento), evitando tener una visión monolítica de cumplimiento y llevando a un proceso de cumplimiento unificado.

La norma ISO 27001 propone un ciclo de implementación del Sistema de Gestión de Seguridad de la Información que se puede resumir en las fases que se muestran en la siguiente imagen:

Ilustración: ciclo de implementación del Sistema de Gestión de Seguridad



Los requerimientos establecidos en cada una de las fases se encuentran debidamente detallados en la sección 4.2 de la norma ISO27001 llamada “Establecer y Manejar el SGSI”.

A continuación se buscar establecer un mecanismo para facilitar la implementación de la Circular 14 ,basados en el alcance de este documento que corresponde a los controles técnicos de las sección 7.6.2 , partiendo del enfoque propuesto por la ISO27001, de manera que sea posible estructurar un proceso integrado de Cumplimiento de la Circular y la Norma permitiendo a las organizaciones una integración a nivel regulatorio, reduciendo tiempos en reportes de auditoría y evitando rehacer tareas cada vez que se requiera implementar un nuevo componente regulatorio.

A continuación se establecen posibles parámetros para alinear los requerimientos técnicos exigidos en la circular 14 y que en paralelo facilite la implementación de la ISO 27001, ya que las dos establecen requerimientos similares en su implementación.

ISO27001	CIRCULAR 014	ALCANCE
DEFINICIÓN DE POLÍTICA, OBJETIVOS Y ALCANCE	7.2. ÁMBITO DE APLICACIÓN 7.3 DEFINICIÓN Y OBJETIVO DEL SISTEMA DE CONTROL INTERNO 7.4 PRINCIPIOS DEL SISTEMA DE CONTROL INTERNO	El proceso inicial para la norma es el establecimiento de la política, objetivos, procesos y procedimientos que para la Circular 014 deben orientarse a los sistemas que contienen información sensitiva financiera, de manera que el alcance de la implementación de la Circular 014, corresponda al alcance y límites de la Norma . El ámbito de Aplicación para la Circular 014 y en general todos los elementos que corresponden a las secciones 7.2 - 7.3 y 7.4 de la Circular, deber estar enmarcados en los requerimientos necesarios para la definición de la Política del SGSI.

ANÁLISIS DE RIESGOS	7.5.2 GESTIÓN DE RIESGOS	Las organizaciones deben contar con su metodología de evaluación, definición y tratamiento de riesgos. Ni la Circular 014 ni la norma ISO27001 cuenta con una propia. Adicionalmente la metodología adoptada debería ser usada para los dos procesos, de manera que al dar tratamiento a un riesgo, se asegure su cumplimiento para las dos certificaciones.
TRATAMIENTO DE RIESGOS	7.5.2 GESTIÓN DE RIESGOS	(Ver anterior) A manera de ejemplo. Es posible usar el modelo planteado por la norma ISO27005 para establecer el tratamiento de riesgos facilitando el cumplimiento de los 11 ítems de la sección 7.5.2
IMPLANTACIÓN Y OPERACIÓN DEL SGSI	7.5 ELEMENTOS DEL SISTEMA DE CONTROL INTERNO 7.6 ÁREAS ESPECIALES DENTRO DEL SISTEMA DE CONTROL INTERNO	El alcance del ejercicio corresponde a la sección 7.6.2. Por otro lado la implementación estará basada en los modelos de arquitectura propuestos, que se definieron de acuerdo al tamaño y características de cada empresa. Al implementar la solución propuesta, deberá remitirse al capítulo 2.3. Alineación de la Circular 014 de 2009 de la Superintendencia Financiera y las ISO27001 con los productos ORACLE seleccionados. , donde se encontrará la manera en la que los controles técnicos de la Circular 014 se homologan con los controles técnicos del anexo A de la norma ISO27001. Para cada organización debe definirse cuáles son sus criterios de cumplimiento de estos controles de acuerdo con sus características técnicas y de operación y pueden ser monitoreados

		en línea con los componentes incluidos en cada arquitectura. De manera adicional de acuerdo a la sección 7.7 de la Circular 014, cada entidad financiera deberá asignar los responsables y mecanismos de gestión y operación.
MONITORIZACIÓN Y REVISIÓN DEL SGSI	7.7 RESPONSABILIDADES DENTRO DEL SISTEMA DE CONTROL	Las plataformas propuestas proveen mecanismos automáticos que permiten el monitoreo en línea de los controles definidos. Se cuenta con controles (Oracle) tanto preventivos como de detección y serán habilitados acorde con las necesidades de cada entidad. Los responsables asignados para el monitoreo de la circular contarán con herramientas que facilitan su labor e inclusive, recibirán recomendaciones de cómo ir alineando la solución acorde con la evolución y cambios en los sistemas.
MANTENIMIENTO Y MEJORA DEL SGSI	7.8 PRODUCTOS QUE DEBEN PRESENTARSE A LA SFC	Cualquier actividad de cumplimiento regulatorio exige generar reportes y documentos soporte al proceso, así como las acciones y gestión de riesgos definidos. La solución busca minimizar las tareas manuales para la generación de estos documentos, incluyendo reportes asociados a cumplimiento y parametrizando los documentos de acuerdo con las diferentes regulaciones.

Los Puntos “Análisis de Riesgos” y” Tratamiento de Riesgos” son abordados con más detalle en la ISO/IEC 27005 que trata de la gestión de riesgos en seguridad de la información.

V - CONCLUSIONES Y TRABAJOS FUTUROS

1. Conclusiones

- Durante la ejecución del proyecto se observó que la circular 014 de la superintendencia financiera, presenta sus controles de manera genérica, lo cual posibilita llegar a su cumplimiento desde diferentes aproximaciones, pero esto también puede hacer que las empresas no tengan claro cómo abordar la circular.

- La alineación de las circular 014 con la ISO 27001 muestra que hay muchos puntos en común lo cual permite los métodos ya utilizadas para el cumplimiento de la ISO 27001 sean de gran apoyo para el cumplimiento de la Circular 014.

- Se ha concluido que es posible homologar aspectos tanto de la Circular 014 como la norma ISO27001 para así agilizar el proceso de certificación. Con esto, adicionalmente se busca que las tareas realizadas, los requerimientos asociados y el tiempo invertido en el cumplimiento de la Circular 014 pueda usarse como apoyo al proceso de adopción de la norma ISO27001.

- El análisis de las aplicaciones propuestas para la solución deja ver que muchas de estas soluciones ya están pensadas para ayudar a cumplir con normativas, regulaciones y buenas prácticas que se encuentran a nivel mundial y debido a que la Circular 014 tiene como fuente muchas de estas regulaciones y estándares, el apoyo que estas le brindan es amplio.

- Propagar la adopción de la filosofía GRC (Governance, Risk management, and Compliance) para las organizaciones que aborden esta propuesta de manera que estén alineados con las tendencias actuales de evolución a nivel de cumplimiento regulatorio.

- Las organizaciones actuales y en especial las entidades financieras deben cumplir con un gran número de frameworks internacionales como lo son COSO, SOX, COBIT entre otros y unas regulaciones nacionales como la Circular 052, Circular 014 y Circular 38, y dichas organizaciones no cuentan con una estrategia clara y estructurada de cómo hacerlo, lo cual conlleva a grandes costos y esfuerzos.

- Es de gran importancia conocer las tendencias tecnológicas que se encuentran en el mercado ya que estas podrán apoyar, facilitar e incluso agilizar el proceso de cumplimiento de controles.

- Las organizaciones de hoy en día deben conocer, entender y gestionar los riesgos a los que están expuestas con base en su actividad económica, y apuntar a estrategias y modelos basados en GRC.

- Es importante contar con una muestra que permita realizar un análisis porcentual del uso de bases de datos Oracle a nivel nacional, esto con el fin de dar un mayor peso al proyecto presentado, ya que las cifras internacionales no necesariamente reflejan la realidad nacional.

- Evaluar si las entidades financieras tienen conocimiento de la existencia de herramientas tecnológicas Oracle que apoyen el proceso de cumplimiento y que tan dispuestas están al proceso de adopción de las mismas, considerando sus características y costos.

2. Trabajos Futuros

Después de la solución desarrollada se identificaron aspectos que por su importancia ameritan ser tomados en cuenta como parte del mejoramiento y actualización de la propuesta actual:

- Con la emisión de la Circular 038 de la Superintendencia Financiera la cual modifica la Circular 014 se generan nuevas oportunidades de trabajo, puesto que se incluyen modificaciones en los procedimientos y posibles controles los cuales requerirán una evaluación y generación de nuevas alineaciones y productos con el fin de contar con un solución que responda a los ambientes dinámicos.

- Queda abierta la posibilidad de generar nuevas arquitecturas basadas en productos diferentes a los que cuenta Oracle, como el caso de soluciones Microsoft, IBM e incluso herramientas de software libre.

- Debido a la gran variedad de soluciones existentes en el mercado es válido generar arquitecturas que no solo se integren de productos de la misma casa matriz, por el contrario presentar arquitecturas que contemplen la integración de sistemas heterogéneos entre sí, donde se cuente con herramientas Microsoft, IBM y de software libre.

VI - REFERENCIAS Y BIBLIOGRAFÍA

1. Referencias

ACIS. (2010). *II Encuesta Latinoamericana de Seguridad de la información.* Recuperado el 13 de Septiembre de 2010, de ACIS: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XJNSI/IIELSI-2010.pdf

Archivo General de la Nacion. (29 de 10 de 2010). *Programa de Gestión Documental (PGD).* Recuperado el 30 de Octubre de 2010, de Archivo General de la Nacion: http://www.archivogeneral.gov.co/index.php?idcategoria=1232

Bae, B. (2003). Internal Control Issues: The Case of Changes to Information Processes.

BDO. (2010). Adoptando los Modelos de Control Interno COSO y COBIT.

Bueno, L. A. (2010).

Cano, J. (2009). Seguridad de la Información en Latinoamerica Tendencias.

Colombia, R. d. (2005). MODELO ESTANDAR DE CONTROL INTERNO PARA EL ESTADO COLOMBIANO. Bogotá.

Colombiahosting.com. (2010). La Seguridad de la Información.

Deloitte. (2010). *2010 Financial Services Global Security Study: The faceless threat.* Recuperado el Agosto de 29 de 2010, de Deloitte: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/Financial%20Services/dtt_fsi_2010%20Global%20FS%20Security%20Survey_20100603.pdf

Deloitte. (2010). *2010 Financial Services Global Security Study: The faceless threat.*Recuperado el Agosto de 29 de 2010, de deloitte: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/Financial%20Services/dtt_fsi_2010%20Global%20FS%20Security%20Survey_20100603.pdf

Deloitte. (2010). Alineando Procesos de Negocio con la ISO27001.

Dutra, E. G. (24 de febreo de 2006). *Seguridadit Blogspot*. Recuperado el 16 de Agosto de 2010, de http://seguridadit.blogspot.com/2006/02/mas-sobre-iso-1779927001.html

Estrada, A. (2006). ISO27001: Los Controles.

Grupo Inversión, financiación y control Universidad Icesi. (Enero de 2010). *Universidad ICESI.* Recuperado el 15 de Agosto de 2010, de

http://www.icesi.edu.co/departamentos/finanzas_contabilidad/images/proyectos/control_interno.pdf

Institute, M. T. (2009). CISO Information Security Survey.

ISO. (2005). *International Standards for Business.*Recuperado el 16 de Agosto de 2010, de http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

IT Governance Institute. (2007). *cobiT4.1.* Recuperado el 12 de Septiembre de 2010, de isaca: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

ITGI. (2005). *itgovernance.* Recuperado el 15 de Agosto de 2010, de http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf

López Neira, A. (2005). *iso27000.es el Portal de ISO 27001 en español*. Recuperado el 16 de Agosto de 2010, de http://www.iso27000.es/sgsi.html

López Neira, A. (s.f.). *Otros Estandares.* Recuperado el 14 de Septiembre de 2010, de iso27000.es: http://www.iso27000.es/download/doc_otros_estandar_all.pdf

Machines, L. (2002). Information Security Survey on Internal Threats.

Mantilla, S. A. (2005). Auditoría del control interno.

Meyer, C. O. (2010). Seguridad Informatica vs Seguridad de la Información.

ORACLE. (2010). Conceptos de Seguridad.

Oracle. (2009). Enfoque Tecnico Oracle Circular 14 V5. Bogota.

Security, E. (2010). ISO 27001 · Certificación de la Gestión de la Seguridad de la Información · Implantación SGSI.

Singleton, T. (2007). The COSO Model: How IT Auditors Can Use It to Evaluate the Effectiveness of Internal Controls.

Solla, J. L. (2009). Gestión del Ciclo de Vida de la Información.

Superintendencia Financiera de Colombia. (2009). *superfinanciera.* Recuperado el 16 de Agosto de 2010, de http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ance038_09.doc

WHITE HOUSE. (29 de Mayo de 2009). *REMARKS BY THE PRESIDENT*. Recuperado el 2010 de Septiembre de 5, de whitehouse:

http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

2. Bibliografía

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. "Compendio tesis y otros trabajos de grado". Bogotá: Legis S.A, 2006.

3. Glosario

SCI: Sistema de Control Interno.

ISO: International Standarization Organization.

SOX: Sarbanes-Oxley Act of 2002(Ley Sarbanes Oxley).

SGSI: Sistema de Gestión de Seguridad de la Información.

COSO: Committee of Sponsoring Organizations of the Tread- way Commission.

Hacker: "Programador perfeccionista y obsesivo, hábil en el uso de los sistemas, que gusta de explorarlos al detalle" (Prieto, 2010)

Malware: Forma reducida de "*malicious* y *software"* y este contiene programas espías, envío de spam, virus.

Red Zombi: BotNet.

BotNets: Conjunto de computadores que son controlados remotamente para fines maliciosos.

Ataque Dirigido: Uso de grandes redes de computadores para realizar peticiones constantes a un punto específico, por ejemplo un servidor de correo.

Ciberseguridad: Seguridad relacionada con los medios tecnológicos como computadores, celulares, televisión digital.

Ciberdelincuencia: Es un delito informático el cual ha sido realizado a través de un medio digital y ha repercutido en un sistema protegido de manera jurídica.

TI: Tecnología de la Información.

DBA: Database Administrator. Rol que desempeña labores de administración de una base de datos.

GRC: Governance Risk and Compliance

V- ANEXOS

Documento completo en TG_Documento Final.doc