UNIVERSIDAD GABRIELA MISTRAL
FACULTAD DE INGENIERIA

ANÁLISIS DE RIESGOS APLICADO A BASE DE DATOS ORACLE SOBRE SISTEMA OPERATIVO LINUX; ADHERIDO AL MARCO METODOLÓGICO COBIT®

Memoria para optar al título de Ingeniero de Ejecución en Informática

Autor : Manuel René Castro Sandoval
Profesor Guía : Roberto Carú Cisternas
Profesor Integrante : Jorge Tapia Castillo

Santiago – Chile
Noviembre, 2010

ÍNDICE

DEDICATORIA

"Padre es quién te cría, te da amor, esperanza y fe…El esfuerzo dedicado en este estudio y los años previos a mi formación académica estuvieron, en cada minuto, pensados en el impulsor de mi formación profesional y personal, que con esfuerzo y perseverancia, me entregó los valores y principios que no me permitieron desistir de mis metas y objetivos durante su vida, y desde adonde ahora se encuentre".

René Manuel Sandoval Baeza (1937-2004)

AGRADECIMIENTOS

*"A mi familia, padres, hermanos y en especial a mi **Esposa e Hijo** que sacrificaron su valioso tiempo en función de mi desarrollo profesional otorgándome apoyo, comprensión y amor durante estos años."*

1. INTRODUCCIÓN

Hace algunos unos años la seguridad de la información no tenía la prioridad que tiene en la actualidad, sin embargo, toda solución tecnológica que opere a través de un sistema y/o aplicación que maneje datos de algún tipo, es soportado por algún fichero o repositorio de datos sobre el cual se puedan ejecutar consultas, actualizaciones y modificaciones. Hoy en día, cualquier aplicación independientemente del lenguaje en el que este programada, consulta, modifica e introduce nuevos datos en una Base de Datos[1] (BD). Las BD se han convertido en el punto en el que convergen todas las aplicaciones, es por esto, que cualquier tipo de ataque a un sistema se realiza con el único fin de la obtención de datos e información, por ende, es necesario conocer los accesos no autorizados, los accesos de personas a información para la cual no tienen privilegios, el borrado o modificación de información privilegiada y procedimientos de recuperación y mantención, entre otros. En la actualidad la creación e implementación de procedimientos de seguridad ayudan a proteger lo que se han convertido en el bien más importante de las empresas: los datos. Y, aunque el almacenamiento de estos datos en una BD los hace mas útiles y disponibles para todo propósito, también los hace vulnerables a un acceso no autorizado. Por otra parte la dependencia de la disponibilidad de los datos para que las aplicaciones funcionen se hace imprescindible. Además la optimización y mantención de las BD es esencial, ya que, si actúa como una arquitectura concurrente puede degradarse fácilmente el nivel de servicio hacia los usuarios.

Toda la información importante debe estar protegida, este resguardo debe cumplir, ante todo, con las leyes y regulaciones locales, y objetivos para lo que esta fue dispuesta. La información es necesaria resguardarla pero debe ser confiable, confidencial y debe de estar disponible cuando se requiera, esto se refiere a que esta debe ser verídica e íntegra desde su origen, pero no debe de ser eliminada o alterada sin consentimiento explícito, ya sea, por error o intencionalmente, además debe de

[1] Repositorio que almacena datos lógicos.

estar disponibles en todo momento, pero solo para los propósitos para la que fue almacenada

Toda organización tiene una misión en donde los riesgos de seguridad de información deben ser considerados bajo un contexto de negocio. En esta era digital, las organizaciones utilizan sistemas tecnológicos para automatizar sus procesos o manejo de información y deben estar conscientes que la administración del riesgo informático juega un rol crítico para cumplir con los objetivos de negocio.

Según la ISO 17799: *"La seguridad de la información se puede caracterizar por la preservación de la Confidencialidad, Integridad y Disponibilidad".*

Actualmente, gran parte de la industria, tiene la convicción de que su información es uno de sus activos más valiosos, grandes corporaciones, organizaciones gubernamentales, establecimientos educacionales y pequeños empresarios utilizan herramientas para análisis de información en las más diversas áreas, tales como, ventas, marketing, contabilidad, recursos humanos, estudios de mercado, entre otras. También podemos mencionar que en base a los sistemas de información se ejecutan operaciones cotidianas que en su objetivo final es otorgar simplicidad, seguridad y comodidad sobre una transacción específica, tales como, transacciones financieras, operaciones relacionadas al sistema de salud y previsional, entre otras. La base de todo sistema tecnológico tiene, de alguna forma, su fin en el manejo de datos, que dispuestos de distintas formas se traducen en información para un objetivo específico.

"El dato es una afirmación aislada sobre la realidad, y la información es un conjunto de datos que permite llegar a conclusiones útiles."

Para el usuario que maneja datos en un sistema de información, las expectativas de este incluyen:

- Que pueda tener acceso a los datos cuando los necesita (un sistema confiable).
- Que los datos mantengan su integridad en el futuro (que los datos no cambien en su transporte).

- Que los datos no se alteren sin autorización.
- Que los datos no se lean sin autorización.

Estas expectativas pueden verse fracasadas por factores accidentales o intencionales.

"Los defensores tienen que cerrar todas las puertas. Los invasores sólo tienen que encontrar una abierta".

Dado lo anterior es que el trabajo pretende demostrar, a través de un análisis de riesgos, la importancia de asegurar los datos almacenados en una BD bajo el contexto del Software y Sistema Operativo base utilizados para este propósito, según el alcance de esta revisión.

Como antecedente podemos mencionar que Oracle es un SGBDR[2] ampliamente usado en el mercado por grandes y medianas organizaciones para la gestión de sus datos (Ver punto 2.3).

Por otra parte, la metodología para alcanzar el objetivo del estudio es COBIT[3] 4.1 perteneciente al ITGI, quienes han diseñado y creado esta publicación de buenas prácticas titulada COBIT® 4.1, principalmente como un recurso educacional para los Oficiales de Seguridad de la Información, Alta Gerencia y profesionales de la administración y control de las tecnologías de la información.

1.1. Hipótesis

Demostrar que utilizando un estándar de trabajo común en la industria de tecnologías de información (COBIT), es posible identificar debilidades y vulnerabilidades, para así, proponer medidas mitigantes a los riesgos inherentes a un sistema que utilice una base de datos (Oracle) y un sistema operativo (Linux[4]) habitualmente usado por las empresas.

[2] Sistema de Gestión de Bases de Datos Relacionales
[3] Metodología que unifica las mejores prácticas de las TI
[4] Es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando así origen a ediciones domésticas, empresariales y para servidores

1.2. Objetivo General

El objetivo general de esta revisión es otorgar un marco de trabajo para identificar, mitigar, aceptar o transferir los riesgos inherentes a un SGBDR Oracle que resida en un sistema operativo Linux.

1.3. Objetivo Específico

El objetivo principal del estudio es otorgar un marco de trabajo de control para identificar los riesgos de seguridad existentes en la arquitectura compuesta por el uso del SGBDR propietario de Oracle en su versión Express 10G, sobre un sistema operativo Linux bajo su distribución Centos en su versión 5.5, en consecuencia identificar los controles y contramedidas existentes para mitigar, aceptar o transferir los riesgos de seguridad asociados a esta arquitectura y en su defecto, proponer nuevos controles como resultado del estudio.

1.4. Alcance

Desarrollar un análisis de riesgos que como resultado otorgue un programa de trabajo genérico, que como línea base, permita asegurar las condiciones mínimas de seguridad y disponibilidad de los datos que residan en el SGBDR Oracle elegido, (Oracle 10g Express Edition, sobre un sistema operativo Linux en su distribución Centos versión 5.5).

1.5. Antecedentes

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (StakeHolders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los

riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

La versión de Oracle utilizada para este estudio será la última liberada por el fabricante correspondiente a la Express Edition 10g, la versión libre que provee el fabricante y se ajusta a los propósitos del estudio, sin perjuicio en la aplicabilidad de los resultados a otras versiones pagadas.

La elección del sistema operativo es Linux en su distribución Centos bajo la versión 5.3, esta distribución de Linux fue seleccionada, ya que, responde a la versión paralela del fabricante Red Hat Enterprise, muy usado a nivel corporativo, pero que conlleva en sus propósitos facilitar los estudios de laboratorio con licencia libre de uso.

La arquitectura propuesta será levantada en un laboratorio que permitirá el desarrollo de pruebas y su documentación durante el estudio. La metodología del análisis utilizada será COBIT 4.1, la cual nos permitirá trabajar dentro de un marco que actualmente permite el desarrollo de políticas claras y de buenas prácticas para control de las Tecnologías de la Información (TI), en las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de las TI y el marco de referencia general para el gobierno de las TI que ayuda a comprender y administrar los riesgos y beneficios asociados con estas mismas. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de las TI y de las decisiones a tomar acerca de las tecnologías usadas en las empresas, en el caso específico de este estudio al SGBDR de Oracle sobre el sistema operativo Linux, Centos, será un análisis que nos permitirá verificar los controles y contramedidas inherente a esta arquitectura, o en su defecto proponerlas como resultados del análisis sobre la arquitectura ya mencionada. Esta última toma relevancia, ya que, es una de las arquitecturas más utilizadas en la industria.

El aspecto de la informática más relevante, en este estudio, es referente a la seguridad de la información provista por un conjunto de herramientas que usa la

empresa actual, en donde se presume con fundamentos, el manejo de datos críticos en la mayoría de los rubros y áreas de servicios, en consecuencia, el análisis tendrá un fuerte enfoque acerca de la seguridad cubierta sobre este tipo de arquitectura tecnológica en donde los procedimientos a seguir serán los que se adhieran a la metodología COBIT, por qué cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito del negocio. La dirección espera un alto entendimiento de la manera en que las TI son dispuestas y la posibilidad de que sean aprovechadas con éxito para tener una ventaja competitiva.

En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Se garantice el logro de sus objetivos.
- Tenga suficiente flexibilidad para aprender y adaptarse.
- Cuente con un manejo juicioso de los riesgos que enfrenta.
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas.

Las empresas exitosas entienden los riesgos y aprovechan los beneficios de las TI, y encuentran maneras para:

- Alinear la estrategia de TI con la estrategia del negocio.
- Medir el desempeño de TI.

Además, el gobierno y los marcos de trabajo de control están siendo parte de las mejores prácticas de la administración de TI y sirven como facilitadores para establecer el gobierno de las TI y cumplir con el constante incremento de requerimientos regulatorios, según su rubro o prestación de servicios.

Las mejores prácticas de las TI se han vuelto significativas debido a un número de factores:

- Los directores de negocio y consejos directivos que demandan un mayor retorno de la inversión en las TI, es decir, que las TI generen lo que el negocio necesita para mejorar el valor de los participantes
- Preocupación por el creciente nivel de gasto en las TI.

- La necesidad de satisfacer requerimientos regulatorios para controles de las TI en áreas como privacidad y reportes financieros (por ejemplo, Sarbanes-Oxley[5], Basilea II[6], entre otros) y en sectores específicos como el financiero, farmacéutico y de atención a la salud.
- La selección de proveedores de servicio y el manejo de Outsourcing y de adquisición de servicios.
- Riesgos crecientes y complejos de las TI, como por ejemplo la seguridad de base de datos.
- Iniciativas de gobierno de las TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de las TI, aumentar el valor del negocio y reducir los riesgos de éste.
- La madurez creciente y la consecuente aceptación de marcos de trabajo respetados tales como COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2.
- La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia (Benchmarking[7]).

El trabajo se enfocó principalmente en tres partes que consistieron en ejecutar un descubrimiento de puertos, un análisis de vulnerabilidades y un test de penetración a las arquitecturas instalada por defecto, para que con los resultados obtenidos de estos estudios se estableciera un marco de trabajo que permitiese efectuar un análisis de riesgos y sus controles mitigantes, como adheridos a una extracción del marco referencial COBIT.

[5] La Ley Sarbanes Oxley, cuyo título oficial en inglés es Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002), es una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. También es llamada Sox, Sarbox o SOA.
[6] Es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea
[7] Comparación en términos comerciales o financieros

2. MARCO TEÓRICO REFERENCIAL

2.1. COBIT®: Marco metodológico.

COBIT fue publicado por primera vez por ITGI[8] en abril de 1996. Su última actualización – COBIT® 4.1 hace énfasis en el cumplimiento reglamentario, ayudando a la organizaciones a incrementar el valor de TI, destacando los vínculos entre los objetivos del negocio y TI, y simplificando la implementación del marco de trabajo COBIT. Este marco de trabajo es la base para diferentes entes reguladores a nivel mundial, con la finalidad de lograr que las entidades reguladas optimicen sus inversiones de TI y administren adecuadamente sus riesgos tecnológicos.

2.1.1. COBIT reduce riesgos y mejora desempeño de las TI.

El Instituto de Gobierno de Tecnologías de la Información (ITGI) anunció la publicación de COBIT 4.1, una actualización de la guía COBIT (Control de Objetivos para Tecnologías de la Información y Relacionadas), que ayuda a reducir riesgos de las tecnología de la información (TI).

Usado generalmente como herramienta para uso conjunto con Sarbanes-Oaxley y otros estándares mundiales, COBIT se anticipa a la reglamentación que es decretada alrededor del mundo. Es el producto de 15 años de investigación y cooperación entre expertos mundiales en las TI y negocios. La nueva versión está disponible gratuitamente en la dirección electrónica de la organización no lucrativa e independiente ITGI en: www.itgi.org

COBIT 4.1 es una actualización significativa del marco mundial aprobado que asegura que las TI estén alineadas con los objetivos de negocio, sus recursos sean usados responsablemente y sus riesgos administrados de forma apropiada. COBIT 4.1 representa una mejora indiscutible del COBIT 4.0 y puede usarse para perfeccionar el trabajo basado en versiones anteriores de COBIT.

COBIT ayuda a las organizaciones a reducir riesgos en el manejo de las TI e incrementar el valor derivado de su uso. Las actualizaciones en COBIT 4.1

[8] Information of Tecnology Governance Institute (por sus siglas en inglés)

incluyen: avances en la medición del desempeño; mejores objetivos de control; y una excelente alineación entre objetivos de negocio y de TI.

COBIT es el único marco administrativo que comprende el ciclo de vida completo de la inversión en TI. Considera los logros en los objetivos de negocio, asegura alineación de las TI con el negocio y mejora la eficiencia y efectividad de las TI, afirma Roger Debreceny, Jefe del Comité de Manejo de COBIT del ITGI. COBIT 4.1 está creado como una guía práctica para administradores alrededor del mundo que lo utilizan para perfeccionar el gobierno de TI en sus organizaciones, así que ha sido probado y validado.

Además de COBIT 4.1, ITGI lanzó tres publicaciones complementarias disponibles a través de la biblioteca ISACA (www.isaca.org/bookstore):

Practicas de Control de COBIT, 2da Edición, que contiene prácticas de control mejoradas y alineadas con COBIT 4.1. Dichas prácticas están orientadas a la acción y proveen argumentos dirigidos a la forma de obtener valor y limitar riesgos.

Guía de Implementación de Gobierno TI: Uso de COBIT y Val IT, 2da Edición. Esta publicación proporciona un itinerario detallado para establecer efectivamente el gobierno de TI en una organización, con una guía que muestra como COBIT puede dar soporte a esta actividad. También ofrece una explicación detallada del alcance del proyecto de gobierno.

2.1.2. Guía de Aseguramiento de TI

Uso de COBIT al remplazar la Guía del Aseguramiento[9], este libro ofrece una guía de cómo COBIT puede dar soporte a una gran variedad de acciones de aseguramiento y cómo una revisión del mismo puede ser desarrollada para cada uno de los procesos de TI.

[9] Publicación del ITGC

2.1.3. Beneficios

COBIT se ha convertido en el integrador de la mejores prácticas de TI y el marco de trabajo global de gobierno de TI, debido a su armonización con otros estándares como ITIL[10], COSO[11], ISO 20000[12], ISO 9000[13], ISO 25999[14], ISO 27001[15], PRINCE2[16], TOGAF[17], entre otros y su constante actualización.

La estructura de procesos de COBIT, en conjunto con su alto nivel y su enfoque "orientado al negocio" provee una visión de punta a punta de TI, que ayuda a las organizaciones a obtener el mayor valor posible de sus inversiones de TI.

2.1.3.1. Algunos de los beneficios que se pueden obtener con COBIT

- Mejor alineación basada en una focalización sobre el negocio.
- Visión comprensible de las TI para su administración.
- Clara definición de propiedad y responsabilidades.
- Aceptabilidad general con terceros y entes reguladores.
- Entendimiento compartido entre todos los interesados basados en un lenguaje común.
- Cumplimiento global de los requerimientos de las TI planteados en el Marco de Control Interno de Negocio COSO.

COBIT apoya al Gobierno de las TI, proporcionando un marco para garantizar que:

- Las TI estén alineada con el negocio
- Permite a las empresas maximizar sus beneficios

10 La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI)

11 Committee of Sponsoring Organizations of the Treadway Commission

12 Service Management normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) el 14 de diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información)

13 designa un conjunto de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional para la Estandarización (ISO). Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios

14 Business Continuity Management. Code of Practice

15 Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar)

16 PRojects IN Controlled Environments (PRINCE), en español: proyectos en entornos controlados, es un método de gestión de proyectos que cubre la administración, control y organización de un proyecto. PRINCE2 es una marca registrada de la OGC del Reino Unido.

17 The Open Group Architecture Framework (TOGAF) (o Esquema de Arquitectura de Open Group, en español) es un esquema (o marco de trabajo) de Arquitectura Empresarial que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial de información

- Los recursos de las TI se utilicen de manera responsable
- Riesgos de las TI se gestionan adecuadamente

2.1.3.2. Beneficios de la aplicación de COBIT

La aplicación de COBIT permite:

- Mejor alineación con el negocio.
- Una cuenta comprensible para la gestión de las TI.
- Borrar la propiedad y las responsabilidades.
- Por lo general es aceptado por terceros (proveedores y clientes) y entes reguladores.
- Entendimiento común entre todas las partes interesadas sobre la base de un idioma común.
- Cumplimiento de los requisitos COSO para el entorno de control de las TI.
- COBIT se ha convertido en el integrador de las TI de las mejores prácticas y el marco general para los profesionales que trabajan con TI, ya que, se han armonizado con otras normas y se mantiene actualizado continuamente hasta la fecha. La estructura de un proceso de COBIT, en conjunto con su alto nivel y el enfoque orientado al negocio, proporciona una visión de extremo a extremo el entendimiento en las mejoras de las organizaciones para obtener el máximo valor posible de las inversiones en las TI.

2.1.3.3. Panorama General de COBIT 4.1

COBIT ® 4.0 fue liberado en noviembre de 2005 y marcó la primera gran actualización del contenido básico desde la liberación de COBIT ® 3 ª edición del año 2000. Un incremento en la actualización de COBIT 4.0 y COBIT 4.1 incluye racionalización de los objetivos de control y controles de aplicación, la

mejora de procesos, controles y una mayor explicación de la medición del desempeño.

Al igual que en versiones anteriores de COBIT, COBIT 4.1 aprovecha la experiencia de numerosos expertos internacionales. El marco de control de COBIT vinculó iniciativas de las TI a las necesidades del negocio, organiza las actividades de las TI en un modelo y proceso generalmente aceptados, identifica los principales recursos de TI y define la gestión de tener en cuenta los objetivos de control. COBIT 4.1 representa un consenso de expertos de todo el mundo que continuamente trabajan juntos para mantener la relevancia de este, se benefician de la oportunidad que otorga COBIT.

COBIT 4.1 se compone de cuatro secciones:

La visión general ejecutiva

- El marco
- El contenido básico (objetivos de control, directrices de gestión y los modelos madurez)
- Apéndices (mapeos y cruzadas, modelo de madurez adicionales información, material de referencia, un proyecto y descripción de un glosario)

El contenido básico está dividido de acuerdo con los 34 procesos de las TI. Cada proceso es cubierto en cuatro secciones de aproximadamente una página cada uno, combinando para dar un imagen completa de cómo controlar, gestionar y medir el proceso.

Las cuatro secciones para cada proceso, en fin, son los siguientes:

2.1.3.4. El alto nivel de control objetivo del proceso

Es una descripción del proceso para resumir los objetivos de este mismo.

2.1.3.5. El alto nivel de control, de los objetivos representados en una cascada de procesos

Se refiere al mapeo de los procesos para el proceso de dominios, describir la información de criterios y los recursos.

2.1.3.6. Directrices de gestión

Se refiere a las entradas y salidas del proceso, un gráfico de RACI[18] , las metas y las métricas.

2.1.3.7. Modelo de madurez para el proceso, es otra forma de ver el rendimiento de este mismo

- Proceso de insumos son lo que el proceso propietario tiene como necesidades de los demás.
- El proceso de descripción, describe lo que el proceso propietario tiene que hacer.
- El proceso de los productos son lo que el proceso propietario debe entregar.
- Las metas y los indicadores muestran cómo el proceso debe ser medido.
- El gráfico RACI define lo que es necesario ser delegado y a quién.
- El modelo de madurez muestra cómo el proceso puede ser mejorado.

2.1.4. Áreas del foco del Gobierno de las TI

La alineación estratégica se centra en asegurar la vinculación de negocios y de los planes de las TI, en definir, mantener y validar el valor de las proposiciones de las IT, y en la adaptación de las operaciones de las TI con las operaciones de la empresa.

El valor de la entrega se acerca a la ejecución de la propuesta de valor en todo el ciclo de entrega, garantizando que ofrece los beneficios prometidos en post

[18] Matriz de Asignación de Responsabilidades (según sus siglas en inglés de: Responsable, Accountable, Consulted, Informed)

de la estrategia, centrándose en la optimización de costos y demostrar el valor intrínseco de la tecnología de la información.

Gestión de recursos se refiere a la inversión óptima, y la adecuada gestión de los recursos de TI críticos: procesos, personas, aplicaciones, la infraestructura y la información. Las cuestiones clave se relacionan con la optimización de los conocimientos y la infraestructura.

La gestión del riesgo requiere concientización de los riesgos los por altos directivos, una clara comprensión de la empresa para el apetito de riesgo, transparencia acerca de los importantes riesgos para la empresa, y la incorporación de la gestión del riesgo a las responsabilidades en la organización.

Medición del desempeño, pistas de auditoría y monitores de la aplicación de la estrategia, la finalización del proyecto, la utilización de recursos, el rendimiento del proceso y la prestación de servicios, utilizando, por ejemplo, la puntuación equilibrada que traduce la estrategia en acción para lograr objetivos mesurables más allá de contabilidad convencional.

2.2. La Triada

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability"), son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez

conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.

2.2.1. Confidencialidad

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

2.2.2. Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto

de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

2.2.3. Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad de los sistemas críticos debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones de estos mismos.

Garantizar la disponibilidad implica también la prevención de ataques de denegación de servicio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de Web etc., mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN[19]), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

2.2.4. Servicios de Seguridad

El objetivo de este servicio es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones.

[19] Storage Area Network

Los servicios de seguridad están diseñados para contrarrestar los ataques y hacen uso de uno o más mecanismos para proporcionarlo.

2.2.5. No Repudio

Proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2[20].

No Repudio de origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

Prueba que el mensaje fue enviado por la parte específica.

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Prueba que el mensaje fue recibido por la parte específica.

Si la autenticidad prueba quién es el autor de un documento y cual es su destinatario, el “no repudio” prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje. Definición según la recomendación X.509[21] de la UIT-T [22]

[20] Estándar internacional referente a los sistemas de tratamiento de Información, Interconexión de Sistemas Abiertos, Modelos de Referencia Básicos de Arquitectura de Seguridad

[21] En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas

Servicio que suministra la prueba de la integridad y del origen de los datos- ambos en una relación infalsificable que pueden ser verificados por un tercero en cualquier momento.

2.2.6. Protocolos de Seguridad de la Información

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información.

Se componen de:

2.2.6.1. Criptografía (cifrado de datos)

Se ocupa del cifrado de mensajes un mensaje es enviado por el emisor lo que hace es transposicionar o ocultar el mensaje hasta que llega a su destino y puede ser descifrado por el receptor.

2.2.6.2. Lógica (estructura y secuencia)

Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuando se va enviar el mensaje.

2.2.6.3. Autenticación

Es una validación de identificación, es la técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

2.2.7. Principales atacantes

2.2.7.1. El Hacker

Es una persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, se mantiene permanentemente

[22] El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT)

actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador innato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura".

Su formación y las habilidades que posee le dan una experticia mayor que le permite acceder a sistemas de información seguros, sin ser descubierto, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

2.2.7.2. El Cracker

Se denomina así a aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un Cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.

2.2.7.3. El Lammer

A este grupo pertenecen aquellas personas deseosas de alcanzar el nivel de un hacker pero su poca formación y sus conocimientos les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa publicado en la red.

2.2.7.4. El Copyhacker

Son una nueva generación de falsificadores dedicados al crackeo de Hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos los bucaneros.

Se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.

2.2.7.5. Bucaneros

Son los comerciantes de la red, aunque no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.

2.2.7.6. Phreaker

Se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los celulares, han tenido que ingresar también al mundo de la informática y del procesamiento de datos.

2.2.7.7. Newbie

Es el típico "novato" en la red, sin proponérselo tropieza con una página de hacking y descubre que en ella existen áreas de descarga de buenos programas de hackeo, baja todo lo que puede y empieza a trabajar con ellos.

2.2.7.8. Script Kiddie

Denominados también “Skid kiddie”, son simples usuarios de Internet, sin conocimientos sobre Hack o Crack aunque aficionados a estos temas, no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red y a buscar programas que luego ejecutan sin los más mínimos conocimientos, infectando en algunos casos de virus a sus propios equipos. También podrían denominarse los “Pulsa Botones o Clickquiadores” de la red.

2.2.8. Planificación de la seguridad

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad del sistema es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles en el lugar o los previstos para cumplir esos requisitos. El plan de seguridad del sistema también delinea las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema. Debe reflejar las aportaciones de distintos gestores con responsabilidades sobre el sistema, incluidos los propietarios de la información, el propietario de la red, y el alto funcionario de la agencia de información de seguridad.

Los administradores de programas, los propietarios del sistema, y personal de seguridad en la organización debe entender el sistema de seguridad en el proceso de planificación. Los responsables de la ejecución y gestión de sistemas de información deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas.

2.2.9. Creación de un plan de respuesta a incidentes

Es importante formular un plan de respuestas a incidentes, soportarlo a lo largo de la organización y probarlo regularmente. Un buen plan de respuestas a incidentes puede no sólo minimizar los efectos de una violación sino también, reducir la publicidad negativa.

Desde la perspectiva del equipo de seguridad, no importa si ocurre una violación o abertura (pues tales eventos son una parte eventual de cuando se hacen negocios usando un método de poca confianza como lo es Internet), si no más bien cuando ocurre. El aspecto positivo de entender la inevitabilidad de una violación a los sistemas (cualquier sistema donde se procese información confidencial, no esta limitado a servicios informáticos) es que permite al equipo de seguridad desarrollar un curso de acciones para minimizar los daños potenciales.

Combinando un curso de acciones con la experiencia le permite al equipo responder a condiciones adversas de una manera formal y oportuna.

El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata para detener o minimizar el incidente
- Investigación del incidente
- Restauración de los recursos afectados
- Reporte del incidente a los canales apropiados

Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

Un plan de respuesta a incidentes tiene un número de requerimientos, incluyendo:

- Un equipo de expertos locales (un equipo de respuesta a emergencias de computación)
- Una estrategia legal revisada y aprobada
- Soporte financiero de la compañía
- Soporte ejecutivo de la gerencia superior
- Un plan de acción factible y probado
- Recursos físicos, tal como almacenamiento redundante, sistemas en stand by y servicios de respaldo

Consideraciones legales. Otros aspectos importantes a considerar en una respuesta a incidentes son las ramificaciones legales. Los planes de seguridad deberían ser desarrollados con miembros del equipo de asesoría jurídica o alguna forma de consultoría general. De la misma forma en que cada compañía debería tener su propia política de seguridad corporativa, cada compañía tiene su forma

particular de manejar incidentes desde la perspectiva legal. Las regulaciones locales, de estado o federales están más allá del ámbito de este documento, pero se mencionan debido a que la metodología para llevar a cabo el análisis post-mortem, será dictado, al menos en parte, por la consultoría jurídica. La consultoría general puede alertar al personal técnico de las ramificaciones legales de una violación; los peligros de que se escape información personal de un cliente, registros médicos o financieros; y la importancia de restaurar el servicio en ambientes de misión crítica tales como hospitales y bancos.

Planes de Acción. Una vez creado un plan de acción, este debe ser aceptado e implementado activamente. Cualquier aspecto del plan que sea cuestionado durante la implementación activa lo más seguro es que resulte en un tiempo de respuesta pobre y tiempo fuera de servicio en el evento de una violación. Aquí es donde los ejercicios prácticos son invalorables. La implementación del plan debería ser acordada entre todas las partes relacionadas y ejecutada con seguridad, a menos que se llame la atención con respecto a algo antes de que el plan sea colocado en producción.

La respuesta a incidentes debe ir acompañada con recolección de información siempre que esto sea posible. Los procesos en ejecución, conexiones de red, archivos, directorios y mucho más deberían ser auditados activamente en tiempo real. Puede ser muy útil tener una toma instantánea de los recursos de producción al hacer un seguimiento de servicios o procesos maliciosos. Los miembros de CERT[23] y los expertos internos serán recursos excelentes para seguir tales anomalías en un sistema.

2.2.10. El manejo de riesgos dentro de la seguridad en la información

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riegos que un activo ó bien puede tener dentro de los procesos en una empresa. Esta clasificación lleva el nombre de manejo de riegos. El manejo de riesgos, conlleva una estructura bien definida, con

[23] Por el acrónimo inglés "Computer Emergency Response Team"

un control adecuado y su manejo, habiéndolo identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

2.2.10.1. Evitar

El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades.

Ejemplo: No instalar empresas en zonas sísmicas

2.2.10.2. Reducir

Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación controles y su monitoreo constante.

Ejemplo: No fumar en ciertas áreas, instalaciones eléctricas anti flama, planes de contingencia.

2.2.10.3. Retener, Asumir o Aceptar el riesgo

Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento.

Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas.

La retención involuntaria se da cuando el riesgo es retenido inconscientemente.

Ejemplo de Asumir el riesgo: Con recursos propios se financian las pérdidas.

Transferir. Es buscar un respaldo y compartir el riego con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riego de un lugar y transferirlo a otro, ó para minimizar el mismo, compartiéndolo con otras entidades.

Ejemplo: Transferir los costos a la compañía aseguradora

2.2.11. Medios de transmisión de ataques a los sistemas de seguridad

El mejor en soluciones de su clase permite una respuesta rápida a las amenazas emergentes, tales como:

Malware[24] propagación por e-mail y Spam[25].

La propagación de malware y botnets[26].

Los ataques de phishing[27] alojados en sitios Web.

Los ataques contra el aumento de lenguaje de marcado extensible (XML[28]) de tráfico, arquitectura orientada a servicios (SOA[29]) y Web Services.

Estas soluciones ofrecen un camino a la migración y la integración. Como las amenazas emergentes, cada vez más generalizada, estos productos se vuelven más integrados enfocándose a los sistemas.

El enfoque de configuración de sistemas, la política, y el seguimiento, reúnen cumplimiento necesario de las normativas en curso y permite a los sistemas de gestión una mayor rentabilidad.

En la actualidad gracias a la infinidad de posibilidades que se tiene para tener acceso a los recursos de manera remota y al gran incremento en las conexiones a la Internet, los delitos en el ámbito de TI se han visto incrementado, bajo estas circunstancias los riesgos informáticos son más latentes. Los delitos cometidos mediante el uso de la computadora han crecido en tamaño, forma y

[24] Malware (del inglés malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario
[25] Se llama spam, correo basura o sms basura a los mensajes no solicitados, no deseados o de remitente desconocido
[26] Botnet es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática.
[27] Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta
[28] XML, siglas en inglés de eXtensible Markup Language (lenguaje de marcas extensible), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C)
[29] Arquitectura Orientada a Servicios (en inglés Service Oriented Architecture)

variedad. Los principales delitos hechos por computadora o por medio de computadoras son:

Fraudes

Falsificación

Venta de información

Entre los hechos criminales más famosos en los EE.UU. están:

El caso del Banco Wells Fargo donde se evidencio que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.

El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.

El caso de un muchacho de 15 años que entrando a una computadora de la Universidad de Berkeley en California destruyo gran cantidad de archivos.

También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una pérdida de USD 3 millones.

Los virus[30], trojanos[31], spyware[32], malware y demás código llamado malicioso (por las funciones que realiza y no por tratarse de un código erróneo), tienen como objetivo principal el ejecutar acciones no solicitadas por el usuario, las cuales pueden ser desde, el acceso a un pagina no deseada, el redireccionamiento de algunas páginas de Internet, suplantación de identidad o incluso la destrucción o daño temporal a los registros del sistemas, archivos y/o carpetas propias. El virus informático es un programa elaborado accidental o intencionalmente, que se introduce y se transmite a través de cualquier medio

[30] Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario

[31] e denomina troyano o caballo de Troya (traducción literal del inglés Trojan horse) a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños

[32] Un programa espía, traducción del inglés spyware, es un programa, dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste

extraíble y transportable o de la misma red en la que se encuentre un equipo infectado, causando diversos tipos de daños a los sistemas. Por ejemplo: El virus llamado viernes trece o Jerusalén, que desactivó el conjunto de ordenadores de la defensa de Israel y que actualmente se ha extendido a todo el mundo.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba de un virus que fue se distribuyo desde un BBS[33] y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica EGA[34], pero al ejecutarlo salía la presentación pero al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía "Caíste".

Este dato se considera como el nacimiento de su nombre, ya que los programas con código integrado, diseñados para hacer cosas inesperadas han existido desde que existen las propias computadoras. Las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipament Corporation (DEC) empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

2.2.12. Otros Conceptos

Otros conceptos relacionados son:

Auditabilidad: Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Identificación: verificación de una persona o cosa; reconocimiento.

Autenticación: Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Autorización: Lo que se permite cuando se ha otorgado acceso.

No repudio: no se puede negar un evento o una transacción.

Seguridad en capas: La defensa a profundidad que contenga la inestabilidad.

[33] Bulletin Board System (Sistema de Tablón de Anuncios)
[34] EGA es el acrónimo inglés de Enhanced Graphics Adapter, la especificación estándar de IBM PC para visualización de gráficos

Control de Acceso: limitar el acceso autorizado solo a entidades autenticadas.

Métricas de Seguridad, Monitoreo: Medición de actividades de seguridad.

Gobierno: proporcionar control y dirección a las actividades.

Estrategia: los pasos que se requieren para alcanzar un objetivo.

Arquitectura: el diseño de la estructura y las relaciones de sus elementos.

Gerencia: Vigilar las actividades para garantizar que se alcancen los objetivos.

Riesgo: la explotación de una vulnerabilidad por parte de una amenaza.

Exposiciones: Áreas que son vulnerables a un impacto por parte de una amenaza.

Vulnerabilidades: deficiencias que pueden ser explotadas por amenazas.

Amenazas: Cualquier acción o evento que puede ocasionar consecuencias adversas.

Riesgo residual: El riesgo que permanece después de que se han implementado contra medidas y controles.

Impacto: los resultados y consecuencias de que se materialice un riesgo.

Criticidad: La importancia que tiene un recurso para el negocio.

Sensibilidad: el nivel de impacto que tendría una divulgación no autorizada.

Análisis de impacto al negocio: evaluar los resultados y las consecuencias de la inestabilidad.

Controles: Cualquier acción o proceso que se utiliza para mitigar el riesgo.

Contra medidas: Cualquier acción o proceso que reduce la vulnerabilidad.

Políticas: declaración de alto nivel sobre la intención y la dirección de la gerencia.

Normas: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

Ataques: tipos y naturaleza de inestabilidad en la seguridad.

Clasificación de datos: El proceso de determinar la sensibilidad y Criticidad de la información.

2.3. Oracle

Oracle es un sistema de gestión de base de datos relacional (o RDBMS por el acrónimo en inglés de Relational Data Base Management Systems), desarrollado por Oracle Corporation[35].

Se considera a Oracle como uno de los sistemas de bases de datos más completos destacándose por, soporte de transacciones, estabilidad, escalabilidad y soporte multiplataforma.

Su dominio en el mercado de servidores empresariales ha sido casi total hasta hace poco, recientemente sufre la competencia del Microsoft SQL Server y de la oferta de otros RDBMS con licencia libre como PostgreSQL, MySql o Firebird. Las últimas versiones de Oracle han sido certificadas para poder trabajar bajo GNU/Linux.

2.3.1. Historia

Oracle surge a finales de los 70 a partir de un estudio sobre SGBD (Sistemas Gestores de Base de Datos) de George Koch. Computer World definió este estudio como uno de los más completos jamás escritos sobre bases de datos. Este artículo incluía una comparativa de productos que fundaba que estos Software como los más completos desde el punto de vista técnico. Esto se debía a que usaba la filosofía de las bases de datos relacionales, algo que por aquella época era todavía desconocido.

En la actualidad, Oracle (Nasdaq: ORCL) todavía encabeza la lista. La tecnología Oracle se encuentra prácticamente en todas las industrias alrededor del mundo y en las oficinas de 98 de las 100 empresas descritas en la revista “Fortune 100”. Oracle es la primera compañía de software que desarrolla e implementa software para empresas cien por ciento activado por Internet a través de toda su línea de productos: base de datos, aplicaciones comerciales y herramientas de desarrollo de aplicaciones y soporte de decisiones. Oracle es el proveedor mundial

[35] Oracle Corporation es una de las mayores compañías de software del mundo. Sus productos van desde bases de datos (Oracle) hasta sistemas de gestión

líder de software para administración de información, y la segunda empresa de software.

Oracle a partir de la versión 10g Release 2, cuenta con 6 ediciones:

Oracle Database Enterprise Edition (EE).

Oracle Database Standard Edition (SE).

Oracle Database Standard Edition One (SE1).

Oracle Database Express Edition (XE).

Oracle Database Personal Edition (PE).

Oracle Database Lite Edition (LE).

La única edición gratuita es la Express Edition, que será utilizada en esta prueba, que a su vez es compatible con las demás ediciones de Oracle Database 10g Release 2 y Oracle Database 11g.

2.4. Distribución Linux

Una distribución Linux (coloquialmente llamada distro) es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando así origen a ediciones domésticas, empresariales y para servidores. Por lo general están compuestas, total o mayoritariamente, de software libre, aunque a menudo incorporan aplicaciones o controladores propietarios.

Además del núcleo Linux, las distribuciones incluyen habitualmente las bibliotecas y herramientas del proyecto GNU[36] y el sistema de ventanas X Window System[37]. Dependiendo del tipo de usuarios a los que la distribución esté dirigida se incluye también otro tipo de software como procesadores de texto, hoja de cálculo, reproductores multimedia, herramientas administrativas, etcétera. En el caso de incluir herramientas del proyecto GNU, también se utiliza el término distribución GNU/Linux.

[36] El proyecto GNU fue iniciado por Richard Stallman con el objetivo de crear un sistema operativo completamente libre: el sistema GNU

[37] X Window System (en español sistema de ventanas X) es un software que fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix.

Existen distribuciones que están soportadas comercialmente, como Fedora (Red Hat), openSUSE (Novell), Ubuntu (Canonical Ltd.), Mandriva, y distribuciones mantenidas por la comunidad libres como Debian y Gentoo. Aunque hay otras distribuciones que no están relacionadas con alguna empresa o comunidad, como es el caso de Slackware[38].

2.4.1. Historia

Antes de que surgieran las primeras distribuciones, un usuario de Linux debía ser algo experto en Unix; no sólo debía conocer qué bibliotecas y ejecutables necesitaba para iniciar el sistema y que funcionase, sino también los detalles importantes que se requieren en la instalación y configuración de los archivos en el sistema.

Las distribuciones Linux comenzaron a surgir poco después de que el núcleo Linux fuera utilizado por otros programadores además de los creadores originales. Existía mayor interés en desarrollar un sistema operativo que en desarrollar aplicaciones, interfaces para los usuarios o un paquete de software conveniente.

Entre las distribuciones más antiguas se incluían:

- Dos discos denominados H J Lu's "Boot-root" con el núcleo y un mínimo de herramientas para utilizar.
- MCC Interim Linux[39], que se podía descargar en un servidor público FTP de la Universidad de Mánchester en febrero de 1992.
- TAMU[40], creado por entusiastas de la Universidad de Texas A&M al mismo tiempo que SLS
- SLS[41] (Softlanding Linux System).
- Yggdrasil [42]Linux creó el primer CD-ROM de una distribución Linux.

[38] Slackware Linux es la distribución Linux más antigua que tiene vigencia.
[39] MCC Interim Linux es una distribución Linux obsoleta inicialmente desarrollada en febrero de 1992 por Owen Le Blanc del Manchester Computing Centre (MCC)
[40] Texas A&M University
[41] Softlanding Linux System (SLS) fue una de las primeras distribuciones del sistema operativo GNU/Linux, fundada por Peter MacDonald a mediados de 1992, que provenía de la distribución conocida como MCC Interim Linux.
[42] fue una de las primeras distribuciones de Linux, desarrollada por Yggdrasil Computing, Incorporated, una empresa fundada por Adam J. Richter en Berkeley, California.

SLS no estuvo bien mantenida; así pues, Patrick Volkerding lanzó una distribución basada en SLS a la que llamó Slackware; lanzada el 16 de julio de 1993.1 Esta es la distribución más antigua que está en desarrollo activo.

Los usuarios vieron en Linux una alternativa a los sistemas operativos DOS[43], Microsoft Windows[44] en la plataforma PC, Mac OS[45] en Apple Macintosh y las versiones de uso bajo licencia (de pago) de UNIX[46]. La mayoría de estos primeros usuarios se habían familiarizado con el entorno UNIX en sus trabajos o centros de estudios. Estos adoptaron GNU/Linux por su estabilidad, reducido (o nulo) costo y por la disponibilidad del código fuente del software.

Las distribuciones eran originalmente una cuestión de comodidad para el usuario medio, evitándole la instalación (y en muchos casos compilación[47]) por separado de paquetes de uso común, pero hoy se han popularizado incluso entre los expertos en éste tipo de sistemas operativos (UNIX / Linux). Si bien, históricamente, Linux estuvo mejor posicionado en el mercado de los servidores, distribuciones centradas en la facilidad de instalación y uso, tales como Fedora, Mandriva, Opensuse, Knoppix y Ubuntu, entre otras, han logrado una mayor aceptación en el mercado doméstico.

2.4.2. Componentes

El escritorio típico de una distribución Linux contiene un núcleo, herramientas y librerías, software adicional, documentación, un sistema de ventanas, un administrador de ventanas y un entorno de escritorio, este suele ser GNOME[48] o KDE[49]. Gran parte del software incluido es de fuente abierta o

[43] "DOS" es una familia de sistemas operativos para PC. El nombre son las siglas de disk operating system
[44] Microsoft Windows es el nombre de una serie de sistemas operativos desarrollados por Microsoft desde 1981, año en que el proyecto se denominaba "Interface Manager".
[45] Mac OS (del inglés Macintosh Operating System, en español Sistema Operativo de Macintosh) es el nombre del sistema operativo creado por Apple para su línea de computadoras Macintosh
[46] Unix (registrado oficialmente como UNIX®) es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy
[47] Un compilador es un programa informático que traduce un programa escrito en un lenguaje de programación a otro lenguaje de programación, generando un programa equivalente que la máquina será capaz de interpretar.
[48] GNOME es un entorno de escritorio e infraestructura de desarrollo para sistemas operativos Unix y derivados Unix como GNU/Linux, BSD o Solaris; compuesto enteramente de software libre.

software libre y distribuido por sus desarrolladores tanto en binario[50] compilado como en forma de código fuente, permitiendo a sus usuarios modificar o compilar el código fuente original si lo desean. Muchas distribuciones incorporan software privativo, no disponible en forma de código fuente.

Muchas distribuciones proveen un sistema de instalación gráfica como lo hacen otros sistemas modernos. Distribuciones independientes como Gentoo Linux, T2 y Linux From Scratch proveen el código fuente de todo el software y solo incluyen los binarios del núcleo, herramientas de compilación y de un instalador; el instalador compila todo el software para el CPU[51] específico de la PC del usuario.

2.4.3. Gestión de paquetes[52]

Las distribuciones están divididas en “paquetes”. Cada paquete contiene una aplicación específica o un servicio. Ejemplos de paquetes son una librería para manejar el formato de imagen PNG[53], una colección de tipografías o un navegador Web.

El paquete es generalmente distribuido en su versión compilada y la instalación y desinstalación de los paquetes es controlada por un sistema de gestión de paquetes en lugar de un simple gestor de archivos. Cada paquete elaborado para ese sistema de paquetes contiene meta-información tal como fecha de creación, descripción del paquete y sus dependencias. El sistema de paquetes analiza esta información para permitir la búsqueda de paquetes, actualizar las librerías y aplicaciones instaladas, revisar que todas las dependencias se cumplan y obtenerlas si no se cuenta con ellas de manera automática.

Algunos de los sistemas de paquetes más usados son:

[49] KDE es un proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.
[50] El código binario es el sistema de representación de textos, o procesadores de instrucciones de ordenador, utilizando el sistema binario (sistema numérico de dos dígitos, o bit: el "0" y el "1")
[51] La unidad central de procesamiento o CPU (por el acrónimo en inglés de central processing unit), o simplemente el procesador o microprocesador, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos
[52] Un paquete de software es una serie de programas que se distribuyen conjuntamente.
[53] (Portable Network Graphics) es un formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps no sujeto a patentes.

RPM[54], creado por Red Hat y usado por un gran número de distribuciones de Linux, es el formato de paquetes del Linux Standard Base. Originalmente introducido por Red Hat, pero ahora se usa en muchas distribuciones, como por ejemplo Mandriva.

Deb, paquetes Debian, originalmente introducidos por Debian, pero también utilizados por otros como Knoppix y Ubuntu.

.tgz, usado por Slackware, empaqueta el software usando tar[55] y gzip[56]. Pero, además, hay algunas herramientas de más alto nivel para tratar con este formato: slapt-get, slackpkg y swaret[57].

Ebuilds, archivo que contiene información acerca de cómo obtener, compilar e instalar un paquete en el sistema Portage[58] de Gentoo Linux con el comando emerge. Generalmente, estas instalaciones se basan en la compilación de fuentes, aunque algunos paquetes binarios se pueden instalar de esta manera.

Pacman, para Arch Linux usa binarios precompilados distribuidos en un archivo con extensión .pkg.tar.gz ó .pkg.tar.xz (extensiones para archivos comprimidos).

PET, Utilizado por Puppy Linux sus derivados y Quirky su proyecto hermano.

Aunque las distribuciones casi siempre vienen con mucha mayor cantidad de software que los sistemas propietarios, en ocasiones algunos usuarios pueden instalar software que no fue incluido en la distribución. Un ejemplo podría ser el instalar una versión experimental de alguna de las aplicaciones de la distribución o alguna alternativa (como podría ser utilizar una aplicación de KDE dentro de GNOME o viceversa). Si el software es distribuido sólo en forma de código fuente, requerirá ser compilado por el computador. Sin embargo, si el programa es compilado, el paquete no será registrado por el gestor de paquetes y por lo tanto

[54] Package Manager (o RPM, originalmente llamado Red Hat Package Manager, pero se convirtió en acrónimo generalizado) es una herramienta de administración de paquetes pensada básicamente para GNU/Linux
[55] Tar se refiere en Informática a un formato de archivos ampliamente usado en entornos UNIX, identificados con la extensión tar
[56] es una abreviatura de GNU ZIP, un software libre GNU que reemplaza al programa compress de UNIX. gzip fue creado por Jean-loup Gailly y Mark Adler. Apareció el 31 de octubre de 1992 (versión 0.1). La versión 1.0 apareció en febrero de 1993.
[57] sistemas para el manejo de paquetes en la distribución Slackware GNU/Linux.
[58] es el gestor de paquetes oficial de la distribución de Linux Gentoo

no podrá ser controlado por él. Esto significa que el administrador del equipo tendrá que tomar medidas adicionales para mantener el software actualizado. El gestor de paquetes no lo podrá hacer automáticamente.

La mayor parte de las distribuciones instalan los paquetes, incluyendo el núcleo Linux y otras piezas fundamentales del sistema operativo con una configuración preestablecida. Esto hace la instalación más sencilla, especialmente para los usuarios nuevos, pero no es siempre aceptable, pues hay programas que deben de ser cuidadosamente configurados para que sean funcionales, para que operen correctamente con otra aplicación o para que su seguridad sea robusta. En estos casos, los administradores se ven obligados a invertir tiempo reconfigurando y revisando software soportado por la distribución.

En otras distribuciones la instalación puede llegar a ser muy lenta, pues es posible ajustar y configurar la mayor parte o la totalidad del software incluido en la distribución. No todas lo hacen. Algunas ofrecen herramientas de configuración para ayudar en el proceso.

Es también posible armar un sistema a la medida en su totalidad, descartando incluso el uso de una distribución. Lo primero que hay que hacer es generar un sistema base que permita conseguir, compilar, configurar e instalar el código fuente. Generar los binarios de este sistema base requerirá de otra máquina que sea capaz de generar los binarios para el dispositivo deseado, esto puede ser alcanzado por medio de una compilación cruzada.

2.4.4. Tipos y tendencias

En general, las distribuciones Linux pueden ser:

Comerciales o no comerciales.

Ser completamente libres o incluir software privado o comercial.

Diseñadas para uso en el hogar o en las empresas.

Diseñadas para servidores, escritorios o dispositivos móviles.

Orientadas a usuarios regulares o usuarios avanzados.

De uso general o para dispositivos altamente especializados, como un cortafuegos, un enrutador o un cluster computacional.

Diseñadas e incluso certificadas para un hardware o arquitectura específicos.

Orientadas hacia grupos en específico, por ejemplo a través de la internacionalización y localización del lenguaje, o por la inclusión de varios paquetes para la producción musical o para computación científica.

Configuradas especialmente para ser más seguras, completas, portables o fáciles de usar.

Soportadas bajo distintos tipos de hardware.

La diversidad de las distribuciones Linux es debido a cuestiones técnicas, de organización y de puntos de vista diferentes entre usuarios y proveedores. El modo de licenciamiento del software libre permite que cualquier usuario con los conocimientos e interés suficiente pueda adaptar o diseñar una distribución de acuerdo a sus necesidades.

2.4.5. Distribuciones que no requieren instalación (Live CD[59])

Una distribución live o Live CD o Live DVD, más genéricamente Live Distro, (traducido en ocasiones como CD vivo o CD autónomo), es una distribución almacenada en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

Cuando el sistema operativo es ejecutado por un dispositivo de sólo lectura como un CD o DVD, el usuario necesita utilizar una memoria USB o un disco duro instalado en la máquina para conservar su información entre sesiones. La información del sistema operativo es usualmente cargada en la memoria RAM.

[59] Una distribución live o Live CD o Live DVD, más genéricamente Live Distro, (traducido en ocasiones como CD vivo o CD autónomo), es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble

La portabilidad de este tipo de distribuciones las hace ideales para ser utilizadas en demostraciones, operaciones de recuperación, cuando se utiliza una máquina ajena o como medio de instalación para una distribución estándar. Actualmente, casi todas las distribuciones tienen una versión CD/DVD autónomo o "vivo".

2.4.6. Comunidad

La mayoría de las distribuciones están, en mayor o menor medida, desarrolladas y dirigidas por sus comunidades de desarrolladores y usuarios. En algunos casos están dirigidas y financiadas completamente por la comunidad. como ocurre con Debian GNU/Linux, mientras que otras mantienen una distribución comercial y una versión de la comunidad, como hace RedHat con Fedora, o SuSE con OpenSuSE.

En muchas ciudades y regiones, asociaciones locales conocidas como grupos de usuarios promueven este sistema operativo y el software libre. Suelen ofrecer conferencias, talleres o soporte técnico de forma gratuita o introducción a la instalación de Linux para nuevos usuarios.

En las distribuciones y otros proyectos de software libre y código abierto son muy comunes las salas de chat IRC y grupos de noticias. Los foros también son comunes, sobre todo en el soporte a usuarios, y las listas de correo suelen ser el medio principal para discutir sobre el desarrollo, aunque también se utilizan como medio de soporte al usuario.

2.4.7. Escala de desarrollo

Un estudio sobre la distribución Red Hat 7.1 reveló que ésta en particular posee más de 30 millones de líneas de código real. Utilizando el modelo de cálculo de costos COCOMO, puede estimarse que esta distribución requeriría 8.000 programadores por año para su desarrollo. De haber sido desarrollado por

medios convencionales de código cerrado, hubiera costado más de mil millones de dólares en los Estados Unidos.

La mayor parte de su código (71%) pertenecía al lenguaje C, pero fueron utilizados muchos otros lenguajes para su desarrollo, incluyendo C++[60], Bash[61], Lisp[62], Ensamblador, Perl[63], Fortran[64] y Python[65].

Además, la licencia predominante en alrededor de la mitad de su código total (contado en líneas de código) fue la GPL en su versión 2.

El núcleo Linux contenía entonces 2,4 millones de líneas de código, lo que representaba el 8% del total.

En un estudio posterior se realizó el mismo análisis para Debian GNU/Linux versión 2.2. Esta distribución contenía más de 55 millones de líneas de código fuente, y habría costado 1.900 millones de dólares (año 2000) el desarrollo por medios convencionales (no libres); el núcleo Linux en octubre de 2003 tenía unas 5,5 millones de líneas más.

2.4.8. Distribuciones populares

Entre las distribuciones Linux más populares se incluyen:

Arch Linux, una distribución basada en el principio KISS con un sistema de desarrollo continuo entre cada versión (no es necesario volver a instalar todo el sistema para actualizarlo).

CentOS, la versión utilizada en esta investigación, es una distribución creada a partir del mismo código del sistema Red Hat pero mantenida por una comunidad de desarrolladores voluntarios.

[60] C++ es un lenguaje de programación diseñado a mediados de los años 1980 por Bjarne Stroustrup. La intención de su creación fue el extender al exitoso lenguaje de programación C con mecanismos que permitan la manipulación de objetos.
[61] bash es un programa informático cuya función consiste en interpretar órdenes. Está basado en la shell de Unix y es compatible con POSIX
[62] s un dialecto del lenguaje de programación Lisp, publicado en el documento estándar ANSI INCITS 226-1994 (R2004) del ANSI, (antes X3.226-1994 (R1999))
[63] Perl es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.
[64] El Fortran (previamente FORTRAN)1 (del inglés Formula Translating System) es un lenguaje de programación alto nivel de propósito general,2 procedimental3 e imperativo, que está especialmente adaptado al cálculo numérico y a la computación científica
[65] Python es un lenguaje de programación de alto nivel cuya filosofía hace hincapié en una sintaxis muy limpia y que favorezca un código legible.

Debian, una distribución mantenida por una red de desarrolladores voluntarios con un gran compromiso por los principios del software libre.

Fedora, una distribución lanzada por Red Hat para la comunidad.

Gentoo, una distribución orientada a usuarios avanzados, conocida por la similitud en su sistema de paquetes con el FreeBSD Ports, un sistema que automatiza la compilación de aplicaciones desde su código fuente.

gOS, una distribución basada en Ubuntu para netbooks.

Knoppix, la primera distribución live en correr completamente desde un medio extraíble. Está basada en Debian.

Kubuntu, la versión en KDE de Ubuntu.

Linux Mint, una popular distribución derivada de Ubuntu.

Mandriva, mantenida por la compañía francesa del mismo nombre, es un sistema popular en Francia y Brasil. Está basada en Red Hat.

openSUSE, originalmente basada en Slackware es patrocinada actualmente por la compañía Novell.

PCLinuxOS, derivada de Mandriva, paso de ser un pequeño proyecto a una popular distribución con una gran comunidad de desarrolladores.

Puppy Linux,version para pc's antiguas o con pocos recursos que pesa 130 mb.

Red Hat Enterprise Linux, derivada de Fedora, es mantenida y soportada comercialmente por Red Hat.

Slackware, una de las primeras distribuciones Linux y la más antigua en funcionamiento. Fue fundada en 1993 y desde entonces ha sido mantenida activamente por Patrick J. Volkerding.

Slax, es un sistema Linux pequeño, moderno, rápido y portable orientado a la modularidad. Está basado en Slackware.

Ubuntu, una popular distribución para escritorio basada en Debian y mantenida por Canonical.

Dragora y Trisquel GNU/Linux, que van adquiriendo importancia entre las distribuciones que sólo contienen software libre.

Canaima (distribución Linux), es un proyecto socio-tecnológico abierto, construido de forma colaborativa, desarrollado en Venezuela basado en Debian.

El sitio Web DistroWatch ofrece una lista de las distribuciones más populares; la lista está basada principalmente en el número de visitas, por lo que no ofrece resultados muy confiables acerca de la popularidad de las distribuciones.

2.4.9. Distribuciones especializadas

Otras distribuciones se especializan en grupos específicos:

- OpenWrt, diseñada para ser embebida en dispositivos enrutadores.
- Edubuntu, un sistema del proyecto Ubuntu diseñado para entornos educativos.
- MythTV, orientada para equipos multimedia o grabadores de vídeo digital.
- Musix, una distribución de Argentina destinada a los músicos.
- mkLinux, Yellow Dog Linux o Black Lab Linux, orientadas a usuarios de Macintosh y de la plataforma PowerPC.
- 64 Studio, una distribución basada en Debian diseñada para la edición multimedia.
- ABC GNU/Linux, distribución para la construcción de clusters Beowulf desarrollado por Iker Castaños Chavarri, Universidad del País Vasco (España)

3. CONTEXTO

3.1. Descripción del Problema

Resultado del amplio uso de las bases de datos Oracle en el mercado actual es que se visualiza la necesidad de realizar un análisis de riesgos referente al uso de este RDBMS sobre una arquitectura común, en este caso sobre un sistema operativo Linux, arquitectura que nos permitirá emular la gran mayoría de las instalaciones de este RDBMS.

Se deberán ejecutar pruebas de auditoría que permitan identificar los riesgos y controles inherentes a los procesos críticos, además sugerencias y recomendaciones para así certificar la seguridad y continuidad del negocio, según el alcance de este estudio.

3.2. Contexto de la Investigación

La versión de Oracle utilizada para este estudio será la última liberada por el fabricante correspondiente a la Express Edition 10g ya que es la versión libre que provee el fabricante y se ajusta a los propósitos del estudio sin perjuicio en la aplicabilidad de los resultados a otras versiones pagadas. La elección del sistema operativo es Linux Centos 5.3, se seleccionó esta distribución de Linux ya que responde a la versión paralela del fabricante Red Hat Enterprise muy usado a nivel corporativo, pero que conlleva en sus propósitos facilitar los estudios de laboratorio con licencia libre de uso. La arquitectura propuesta será levantada en un laboratorio de pruebas que permitirá el desarrollo de pruebas y su documentación durante el estudio. La metodología usada será COBIT, metodología que nos permitirá trabajar dentro de un marco que actualmente permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los

riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de las tecnologías usadas en las empresas, en el caso específico del estudio al RDBMS de Oracle sobre sistema operativo Linux, análisis que nos permitirá verificar los controles y contramedidas existentes o en su defecto proponerlas como resultados del análisis sobre la arquitectura mencionada.

El aspecto de la informática más relevante en el estudio es referente a la seguridad de la información provista por un conjunto de herramientas que usa la empresa actual, en donde se presume con fundamentos el manejo de datos críticos en la mayoría de los rubros y áreas de servicios, en consecuencia, el análisis tendrá un fuerte enfoque acerca de la seguridad cubierta sobre este tipo de arquitectura tecnológica en donde los procedimientos a seguir serán los establecidos por la metodología COBIT, por qué cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva.

3.3. Beneficiarios

En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

Se garantice el logro de sus objetivos

Tenga suficiente flexibilidad para aprender y adaptarse

Cuente con un manejo juicioso de los riesgos que enfrenta

Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI, y encuentran maneras para:

Alinear la estrategia de TI con la estrategia del negocio

Medir el desempeño de TI

Además, el gobierno y los marcos de trabajo de control están siendo parte de las mejores prácticas de la administración de TI y sirven como facilitadores para establecer el gobierno de TI y cumplir con el constante incremento de requerimientos regulatorios.

Las mejores prácticas de TI se han vuelto significativas debido a un número de factores:

Directores de negocio y consejos directivos que demandan un mayor retorno de la inversión en TI, es decir, que TI genere lo que el negocio necesita para mejorar el valor de los participantes

Preocupación por el creciente nivel de gasto en TI

La necesidad de satisfacer requerimientos regulatorios para controles de TI en áreas como privacidad y reportes financieros (por ejemplo, Sarbanes-Oxley Act, Basilea II) y en sectores específicos como el financiero, farmacéutico y de atención a la salud

La selección de proveedores de servicio y el manejo de Outsourcing y de Adquisición de servicios

Riesgos crecientemente complejos de la TI como la seguridad de base de datos

Iniciativas de gobierno de TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de TI, aumentar el valor del negocio y reducir los riesgos de éste

La madurez creciente y la consecuente aceptación de marcos de trabajo respetados tales como COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2

La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia (Benchmarking)

Los antecedentes bibliográficos utilizados serán los manuales de instalación técnicos provistos por los fabricantes (Oracle y Centos) y los marcos de trabajo provistos por el IT Governance Institute.

3.4. Dominios de COBIT

COBIT define las actividades de TI en un modelo genérico de buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Se entiende por dominio a la agrupación natural de procesos que normalmente corresponden a una responsabilidad organizacional. Por proceso al conjunto de actividades con un objetivo de control. Por actividades a las acciones requeridas para lograr un resultado que se pueda medir.

Estos dominios son:

- Planear y Organizar, dominio que proporciona dirección para la entrega de soluciones y la entrega de servicio.
- Adquirir e Implementar, que proporciona las soluciones y las pasa para convertirlas en servicios.
- Entregar y Dar Soporte que recibe las soluciones y las hace utilizables por los usuarios finales, y por último
- Monitorear y Evaluar, hace seguimiento a los procesos para asegurar que cumplen con lo dispuesto.

Los procesos de COBIT bajo sus respectivos dominios se demuestran en el siguiente cuadro:

PROCESOS	
PLANEAR Y ORGANIZAR	**ENTREGAR Y DAR SOPORTE**
PO1 Definir un Plan Estratégico de TI	DS1 Definir y administrar los niveles de servicio
PO2 Definir la Arquitectura de la Información	DS2 Administrar los servicios de terceros
PO3 Determinar la Dirección Tecnológica	DS3 Administrar el desempeño y la capacidad
PO4 Definir los Procesos, Organización y Relaciones de TI	DS4 Garantizar la continuidad del servicio
PO5 Administrar la Inversión en TI	DS5 Garantizar la seguridad de los sistemas
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	DS6 Identificar y asignar costos
PO7 Administrar Recursos Humanos de TI	DS7 Educar y entrenar a los usuarios
PO8 Administrar la Calidad	DS8 Administrar la mesa de servicio y los

	incidentes
PO9 Evaluar y Administrar los Riesgos de TI	DS9 Administrar la configuración
PO10 Administrar Proyectos	DS10 Administrar los problemas
ADQUIRIR E IMPLEMENTAR	DS11 Administrar los datos
AI1 Identificar soluciones automatizadas	DS12 Administrar el ambiente físico
AI2 Adquirir y mantener software aplicativo	DS13 Administrar las operaciones
AI3 Adquirir y mantener infraestructura tecnológica	**MONITOREAR Y EVALUAR**
AI4 Facilitar la operación y el uso	ME1 Monitorear y Evaluar el Desempeño de TI
AI5 Adquirir recursos de TI	ME2 Monitorear y Evaluar el Control Interno
AI6 Administrar cambios	ME3 Garantizar el Cumplimiento Regulatorio
AI7 Instalar y acreditar soluciones y cambios	ME4 Proporcionar Gobierno de TI

4. DESARROLLO

El desarrollo de esta investigación es efectuar un análisis de riesgos a dos versiones del RDBM (Oracle) sobre el sistema operativo Linux Centos 5.5, efectuado con las herramientas en referencia.

4.1. Marco Metodológico

Se utilizará el marco metodológico COBIT en su versión 4.1 y los procesos que se adhieran a las actividades mínimas de seguridad definidas para evaluar esta misma en un ambiente de prueba que emule una arquitectura habitualmente utilizada por las empresas.

4.2. Definición del requerimiento

Ejecutar un análisis de riesgos, para así, identificar las debilidades y vulnerabilidades al sistema operativo y base en un ambiente de prueba, con herramientas especializadas, con el objetivo de identificar e informar las brechas de seguridad y recomendar la mitigación de los riesgos detectados. Lo anterior utilizando el estándar internacional COBIT.

4.3. Marco de trabajo según COBIT

Si bien, es una metodología que abarca todas las áreas de las TI, según su marco completo, este estudio fue enfocado en los requerimientos de negocio relacionado a la seguridad, de una arquitectura de prueba especifica, es por esto que, de los 4 dominios y los 34 procesos que abarca esta metodología, se revisó su adhesión al estándar las que tuviesen relación con las actividades mínimas de revisión de seguridad. Estas son;

- Identificación de riesgos
- Descripción de arquitectura
- Descubrimiento de accesos lógicos
- Análisis de Vulnerabilidades
- Test de control de acceso, E

o Identificación de controles

De los 34 procesos de COBIT se utilizaron los procesos que se adherían a las actividades definidas, generando así el marco de trabajo definido en el siguiente cuadro:

ACTIVIDADES / PROCESOS	Identificación de riesgos	Descripción de arquitectura	Descubrimiento de accesos lógicos	Análisis de vulnerabilidades	Test de control de accesos	Identificación controles
PLANEAR Y ORGANIZAR						
PO1 Definir un Plan Estratégico de TI	X	X				
PO2 Definir la Arquitectura de la Información		X				
PO9 Evaluar y Administrar los Riesgos de TI	X		X	X		X
ADQUIRIR E IMPLEMENTAR						
AI2 Adquirir y mantener software aplicativo		X		X	X	
AI3 Adquirir y mantener infraestructura tecnológica		X				
AI5 Adquirir recursos de TI		X				
ENTREGAR Y DAR SOPORTE						
DS2 Administrar los servicios de terceros	X	X				
DS4 Garantizar la continuidad del servicio	X			X		X
DS5 Garantizar la seguridad de los sistemas			X	X	X	X
DS7 Educar y entrenar a los usuarios						X
MONITOREAR Y EVALUAR						
ME1 Monitorear y Evaluar el Desempeño de TI						X
ME2 Monitorear y Evaluar el Control Interno	X					X
ME3 Garantizar el Cumplimiento Regulatorio	X					X
ME4 Proporcionar Gobierno de TI	X					X

4.4. Análisis de Riesgos

Se establece un programa de trabajo que consta de pruebas de auditoría, sus hallazgos y recomendaciones, que permitan identificar los riesgos y controles inherentes al proceso críticos, según el alcance, para a así certificar la seguridad y continuidad del negocio, por otra parte, manejar el apetito de riesgo de los StakeHolders. El resultado de el trabajo otorga una conclusión (resumen ejecutivo), y dos reportes del análisis de riesgos, que en su conjunto otorgan la visión del antes y después (plataforma securitizada) de la instalación de la arquitectura, también un mapa de riesgos inherentes al alcance de el trabajo.

4.5. Composición de Riesgos

La gestión del desempeño de las TI apunta a identificar y cuantificar sus costos y beneficios, es por esto que se establece un análisis de riesgos, según el alcance de esta revisión, existen diferentes instrumentos de diseño de análisis disponibles dependiendo de las características de los costos y beneficios de la empresa. Utilizaremos una tabla que identifique;

Amenaza + Vulnerabilidad = Riesgo

Para nuestra plataforma identificamos las amenazas y vulnerabilidades posibles que expongan a distintos riesgos a nuestra plataforma y su alcance.

AMENAZAS	VULNERABILIDADES
Ataque /Hacking	Puertos abiertos o no filtrados.
Denegación de servicios	Falta de parches de Sistema Operativo
Adulteración, extracción o borrado de	Falta de parches del SGBDR

datos sin autorización.	
Exposición de confidencialidad de datos	Servicios en sistema operativo no necesarios para el objetivo del sistema
Caída del Sistema	Falta de monitoreo
Existencia o creación de claves débiles	Falta o incumplimiento de procedimientos de seguridad

Definimos los posibles riesgos:

RIESGOS	APLICA
Que un atacante explote vía fuerza bruta un puerto abierto o no filtrado, desde la red interna	√
Que un atacante explote y/o acceda al sistema por falta de parches de Sistema Operativo	√
Que un atacante explote y/o acceda al sistema por falta de parches del SGBDR.	√
Que un atacante explote y/o acceda al sistema por la existencia de servicios en sistema operativo no necesarios	√
Que un atacante explote y/o acceda al sistema por falta de monitoreo	√
Que un atacante explote y/o acceda al sistema por falta o incumplimiento de procedimientos de seguridad	√
Denegación de servicios a través de puertos abiertos o no filtrados.	√
Denegación de servicios por falta de parches de Sistema Operativo	√
Denegación de servicios por falta de parches del SGBDR	√

Denegación de servicios por servicios en sistema operativo no necesarios para el objetivo del sistema	√
Acción tardía a una denegación de servicios por falta de monitoreo	√
Denegación de servicios por falta o incumplimiento de procedimientos de seguridad	√
Adulteración, extracción o borrado de datos sin autorización, a través de puertos abiertos o no filtrados.	√
Adulteración, extracción o borrado de datos sin autorización, por falta de parches de Sistema Operativo	√
Adulteración, extracción o borrado de datos sin autorización, por falta de parches del SGBDR	√
Adulteración, extracción o borrado de datos sin autorización, a través de servicios en sistema operativo no necesarios para el objetivo del sistema	√
Adulteración, extracción o borrado de datos sin autorización por falta de monitoreo	√
Adulteración, extracción o borrado de datos sin autorización por falta o incumplimiento de procedimientos de seguridad	√
Exposición de confidencialidad de datos a través de puertos abiertos o no filtrados.	√
Exposición de confidencialidad de datos por falta de parches de Sistema Operativo	√
Exposición de confidencialidad de datos por falta de parches del SGBDR	√
Exposición de confidencialidad de datos, a través de servicios en sistema operativo no necesarios para el objetivo del sistema	√
Exposición de confidencialidad de datos por falta de monitoreo	√

Exposición de confidencialidad de datos por falta o incumplimiento de procedimientos de seguridad	√
Caída del Sistema a través de puertos abiertos o no filtrados.	√
Caída del Sistema por falta de parches de Sistema Operativo	√
Caída del Sistema por falta de parches del SGBDR	√
Caída del Sistema, a través de servicios en sistema operativo no necesarios para el objetivo del sistema	√
Caída del Sistema por falta de monitoreo	√
Caída del Sistema por falta o incumplimiento de procedimientos de seguridad	√
Existencia o creación de claves débiles a través de puertos abiertos o no filtrados.	√
Existencia o creación de claves débiles por falta de parches de Sistema Operativo	**N/A**
Existencia o creación de claves débiles por falta de parches del SGBDR	**N/A**
Existencia o creación de claves débiles, a través de servicios en sistema operativo no necesarios para el objetivo del sistema	√
Existencia o creación de claves débiles por falta de monitoreo	√
Existencia o creación de claves débiles por falta o incumplimiento de procedimientos de seguridad	√

4.6. Descripción de la Arquitectura

Esta actividad consistió en definir la arquitectura del ambiente de prueba. Esta se basó en el uso de un motor de base de datos ampliamente utilizado por las organizaciones, ORACLE. Este es un sistema de gestión de base de datos que, se considera como uno de los sistemas de bases de datos más completos

destacándose por su gran robustez y su dominio en el mercado de servidores empresariales ha sido contundente hasta hace poco.

El sistema operativo elegido fue el denominado Linux, por su creciente utilización en la industria de las TI, este es un sistema operativo que incluye determinadas aplicaciones para satisfacer las necesidades de un grupo específico de usuarios, como por ejemplo empresas que requieren un sistema operativo mas versátil a los requerimiento de desempeño y respuesta de acuerdo a las exigencias del negocio.

Existen distribuciones que están soportadas comercialmente y otras de código libre. La distribución de Linux utilizada durante este estudio fue la denominada CENTOS, de licencia libre.

4.6.1. Acerca de las Máquinas Virtuales[66] (VM)

Una máquina virtual es como un computador separado, con sistema operativo independiente que corre en un computador físico con sistema independiente.

4.6.2. Creación de VM para el trabajo

Se creó una VM con el siguiente detalle:

Se asignaron 950 GB (gigabytes) de espacio en disco duro.

Se asignaron 512Kb (kilobytes) en memoria RAM para la VM.

Se asignó una partición de inicio de sistema operativo de 500MB (megabytes) de espacio en disco duro.

Se asignaron 10240MB de espacio en disco duro para la memoria virtual (Swap) .

Se asignó el resto del disco duro a la raíz del sistema operativo (/)

Se instaló la versión de Oracle; según esta investigación, el motor instalado fue instalación por defecto con todas sus funcionalidades.

[66] En informática una máquina virtual es un software que emula a una computadora y puede ejecutar programas como si fuese una computadora real.

4.7. Prueba I: Descubrimiento de accesos lógicos

Con la herramienta de descubrimiento de puertos NMAP[67] en su versión 5.21, se identificaron 7 puertos abiertos de 65535, sin ningún tipo de filtro o bloqueo. Puertos abiertos, sin filtrar, es un riesgo inherente de ataque a la arquitectura en revisión, más detalles en Anexo I

4.8. Prueba II: Análisis de vulnerabilidades

Tras realizar un escaneo de vulnerabilidades a la plataforma en cuestión con la herramienta NESSUS[68] con el resultado descrito en el Anexo II, se identificó que existen 13 puertos abiertos tras la instalación del sistema operativo por defecto, además de puertos abiertos se identificaron vulnerabilidades del tipo de falta de parches del sistema operativo, lo que conlleva a los riesgos de seguridad inherente a acciones maliciosas por parte de un atacante.

4.9. Prueba III: Test de Control de Accesos

Con los resultados anteriores se ejecutaron tests de penetración al motor de BD, detallados en el Anexo III. Test que nos permitió obtener claves débiles de la instalación del motor, además de claves por defecto que se presentaban expiradas y bloqueadas.

[67] Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon
[68] Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.

5. CONCLUSIÓN

Según el alcance y la hipótesis del trabajo, concluimos que de los riesgos analizados y las actividades realizadas para esta tesis, podemos decir que existe una falta de implementación de controles de seguridad, según el ambiente de prueba utilizado, tras su instalación inicial o por defecto.

Conclusión que se obtuvo como resultado de la utilización del estándar de COBIT, aplicando algunos de los procesos del estándar v/s actividades mínimas de seguridad.

De los riesgos analizados para el alcance de esta revisión podemos mencionar 6 controles que eventualmente mitigarían los riesgos descritos en el punto 4.5, estos son:

5.1. Cerrar puertos en desuso y filtrar los utilizados

Cerrar los puertos no utilizados en cualquier sistema, más que una buena práctica es mandatario, ya que, se esta dejando una puerta abierta sin necesidad de una utilidad para el fin del sistema en cuestión.

5.2. Crear un procedimiento de parchado de Sistema Operativo y monitorear su cumplimiento

La vertiginosa expansión de las TI, también crece en cuanto a vulnerabilidades, sin ir mas allá, los hallazgos que más se reiteran en esta revisión son por falta de parches de seguridad. Diseñar, implementar y monitorear cumplimiento de parches de las vulnerabilidades de sistemas operativos se traduce en una necesidad crítica, dado que en estos sistemas residen aplicaciones y bases de datos críticas para el negocio que debemos proteger.

5.3. Crear un procedimiento de parchado del SGBDR y monitorear su cumplimiento

Como mencionamos anteriormente, con la misma celeridad crecen las vulnerabilidades de los SGBDR, ya que, de alguna u otra forma el dato sería el premio del atacante, también reiteramos que los hallazgos en esta revisión son por

falta de parches de seguridad. Diseñar, implementar y monitorear cumplimiento de parches de las vulnerabilidades de los SGBDR se traduce en una necesidad crítica, dado que en estas instancias residen los datos que en su conjunto son la información crítica para el negocio que debemos proteger.

5.4. Eliminar o deshabilitar servicios en el Sistema Operativo no utilizados

Eliminar los servicios no utilizados en cualquier sistema, más que una buena práctica es mandatario, ya que, se están dejando puertas abiertas sin necesidad de una utilidad para el fin del sistema en cuestión, que por otra parte afectan al performance y disponibilidad de los sistemas.

5.5. Implementar procedimientos de monitoreo detectivos inherente a ataques a lo sistemas en cuestión

Los ataques por denegación de servicios son de los más comunes hoy en la industria TI. Diseñar, implementar y monitorear cumplimiento de procedimientos de monitoreo se traduce en una necesidad crítica, dado que en estos sistemas residen aplicaciones y bases de datos críticas para el negocio que debemos proteger.

5.6. Implementar procedimientos preventivos de seguridad inherente a ataques a lo sistemas en cuestión.

Los ataques a los sistemas corporativos son el blanco más preciado por los atacantes contemporáneos. Diseñar, implementar y monitorear cumplimiento de procedimientos de seguridad, sin perjuicio de los anteriores, son unos de los más importantes, ya que, uno de los cimientos principales de una arquitectura tecnológica son las buenas prácticas y buena base de seguridad de sistemas, aplicaciones y bases de datos.

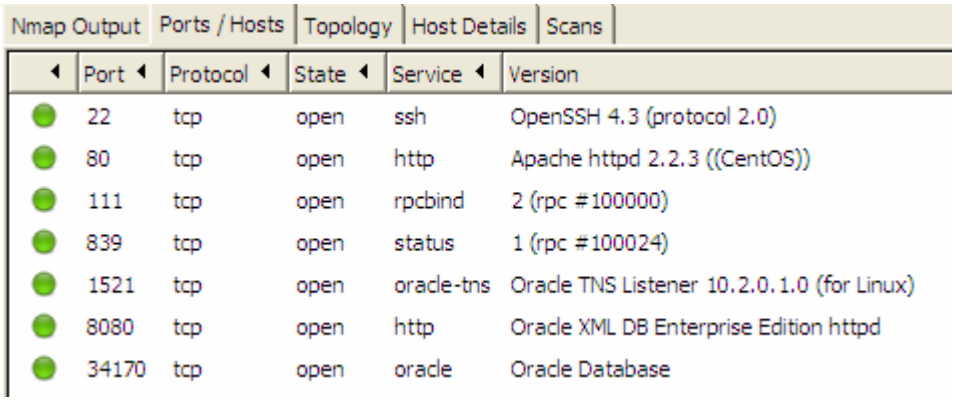
Finalmente, mencionar que se cumple la hipótesis y los objetivos trazados para el trabajo, que se estableció en; utilizar un marco de trabajo aceptado por la industria de

las TI (COBIT), para la realización de un análisis de riesgos, que como resultado nos permitiese identificar las vulnerabilidades existentes en un arquitectura usualmente utilizada en la industria de las tecnologías en la actualidad, y así poder proponer los controles necesarios para mitigar estos riesgos.

6. ANEXO I

Describe el procedimiento técnico utilizado durante la revisión de actividades de seguridad efectuados durante el trabajo.

Para la prueba definida como descubrimiento de accesos lógicos, que utilizó la herramienta NMAP, el comando utilizado fue: nmap -p 1-65535 -T4 -A -v -PE -PS22, 25,80 -PA21, 23, 80,3389 192.168.186.129. Este último arrojó la siguiente información técnica para su análisis.



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
80	tcp	open	http	Apache httpd 2.2.3 ((CentOS))
111	tcp	open	rpcbind	2 (rpc #100000)
839	tcp	open	status	1 (rpc #100024)
1521	tcp	open	oracle-tns	Oracle TNS Listener 10.2.0.1.0 (for Linux)
8080	tcp	open	http	Oracle XML DB Enterprise Edition httpd
34170	tcp	open	oracle	Oracle Database

Starting Nmap 5.21 (http://nmap.org) at 2010-09-14 22:56 Hora est. del Pacífico SA
NSE: Loaded 36 scripts for scanning.
Initiating ARP Ping Scan at 22:56
Scanning 192.168.186.129 [1 port]
Completed ARP Ping Scan at 22:56, 0.88s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:56
Completed Parallel DNS resolution of 1 host. at 22:57, 13.00s elapsed
Initiating SYN Stealth Scan at 22:57
Scanning 192.168.186.129 [65535 ports]
Discovered open port 8080/tcp on 192.168.186.129
Discovered open port 22/tcp on 192.168.186.12
Discovered open port 111/tcp on 192.168.186.129
Discovered open port 80/tcp on 192.168.186.129

```
Discovered open port 34170/tcp on 192.168.186.129
Discovered open port 1521/tcp on 192.168.186.129
Discovered open port 839/tcp on 192.168.186.129
Completed SYN Stealth Scan at 23:14, 1033.48s elapsed (65535 total ports)
Initiating Service scan at 23:14
Scanning 7 services on 192.168.186.129
Completed Service scan at 23:14, 29.33s elapsed (7 services on 1 host)
Initiating RPCGrind Scan against 192.168.186.129 at 23:14
Completed RPCGrind Scan against 192.168.186.129 at 23:14, 1.00s elapsed
(2 ports)
Initiating OS detection (try #1) against 192.168.186.129
NSE: Script scanning 192.168.186.129.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:14
Completed NSE at 23:14, 2.09s elapsed
NSE: Script Scanning completed.
Nmap scan report for 192.168.186.129
Host is up (0.040s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 d3:e8:fb:c0:17:f8:3f:80:19:cd:37:3e:c2:df:01:e4 (DSA)
|_2048 15:5f:11:61:5c:0a:7f:e6:8f:d5:df:8d:93:76:a2:f3 (RSA)
80/tcp    open  http       Apache httpd 2.2.3 ((CentOS))
|_html-title: Apache HTTP Server Test Page powered by CentOS
111/tcp   open  rpcbind    2 (rpc #100000)
| rpcinfo:
| 100000  2    111/udp  rpcbind
| 100024  1    836/udp  status
| 100000  2    111/tcp  rpcbind
```

```
|_100024  1    839/tcp  status
839/tcp   open  status     1 (rpc #100024)
1521/tcp  open  oracle-tns Oracle TNS Listener 10.2.0.1.0 (for Linux)
8080/tcp  open  http       Oracle XML DB Enterprise Edition httpd
|_html-title: ORACLE DATABASE 10g EXPRESS EDITION LICENSE
AGREEMENT Letter-S...
34170/tcp open  oracle     Oracle Database
MAC Address: 00:0C:29:69:9A:8D (VMware)
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.24
Uptime guess: 0.097 days (since Tue Sep 14 20:55:19 2010)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203
IP ID Sequence Generation: All zeros
HOP RTT      ADDRESS
1   40.11 ms 192.168.186.129
Nmap done: 1 IP address (1 host up) scanned in 1095.55 seconds
         Raw packets sent: 67650 (2.977MB) | Rcvd: 66467 (2.659MB)
```

7. ANEXO II

Con la herramienta *Checkpwd* (se utiliza para descubrir claves débiles) se verificaron claves triviales y por defecto, con los siguientes resultados técnicos:

Revisión de claves débiles

```
Checkpwd 1.23 [Win] - (c) 2005-2007 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com
initializing Oracle client library
connecting to the database
retrieving users and password hash values
disconnecting from the database
opening weak password list file
reading weak passwords list
checking passwords
Starting 2 threads
SYS has weak password PASSWORD123 [OPEN]
SYSTEM has weak password PASSWORD123 [OPEN]
MDSYS has weak password MDSYS [EXPIRED & LOCKED]
DIP has weak password DIP [EXPIRED & LOCKED]
FLOWS_FILES has weak password ORACLE [EXPIRED & LOCKED]
DBSNMP has weak password DBSNMP [EXPIRED & LOCKED]
XDB has weak password ORACLE [EXPIRED & LOCKED]
ANONYMOUS       OK [OPEN]
OUTLN has weak password OUTLN [EXPIRED & LOCKED]
TSMSYS has weak password TSMSYS [EXPIRED & LOCKED]
CTXSYS has weak password ORACLE [EXPIRED & LOCKED]
FLOWS_020100 has weak password ORACLE [EXPIRED & LOCKED]
```

```
HR has weak password HR [EXPIRED & LOCKED]

Summary:
  Passwords checked          : 1547213
  Weak passwords found       : 12
  Elapsed time (min:sec)     : 0:34
  Passwords / second         : 45506.3
```

Revisión de claves por defecto

```
Checkpwd 1.23 [Win] - (c) 2005-2007 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Security Trainings
http://www.red-database-security.com
initializing Oracle client library
connecting to the database
retrieving users and password hash values
disconnecting from the database
opening weak password list file
reading weak passwords list
checking passwords
Starting 2 threads
SYSTEM  OK [OPEN]
SYS     OK [OPEN]
MDSYS has weak password MDSYS [EXPIRED & LOCKED]
DIP has weak password DIP [EXPIRED & LOCKED]
ANONYMOUS       OK [OPEN]
FLOWS_FILES has weak password ORACLE [EXPIRED & LOCKED]
OUTLN has weak password OUTLN [EXPIRED & LOCKED]
DBSNMP has weak password DBSNMP [EXPIRED & LOCKED]
TSMSYS has weak password TSMSYS [EXPIRED & LOCKED]
```

```
XDB has weak password ORACLE [EXPIRED & LOCKED]
CTXSYS has weak password ORACLE [EXPIRED & LOCKED]
FLOWS_020100 has weak password ORACLE [EXPIRED & LOCKED]
HR has weak password HR [EXPIRED & LOCKED]

Summary:
  Passwords checked          : 3997
  Weak passwords found       : 10
  Elapsed time (min:sec)     : 0:01
  Passwords / second         : 3997
```

8. ANEXO III

Se efectuó, con la herramienta Nessus, un escaneo de vulnerabilidades que arrojó los siguientes resultados técnicos para su análisis:

N°	PUERTO / SERVICIO	DESCRIPCIÓN
1	http-alt (8080/tcp)	Puerto abierto y sin filtrar
2	ssh (22/tcp)	Servidor SSH con puerto abierto y sin filtrar
3	sunrpc (111/tcp)	Servidor SUNRCP con puerto abierto y sin filtrar
4	vacdsm-app (671/tcp)	Servicio vacdsm-app con puerto abierto y sin filtrar
5	unknown (45089/tcp)	Puerto abierto y sin filtrar
6	ncube-lm (1521/tcp)	Puerto del servicio ORACLE abierto y sin filtrar
7	vacdsm-app (671/tcp)	Un servicio de ONC RPC que se ejecuta en el host. Descripción remota: Al enviar una solicitud DUMP para el mapeador, fue posible enumerar los servicios de ONC RPC que se ejecutan en el puerto remoto. Usando esta información, es posible conectarse a cada servicio enviando una solicitud RPC al puerto.
8	sunrpc (111/tcp)	Un servicio de ONC RPC que se ejecuta en el host. Descripción: Al enviar una solicitud DUMP para el mapeador de puertos, fue posible enumerara los servicios de ONC RPC que se ejecutan en el puerto remoto. Usando esta información, es posible conectarse a cada servicio usando una solicitud RPC al puerto.
9	mecomm (668/udp)	Un servicio de ONC RPC que se ejecuta en el host. Descripción: Al enviar una solicitud DUMP para el mapeador de puertos, fue posible enumerara los servicios de ONC RPC que se ejecutan en el puerto remoto. Usando esta información, es posible conectarse a cada servicio usando una solicitud RPC al puerto.
10	general/udp	Fue posible obtener información .Descripción de la traza: Hace una traza de ruta al host.
11		Traza: 192.168.0.163 a.168.0 .250
12	sunrpc (111/udp)	Un asignador de puertos RPC ONC se ejecuta en el host. Descripción: El portmapper RPC se ejecuta en este puerto. El asignador de puertos permite a alguien para obtener el número de puerto de cada RPCservice se ejecuta en la máquina remota mediante el envío de cualquiera consulta múltiple.
13	mdns (5353/udp)	Es posible obtener información sobre el host. Description: El servicio remoto entiende el Bonjour (también conocido como ZeroConf ormDNS) protocolo, que permite que cualquiera pueda descubrir información remotamente como el tipo de sistema operativo y la versión exacta, , y que lista de servicios está corriendo en el servidor.
14	general/icmp	Es posible determinar el momento exacto en el host .Descriptio: El host remoto responde a una solicitud de marca de tiempo ICMP. Esto permite a un atacante saber la fecha que figura en su máquina. Esto puede ayudarle a derrotar a todos su autenticación de protocolos.
15	general/tcp	El servicio remoto implementa timestamps. Description TCP: El host remoto implementa marcas TCP de tiempo, según se define en RFC1323. Aparte del efecto de esta característica es que el tiempo de funcionamiento de la máquina .
16	ssh (22/tcp)	Un servidor SSH está corriendo en este puerto
17	ncube-lm (1521/tcp)	Un servicio tnslsnr Oracle está escuchando en este puerto. Description: El sistema remoto se ejecuta en el servicio tnslsnr Oracle
18	ncube-lm (1521/tcp)	Es posible identificar las bases de datos sobre el host. Descriptio: El control remoto del servidor de base de datos Oracle de ellas contiene una o más bases de datos que el istema conoce como SID o soporta el comando 'servicios' como un medio de inclusión de los DIM disponible en el sistema afectado. Un SID de Oracle sirve para identificar de forma única una base de datos en particular.

19	ssh (22/tcp)	Un servidor SSH está escuchando en este puerto. Description: Es posible obtener información sobre el control remoto mediante el envío de un requerimiento SSH server.
20	general/tcp	Se pudo acceder a la máquina remota usando la clave suministrada vía el comando "uname-a" es: Linux LAB-TESIS-01-2.6.18
21	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: El control remoto del sistema CentOS es que falta una actualización de seguridad que ha sido documentado en Red Hat como RHSA-2010-0490.
22	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0675.
23	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: El control remoto del sistema CentOS es que falta una actualización de seguridad que ha sido documentado en Red Hat como RHSA-2010-0398.
24	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: El control remoto del sistema CentOS es que falta una actualización de seguridad que ha sido documentado en Red Hat como RHSA-2010-0458.
25	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: El control remoto del sistema CentOS es que falta una actualización de seguridad que ha sido documentado en Red Hat como RHSA-2010-0382.
26	general/tcp	Es posible enumerar el software instalado en la máquina remota, via SSH. Description: Este plugin muestra los programas instalados en la máquina remota mediante comandos apropiados (rpm-qa en distribuciones Linux basadas en RPM, qpkg, dpkg, etc.)
27	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0166.
28	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0361.
29	general/tcp	El fabricante puede deducir de la Ethernet Cada dirección MAC comienza con una vista organizativo 24-bits "identificador único". OUI Estos son registradas por IEEE. Los siguientes fabricantes de tarjetas fueron identificadas: 00:26:5 e: 84: ea: a2: como Hon Hai Precisión Ind. Co., Ltd.
30	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0429.
31	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0528.
32	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0534.
33	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0501.
34	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0578.
35	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0616.
36	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0547.

37	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0533.
38	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0681.
39	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0580.
40	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0459.
41	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0488.
42	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0697.
43	general/tcp	Este plugin enumera las interfaces IPv4 en un host. Description: Mediante la conexión al host remoto a través de SSH con la credenciales otorgadas, este plugin enumera las interfaces de red configurados con direcciones.
44	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0347.
45	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0585.
46	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0542.
47 48	general/tcp	Este plugin enumera las direcciones MAC en un host. Description: Mediante la conexión al host remoto a través de SSH con la credenciales otorgadas, este plugin enumera la dirección física.
49	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0556.
50	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0610.
51	unknown (45089/tcp)	El proceso Linux '/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle' está escuchando en este puerto
52	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0423.
53	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0164.
54	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0165.
55	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0475.

56	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0607.
57	general/tcp	El sistema operativo alberga un Kernel Linux en su versión 2.6.18-194.el5 sobre la liberación de CentOS 5.5 (Final)
58	sunrpc (111/tcp)	El proceso Linux '/sbin/portmap' está escuchando en este puerto
59	http-alt (8080/tcp)	El procesos Linux '/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/tnslsnr' está escuchando en este puerto
60	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0504.
61	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0679.
62	ncube-lm (1521/tcp)	El proceso Linux '/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/tnslsnr' está escuchando en este puerto.
63	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0339.
64	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0140.
65	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0343.
66	general/tcp	El host remoto se encuentra desactualizado. Description de seguridad: Al control remoto del sistema CentOS le falta una actualización de seguridad que ha sido documentado en Red Hat asesoramiento RHSA-2010-0519.
67	general/tcp	Este plugin enumera las interfaces IPv6 en un host. Descriptio: Mediante la conexión al host remoto vía SSH con la credenciales otorgadas, este plugin enumeranlas interfaces de red configurados con direcciones IPv6
68	ssh (22/tcp)	El proceso Linux '/usr/sbin/sshd' está escuchando en este puerto.
69	vacdsm-app (671/tcp)	El proceso Linux '/sbin/rpc.statd' está escuchando en este puerto.
70	sun-dr (665/udp)	El proceso Linux '/sbin/rpc.statd' está escuchando en este puerto.
71	mecomm (668/udp)	El proceso Linux '/sbin/rpc.statd' está escuchando en este puerto.
72	unknown (48548/udp)	El proceso Linux '/usr/sbin/avahi-daemon' está escuchando en este puerto.
73	mdns (5353/udp)	El proceso Linux '/usr/sbin/avahi-daemon' está escuchando en este puerto.
74	ipp (631/udp)	El proceso Linux '/usr/sbin/cupsd' está escuchando en este puerto.
75	sunrpc (111/udp)	El proceso Linux '/sbin/portmap' está escuchando en este puerto.
76	unknown (37692/udp)	El proceso Linux '/usr/sbin/avahi-daemon' está escuchando en este puerto.

9. GLOSARIO

Sistema: Un sistema (del latín systema, proveniente del griego σύστημα) es un conjunto de funciones, virtualmente referenciada sobre ejes, bien sean estos reales o abstractos.

Aplicación: En informática, una aplicación es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo.

Fichero: Dado que una unidad de disco, o de hecho cualquier memoria sólo puede almacenar bits, la computadora debe tener alguna manera de convertir la información a ceros y unos y viceversa. Hay diferentes tipos de formatos para diferentes tipos de información. Sin embargo, dentro de cada tipo de formato, por ejemplo documentos de un procesador de texto, habrá normalmentie varios formatos diferentes, a veces en competencia.

Repositorio: Un repositorio, depósito o archivo es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

Oracle: Oracle es un sistema de gestión de base de datos relacional (o RDBMS por el acrónimo en inglés de Relational Data Base Management System), desarrollado por Oracle Corporation.

Linux: GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux

Centos: (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Distribución: En informática, distribución un conjunto de aplicaciones reunidas

StakeHolders: es un término inglés utilizado por primera vez por R. E. Freeman en su obra: “Strategic Management: A Stakeholder Approach”, (Pitman, 1984) para referirse a «quienes pueden afectar o son afectados por las actividades de una empresa».

COBIT: Objetivos de Control para la información y Tecnologías relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

Tecnologías de la Información: según lo definido por la asociación de la tecnología de información de América (ITAA) es “el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras

Outsourcing: La subcontratación (más conocido por "outsourcing", el término en inglés) es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato

Benchmarking: es una técnica utilizada para medir el rendimiento de un sistema o componente del mismo, frecuentemente en comparación con el que se refiere específicamente a la acción de ejecutar un benchmark

ITGI: IT Governance Institute

Sarbanes-Oxley: La Ley Sarbanes Oxley, cuyo título oficial en inglés es Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002), es una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. También es llamada SOx, SarbOx o SOA.

ITIL: La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI)

COSO: Committee of Sponsoring Organizations of the Treadway Commission

ISO 20000: Service Management normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) el 14 de diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información)

ISO 9000: designa un conjunto de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional para la Estandarización (ISO). Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios

ISO 25999: Business Continuity Management. Code of Practice

ISO 27001: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar)

PRINCE2: PRojects IN Controlled Environments (PRINCE), en español: proyectos en entornos controlados, es un método de gestión de proyectos que cubre la administración, control y organización de un proyecto. PRINCE2 es una marca registrada de la OGC del Reino Unido.

TOGAF: The Open Group Architecture Framework (TOGAF) (o Esquema de Arquitectura de Open Group, en español) es un esquema (o marco de trabajo) de Arquitectura Empresarial que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial de información

BASILEA II: es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea.

RACI: Matriz de Asignación de Responsabilidades (Responsable, Accountable, Consulted, Informed).

ISO-7498-2: Sistemas de tratamiento de Información - Interconexión de Sistemas Abierta - Modelo de Referencia Básico - la Parte 2: Arquitectura de Seguridad. Provee una descripción general de servicios de seguridad y mecanismos relacionados, que pueden ser asegurado por el modelo de referencia, y de los puestos dentro del modelo de referencia donde los servicios y los mecanismos pueden ser suministrados. Extiende el campo de la aplicación de 7498 de la ISO cubrir las comunicaciones seguras entre sistemas abiertos. Añade a los conceptos y los principios incluido en 7498 de la ISO pero no modificar ellos. No es ninguna especificación de puesta en práctica, nor una base para tasar la conformidad de las puestas en práctica verdaderas.

X.509: En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas

UIT-T: El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT)

Malware: (del inglés malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario

SPAM: Se llama spam, correo basura o sms basura a los mensajes no solicitados, no deseados o de remitente desconocido

Botnet: es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática.

Phishing: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta

XML siglas en inglés de eXtensible Markup Language (lenguaje de marcas extensible), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C)

SOA: Arquitectura Orientada a Servicios (en inglés Service Oriented Architecture)

Virus: un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario

Troyano: se denomina troyano o caballo de Troya (traducción literal del inglés Trojan horse) a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños

Spyware: Un programa espía, traducción del inglés spyware, es un programa, dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste

BBS: Bulletin Board System o BBS (Sistema de Tablón de Anuncios)

EGA: es el acrónimo inglés de Enhanced Graphics Adapter, la especificación estándar de IBM PC para visualización de gráficos

Oracle Corporation: es una de las mayores compañías de software del mundo. Sus productos van desde bases de datos (Oracle) hasta sistemas de gestión

GNU: El proyecto GNU fue iniciado por Richard Stallman con el objetivo de crear un sistema operativo completamente libre: el sistema GNU

X Window System: (en español sistema de ventanas X) es un software que fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix.

MCC Interim Linux: es una distribución Linux obsoleta inicialmente desarrollada en febrero de 1992 por Owen Le Blanc del Manchester Computing Centre (MCC)

TAMU: Texas A&M University

Yggdrasil: fue una de las primeras distribuciones de Linux, desarrollada por Yggdrasil Computing, Incorporated, una empresa fundada por Adam J. Richter en Berkeley, California.

SLS: Softlanding Linux System (SLS) fue una de las primeras distribuciones del sistema operativo GNU/Linux, fundada por Peter MacDonald a mediados de 1992, que provenía de la distribución conocida como MCC Interim Linux.

Slackware Linux: es la distribución Linux más antigua que tiene vigencia.

DOS: es una familia de sistemas operativos para PC. El nombre son las siglas de disk operating system

Microsoft Windows: es el nombre de una serie de sistemas operativos desarrollados por Microsoft desde 1981, año en que el proyecto se denominaba "Interface Manager".

Mac OS: (del inglés Macintosh Operating System, en español Sistema Operativo de Macintosh) es el nombre del sistema operativo creado por Apple para su línea de computadoras Macintosh

Unix: (registrado oficialmente como UNIX®) es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy

Compilador: es un programa informático que traduce un programa escrito en un lenguaje de programación a otro lenguaje de programación, generando un programa equivalente que la máquina será capaz de interpretar.

GNOME: es un entorno de escritorio e infraestructura de desarrollo para sistemas operativos Unix y derivados Unix como GNU/Linux, BSD o Solaris; compuesto enteramente de software libre.

KDE: es un proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.

Código binario: es el sistema de representación de textos, o procesadores de instrucciones de ordenador, utilizando el sistema binario (sistema numérico de dos dígitos, o bit: el "0" y el "1")

CPU: La unidad central de procesamiento o CPU (por el acrónimo en inglés de central processing unit), o simplemente el procesador o microprocesador, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos

Paquete Un paquete de software es una serie de programas que se distribuyen conjuntamente.

PNG: Portable Network Graphics) es un formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps no sujeto a patentes.

RPM: Package Manager (o RPM, originalmente llamado Red Hat Package Manager, pero se convirtió en acrónimo recursivo1) es una herramienta de administración de paquetes pensada básicamente para GNU/Linux

TAR: se refiere en Informática a un formato de archivos ampliamente usado en entornos UNIX, identificados con la extensión tar

GZIP: es una abreviatura de GNU ZIP, un software libre GNU que reemplaza al programa compress de UNIX. gzip fue creado por Jean-loup Gailly y Mark Adler. Apareció el 31 de octubre de 1992 (versión 0.1). La versión 1.0 apareció en febrero de 1993.

Slapt-get, Slackpkg y Sware: sistemas para el manejo de paquetes en la distribución Slackware GNU/Linux.

Portage: es el gestor de paquetes oficial de la distribución de Linux Gentoo

Live CD: Es una distribución live o Live CD o Live DVD, más genéricamente Live Distro, (traducido en ocasiones como CD vivo o CD autónomo), es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble,

LISP: Es un dialecto del lenguaje de programación Lisp, publicado en el documento estándar ANSI INCITS 226-1994 (R2004) del ANSI, (antes X3.226-1994 (R1999))

BASH: es un programa informático cuya función consiste en interpretar órdenes. Está basado en la shell de Unix y es compatible con POSIX

Perl: es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Fortran: (previamente FORTRAN)1 (del inglés Formula Translating System) es un lenguaje de programación alto nivel de propósito general,2 procedimental3 e imperativo, que está especialmente adaptado al cálculo numérico y a la computación científica

Python: es un lenguaje de programación de alto nivel cuya filosofía hace hincapié en una sintaxis muy limpia y que favorezca un código legible.

Máquina Virtual: En informática una máquina virtual es un software que emula a una computadora y puede ejecutar programas como si fuese una computadora real.

Nmap: es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon

Nessus: es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.

10. BIBLIOGRAFÍA

10.1. Internet

- http://nmap.org
- http://www.itgi.org
- http://www.isaca.org

10.2. Libros

- COBIT 4.1 – ISACA
- Practicas de Control de COBIT, 2da Edición
- Guía de Implementación de Gobierno TI: Uso de COBIT y Val IT, 2da Edición.

10.3. Manuales

- Nessus - Tenable Network Security, Inc.

10.4. Herramientas

- Nessus-4.2.2-i386.msi - Tenable Network Security, Inc.
- Nmap-5.21-setup.exe – NMAP.ORG
- OracleXEClient.exe – Oracle Corporation
- Checkpwd 1.23 [Win] - (c) 2005-2007 by Red-Database-Security GmbH