UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: SHARON RUTH ESTRADA ROJAS

TUTOR: CARLOS ALFREDO BANGUERA DÍAZ

GUAYAQUIL – ECUADOR

2013

Presidencia de la República del Ecuador / Plan Nacional de Ciencia, Tecnología, Innovación y Saberes / SENESCYT Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación		
REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO "CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS"		
	REVISORES:	
INSTITUCIÓN: **Universidad de Guayaquil**	**FACULTAD:** **Ciencias Matemáticas y Físicas**	
CARRERA: **Ingeniería en sistemas computacionales**		
FECHA DE PUBLICACIÓN:	**N° DE PÁGS.:** **207**	
ÁREA TEMÁTICA: **investigación**		
PALABRAS CLAVES: **normas de seguridad, información, base de datos**		
RESUMEN: **El desarrollo de este estudio es establecer cuáles son los riesgos a los que las empresas podrían exponerse cuando poseen bases de datos que no cumplan con normas de seguridad en la información, teniendo como propósito reducir el riesgo asociado al uso de bases de datos que no cumplen con las normas de seguridad, además analizar efecto en el riesgo que causa la seguridad de la información de las empresas.**		
N° DE REGISTRO(en base de datos):	**N° DE CLASIFICACIÓN:** **Nº**	
DIRECCIÓN URL (tesis en la web):		
ADJUNTO PDF	[x] **SI**	[ ] **NO**
CONTACTO CON AUTOR:	**Teléfono: 0993715223**	**E-mail: serget86@hotmail.com**
CONTACTO DE LA INSTITUCIÓN	**Nombre:**	
	Teléfono:	

Guayaquil, Julio 2013

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS" elaborado por la Sra. ESTRADA ROJAS SHARON RUTH, egresada de la Carrera de Ingeniería en Sistemas Computacionales, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

…….

Ing. Carlos Alfredo Banguera Díaz

TUTOR

DEDICATORIA

Esta tesis va dedicada a Dios, mi madre, mi esposo, mis hermanos y familiares por ser un apoyo para terminar mi carrera

AGRADECIMIENTO

Este agradecimiento va a las personas que estaban desde un principio hasta el final de mi carrera Dios, mi madre, mi esposo, mis hermanos, les doy gracias por estar siempre cuando los necesite con el amor para darme para seguir y conseguir el título que hoy en día voy a obtener.

TRIBUNAL DE GRADO

Ing. Fernando Abad Montero

DECANO DE LA FACULTAD

CIENCIAS MATEMATICAS Y FISICAS

Ing. Julio César Castro Rosado

DIRECTOR

Ing. Carlos Banguera Díaz

TUTOR

PROFESOR DEL ÁREA – TRIBUNAL

AB. Juan Chávez A.
SECRETARIO

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS

Proyecto de Tesis de Grado que se presenta como requisito

para optar por el título de

INGENIERO EN SISTEMAS COMPUTACIONALES

Autora: Sharon Ruth Estrada Rojas

C.I. 0922740477

Tutor: Carlos Alfredo Banguera Díaz

Guayaquil, Julio del 2013

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor de Tesis de Grado, nombrado por el Departamento de Investigación, Desarrollo Tecnológico y Educación Contínua de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil,

CERTIFICO:

Que he analizado el Proyecto de Grado presentado por la egresada SHARON RUTH ESTRADA ROJAS, como requisito previo para optar por el título de Ingeniero cuyo problema es:

CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS

Considero aprobado el trabajo en su totalidad.

Presentado por:

_____ _____

SHARON RUTH ESTRADA ROJAS Cédula de ciudadanía Nº

Tutor: Ing. Carlos Banguera Díaz

Guayaquil, Julio 2013

ÍNDICE GENERAL

ÍNDICE CUADROS

ÍNDICE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS

Autora: Sharon Ruth Estrada Rojas

Tutor: Carlos Banguera Díaz

RESUMEN

Las normas de seguridades en las bases de datos hoy en día son muy importantes en nuestros medios ya que hay personas, empresas, entidades públicas, etc., las cuales manejan información que son relevantes y por lo tanto necesitan salvaguardar su información de sufrir alguna pérdida o robo. El desarrollo de este estudio es establecer cuáles son los riesgos a los que las empresas podrían exponerse cuando poseen bases de datos que no cumplan con normas de seguridad en la información. Por lo cual se puede considerar factible este proyecto, la metodología utilizada es para visualizar los problemas y buscar la forma de cómo solucionarlos. El tipo de investigación es explorativa ya que recoger e identificar antecedentes generales, números y cuantificaciones, temas y tópicos respecto del problema investigado, sugerencias de aspectos relacionados que deberían examinarse en profundidad en futuras investigaciones. El propósito de este estudio es reducir el riesgo asociado al uso de bases de datos que no cumplen con las normas de seguridad, además analizar efecto en el riesgo que causa la seguridad de la información de las empresas. Por lo que mediante los instrumentos de investigación realizaremos la evaluación del cumplimiento de las normas de seguridad de las bases de datos (en su actualidad). Los beneficiarios directos son todas las empresas, pues con este estudio tendrán un mejor conocimiento para poder elegir qué base de datos utilizar para su información y que sea segura.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS

Autora: Sharon Ruth Estrada Rojas

Tutor: Carlos Banguera Díaz

ABSTRACT

Standards of assurance in the databases today are very important in our media as there are people, companies, public entities, and so on, Which hold information that is relevant andtherefore need to safeguard your information to suffer some loss or theft. The development of this study is to establish what are the risks to which companies could be exposed when you have databases that do not meet safety standards in the information. Thus can be considered feasible this project, the methodology used to visualize the problems and find ways to fix them. The exploratory research is to collect and identify asgeneral background, numbers and quantifications, themes and topics on the research problem, suggested aspects to be considered in depth in future research. The purpose of this study is to reduce the risk associated with use of databases that do not meet safety standards, but also to analyze the effect on risk causing information security companies.As with the research tools will make the assessment of compliance with safety standardsof the databases (where present). The direct beneficiaries are all companies, as thisstudy will have a better knowledge to choose which database to use for your information and make it safe.

INTRODUCCIÓN

El cumplimiento de las normas de seguridad de información hoy en muestro medio es sumamente importante ya que en el campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial.

La mayoría de las bases de datos contienen, propietario y/o información privada. Esto puede incluir información del cliente, sueldos de empleado, registros de pacientes, números tarjetas de crédito. La clave para mantener esta información de forma segura es la confidencialidad y las empresas que no puedan garantizar la seguridad de esta información confidencial se encontraría en un riesgo muy alto.

Lo más relevante es establecer cuáles son los riesgos que las empresas pueden adquirir cuando su información está en una base de datos que no cumplan con normas de seguridad en la información, ya que la arquitectura de seguridad de las empresas debe ser versátil y extensible, debe ser capaz de crecer y desarrollarse con la organización, apoyar el nuevo negocio iniciativas y estrategias de tecnología, sobre las amenazas que pueden surgiré ya sean estos accesos no autorizados, ataques maliciosos internos o externos.

Otro punto importante es la persona encargada del manejo de la base de datos ya que por más elevado que sea un sistema de seguridad no podrá hacer nada ante los errores cometidos por el factor humano.

A continuación el detalle de los capítulos:

En el Capítulo I encontramos la raíz del proyecto, es decir, el problema, la situación actual, sus causas y consecuencias, delimitación, planteamiento y evaluación del problema, los objetivos generales y específicos del proyecto y por último la importancia y la justificación de la investigación.

En el Capítulo II es el más importante porque se encuentra el contenido de la Investigación, la comprensión del Marco Teórico, el aspecto legal del tema investigado y las hipótesis que se lograrán contestar al final del proyecto.

En el Capítulo III encontramos la aplicación de la Metodología utilizada en el desarrollo de la investigación, además de los instrumentos seleccionados para este tipo de proyecto, donde analizaremos los resultados obtenidos mediante estás técnicas.

En el Capítulo IV encontraremos el cronograma de actividades o Diagrama de Gantt, utilizado para la planificación y control del proyecto, además del

presupuesto de todos los recursos requeridos al desarrollo de la investigación. También se encontrará toda la fuente de información consultada en modo de referencias bibliográficas.

En el Capítulo V como desenlace de la investigación encontraremos las recomendaciones y las conclusiones del proyecto: “CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS”.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIETO DEL PROBLEMA

UBICACIÓN DEL PROBLEMA EN UN CONTEXTO

Hoy en día las bases de datos tienen que cumplir con normas de seguridad.

Lo que se busca de una base de datos es:

Tiene que ser versátil: esto quiere decir que, dependiendo de los usuarios o las aplicaciones, puedan hacer diferentes cosas o traten a los datos de formas distintas.

Tiene que atender con la rapidez adecuada a cada aplicación o empresa, atendiendo a lo que se la requiera.

Tiene que tener un índice de redundancia lo más bajo posible.

Tener una alta capacidad de tiempo y respuesta al acceso para optimizar el mayor tiempo posible en la realización de consultas.

Tener un alto índice de integridad, esto significa que al mayor acceso los usuarios a una misma base de datos no puede haber fallos en la inserción de datos, errores por redundancia o lenta actualización.

Por último tiene que ser posible su constante actualización para no dejar a la base de Datos anticuados e inservibles. Cuando hacemos un cambio en la organización

física de los datos, no debe afectar a los programas por lo que también tiene que tener una independencia física de los datos. Al igual que tiene que tener total independencia lógica con los datos, esto quiere decir que si hacemos cambios en la estructura lógica de los datos (agregar nuevos campos a una tabla) no deben afectar a las aplicaciones que utilicen esos datos.

Lo que conlleva a enfocarnos, es que es sumamente importante la seguridad y privacidad ya que los datos que se pueden almacenar en una base de datos pueden ser altamente confidenciales o importantes. En este punto también entran los medios físicos de protección contra fuego, robo, etc.

SITUACIÓN CONFLICTO NUDOS CRÍTICOS

El problema surge del riesgo que incurre en la información de las empresas, que utilizan bases de datos que no cumplen con las respectivas normas de seguridad; ya que estarían en peligro, ocasionando: pérdidas inesperadas, datos erróneos o hurto de información, fraudes, espionaje, sabotaje, vandalismo, acceso no autorizados.

CAUSAS Y CONSECUENCIAS DEL PROBLEMA

Las causas por las que se obtienen un riesgo alto de inseguridad de datos y/o información es porque no se cumple con normas y políticas de seguridad o no se incluyen los mecanismos que controlan el acceso y uso de la base de datos, no se asignan a los usuarios sus roles o privilegios de acceso.

Las consecuencias de no utilizar las normas o políticas de seguridad seria la pérdida inesperada de la información, datos erróneos.

Dadas que las normas y las políticas de seguridad de la información se basan en lo que es la confidencialidad, disponibilidad e integridad de una base de datos.

Confidencialidad.- La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados es difícil estar 100% seguro de que los datos entregados por el consumidor serán utilizados únicamente para los fines en que se entregaron dichos datos.

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.

Recuperación.- 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.).

DELIMITACIÓN DEL PROBLEMA

La verificación del cumplimiento de normas de seguridad de las bases de datos será solo en las empresas de Guayaquil, enfocándonos en el sector las consultoras y constructoras de obras civiles.

Las empresas a seleccionarse para la verificación se lo hará en una manera explorativa se tendrán en cuenta empresas entre medianas y pequeñas.

Será investigado en un 85 % de las bases más utilizadas, donde abarque más de

dos bases de datos en el cual podemos comparar en que base de datos es más crítico el no usar normas o políticas de seguridad así no obtener un mayor riesgo en la información que es vital en las empresas.

FORMULACIÓN DEL PROBLEMA

¿Cuál es el efecto en el nivel de riesgo de la información si las empresas utilizan bases de datos que no cumplen las normas de seguridad?

EVALUACIÓN DEL PROBLEMA

Los aspectos generales de evaluación son:

Delimitado: En el estudio de la evaluación de cumplimento de normas de seguridad estará basado en las empresas de Guayaquil, enfocándonos en el sector las consultoras y constructoras de obras civiles, el cual se orienta a determinar cuáles son las normas de seguridad que no pueden ser omitidas y son muy riesgosas para las bases de datos que no las cumplen.

Claro: El tema a desarrollar es claro, es saber cuáles son las normas de seguridad que cumplen las mayorías de las bases de datos y ver que bases de datos son usadas en Guayaquil, para así saber si cumplen o no con las normas de seguridad, ver cuál sería el impacto en las empresas y el riesgo que corren los datos de la compañía si sus bases de datos no cumplen con la correcta seguridad de sus datos.

Evidente: El estudio se determina ya que hoy en día se ve mucho lo de fraude informático un antecedente es: según fuente del Diario HOY publico el 12 de diciembre del 2010 “Según estadísticas del Observatorio de Seguridad Ciudadana de Guayaquil (OSC), desde el 1. ° de enero hasta el 12 de diciembre de 2010, se han presentado 199 denuncias por transferencias bancarias ilícitas vía Internet en la urbe porteña, siendo septiembre el mes de mayor incidencia con el 24,62% de los casos. En tanto, diciembre registra el 1,51%. (…) De acuerdo con cifras del organismo, el robo a los clientes del Banco Pichincha en 2010 sumó $193 703,22, seguido por el Banco del Pacífico con $102 022,59, Produbanco con $73 931,87, Banco de Guayaquil con $45 922,23, IESS con $44 251,24, entre otros.” y se puede determinar si es por causa de los usuarios externos de la base datos o de la falta de cumplimiento de normas.

Otras de las causas porque se debe realizar estos estudios es por las fallas que se pueden dar en las bases de datos que hay 5 principales:

Las organizaciones no saben aún donde residen sus datos sensibles.

El monitoreo de la seguridad sigue siendo aún irregular y no sistemático.

Los usuarios privilegiados se siguen ejecutando sin un adecuado control y seguimiento.

Los parches en las bases de datos se despliegan y aplican lentamente.

Existe un evidente retraso en la aplicación de técnicas de cifrado sobre las bases de datos.

Concreto: Porque se determina cual es el riesgo del incumplimiento de las normas, la cual es muy importante no solo en una o dos empresas sino en todas ya que en todos se debe que velar por la seguridad de los datos.

Relevante: El tema no solo es importante para la comunidad educativa sino para todas las comunidades ya que la información que se maneja en todos los medios es de importancia para su crecimiento.

Contextual: Indiscutiblemente el tema forma parte de la sociedad ya que este estudio está incluido en todas las partes de las sociedades; esta contiene información muy importante que tiene que estar con las debidas normas de seguridad.

Factible: El estudio es factible ya que según el alcance del tema, mediante el cual se llega a la verificación si los datos de las empresas no pueden sufrir alguna pérdida o robo de información.

Variables: El estudio presenta tres variables, las cuales se determinan por una variable independiente y por dos variables dependiente.

La variable independiente es la evaluación del cumplimiento de las normas de seguridad de las bases de datos (en su actualidad).

Las variables dependientes son:

El efecto en el riesgo que causa la seguridad de la información de las empresas.

Propuesta para reducir el riesgo asociado al uso de bases de datos que no cumplen con las normas de seguridad.

OBJETIVOS

OBJETIVO GENERAL

Establecer cuáles son los riesgos a los que las empresas podrían exponerse cuando poseen bases de datos que no cumplan con normas de seguridad en la información.

Reducir los riesgos más críticos de la información en las empresas.

OBJETIVOS ESPECÍFICOS

Analizar las normas de seguridad y comparar las bases de datos más utilizadas en Guayaquil, enfocándonos en el sector las consultoras y constructoras de obras civiles, esto equivale al 85% del muestreo de las encuestas verificando entre ellas que normas cumplen o no.

Definir cuáles son los riesgos asociados en la seguridad de información y como se pueden reducir para las empresas que manejan bases de datos sin normas de seguridad.

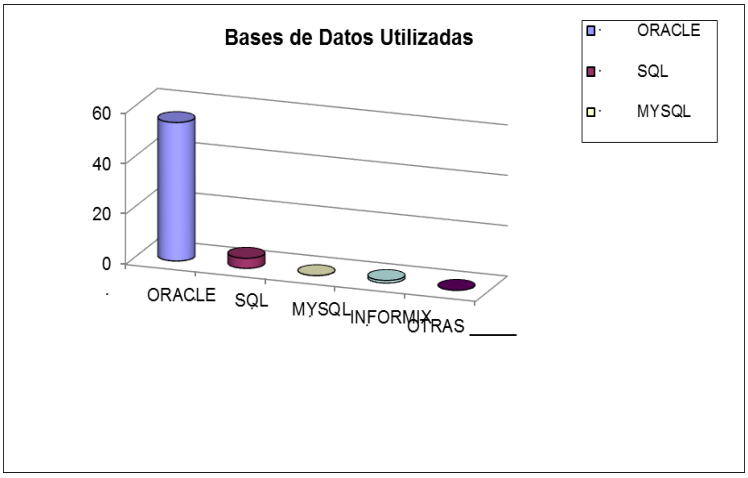
Evaluar soluciones o aplicaciones complementarias que me permita utilizar las normas ISO 27002.

Realizar recomendaciones para disminuir los riesgos en la información de las bases de datos.

ALCANCES

Analizar cada una de las normalizaciones y elegir una norma de seguridad para aplicarla en el 85% del muestreo de las encuestas que corresponden a cuatro bases de datos (Oracle, Sql Server, Informix, Access). Según en el GRAFICO BASE DE DATOS UTILIZADAS D*etermina cuáles de las bases de datos son las utilizadas en Guayaquil en el sector las consultoras y constructoras de obras civiles, escogimos cuatro bases de datos dándonos como resultado que el 90% utiliza Oracle, un 7% utiliza SQL, un 1% utiliza Informix, y una pequeña parte teniendo un 2% utilizan como bases de datos Access, Visual FoxPro.*

GRAFICO BASES DE DATOS UTILIZADAS



Describir mínimo 10 riesgos que una empresa obtiene cuando la información está sobre una base de datos que no cumplan con normas de seguridad.

En base a los criterios de las normas con los que no cumplen las bases de datos, encontrar cinco vulnerabilidades más críticas en las cuatro bases de datos más utilizadas en Guayaquil, basándonos en la normalización de la ISO 27002.

Identificar cuáles son los beneficios cuando una empresa tiene la información sobre una base de datos que cumple con normas de seguridad en la información.

Comparar los beneficios y riesgos que tienen las empresas cuando la información que manejan está sobre bases de datos que cumple y no con normas de seguridad en la información.

Investigar cómo se pueden reducir los riesgos cuando la información que maneja la empresa se encuentra en bases de datos que no cumplen con normas de seguridad en la información.

Realizar recomendaciones para solventar cada vulnerabilidad encontrada.

JUSTIFICACION E IMPORTANCIA

Las razones para la investigación del tema son por la magnitud del problema en que se encontraría una empresa si la información no es la correcta o es manipulada por personas no adecuadas.

Esto con lleva a un gran impacto ya que en todo los entornos para el funcionamiento de las empresas es necesaria la información y está siempre debe ser verídica.

La importancia que se le da a este estudio de verificación de las normas de seguridades en las bases de datos tiene que ver mucho con las empresas quienes son las encargadas de manejar la información privada y/o pública que los usuarios les confían.

Los resultados de este proceso van a beneficiar tanto a la empresa y a los que proporcionan la información ya que si la empresa consta con las debidas seguridades de la información este puede seguir su enfoque correcto sin errores y a su vez a los que la proporcionan porque tiene su información segura y sin que otros puedas manipularlas con otro fines no autorizados.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES DEL ESTUDIO

En la actualidad en nuestro país no hay estudios que se determine cuál es el riesgo que puede causar una base de datos con información sumamente importante que no cumpla con las normas de seguridad adecuadas para salvaguardar los datos de la empresa.

FUNDAMENTACIÓN TEÓRICA

Para entender lo de las normas de seguridades en las bases de datos y cuan importante son en nuestro medio tenemos que definir lo que contiene que son datos & información.

Una definición clara nos la da Carlo Vinicio Caballero Uribe (2006) cuando crea una base de datos para el estudio de la AR en Latinoamérica.

> **"DATOS.- es una representación simbólica (numérica, alfabética, algorítmica etc.) de un atributo o característica de una entidad. El dato no tiene valor semántico (sentido) en sí mismo, pero convenientemente tratados (procesado) se puede utilizar en la realización de cálculos o toma de decisiones. (…).**

> **INFORMACIÓN.- (…) la información es un conjunto organizado de datos, que constituye un mensaje sobre un determinado ente o fenómeno. (…). Los datos se convierten en información cuando su creador les añade significado.” (pág. 317)**

En general la información tiene una estructura interna y puede ser calificada según varios aspectos:

- **Significado (semántica):** ¿Qué quiere decir? Del significado extraído de una información, cada individuo evalúa las consecuencias posibles y adecúa sus actitudes y acciones de manera acorde a las consecuencias previsibles que se deducen del significado de la información. Esto se refiere a qué reglas debe seguir el individuo o el sistema experto para modificar sus expectativas futuras sobre cada posible alternativa.
- **Importancia (relativa al receptor):** ¿Trata sobre alguna cuestión importante? La importancia de la información para un receptor, se referirá a en qué grado cambia la actitud o la conducta de los individuos. En las modernas sociedades, los individuos obtienen de los medios de comunicación masiva gran cantidad de información, una gran parte de la misma es poco importante para ellos, porque altera de manera muy poco significativa la conducta de los individuos. Esto se refiere a en qué grado cuantitativo deben alterarse las expectativas futuras. A veces se sabe que un hecho hace menos probables algunas cosas y más otras, la importancia

tiene que ver con cuanto menos probables serán unas alternativas respecto a las otras.

- **Vigencia (en la dimensión espacio-tiempo):** ¿Es actual o desfasada? En la práctica la vigencia de una información es difícil de evaluar, ya que en general acceder a una información no permite conocer de inmediato si dicha información tiene o no vigencia.
- **Validez (relativa al emisor):** ¿El emisor es fiable o puede proporcionar información no válida (falsa)? Esto tiene que ver si los indicios deben ser considerados en la reevaluación de expectativas o deben ser ignorados por no ser indicios fiables.
- **Valor (activo intangible volátil):** ¿Cómo de útil resulta para el destinatario?

Una vez teniendo la definición de lo que es dato e información podemos sacar las siguientes diferencias:

- Los Datos a diferencia de la información son utilizados como diversos métodos para comprimir la información a fin de permitir una transmisión o almacenamiento más eficaces.
- Aunque para el procesador de la computadora hace una distinción vital entre la información entre los programas y los datos, la memoria y muchas otras partes de la computadora no lo hace. Ambos son registradas temporalmente según la instrucción que se le dé. Es como un pedazo de

papel no sabe ni le importa lo que se le escriba: un poema de amor, las cuentas del banco o instrucciones para un amigo. Es lo mismo que la memoria de la computadora. Sólo el procesador reconoce la diferencia entre datos e información de cualquier programa. Para la memoria de la computadora, y también para los dispositivos de entrada y salida (E/S) y almacenamiento en disco, un programa es solamente más datos, más información que debe ser almacenada, movida o manipulada.

- La cantidad de información de un mensaje puede ser entendida como el número de símbolos posibles que representan el mensaje. "los símbolos que representan el mensaje no son más que datos significativos.
- En su concepto más elemental, la información es un mensaje con un contenido determinado emitido por una persona hacia otra y, como tal, representa un papel primordial en el proceso de la comunicación, a la vez que posee una evidente función social. A diferencia de los datos, la información tiene significado para quien la recibe, por eso, los seres humanos siempre han tenido la necesidad de cambiar entre sí información que luego transforman en acciones. "La información es, entonces, conocimientos basados en los datos a los cuales, mediante un procesamiento, se les ha dado significado, propósito y utilidad".

BASES DE DATOS

Una base de datos o banco de datos (en ocasiones abreviada con la sigla BD o con la abreviatura b. d.) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. En la actualidad, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), que ofrece un amplio rango de soluciones al problema de almacenar datos.

En resumen lo que es una base de datos nos lo da C. J. Date (introducción a los sistemas de bases de datos 7ma edición)

> **"Una base de datos es un conjunto de datos persistentes que es utilizado por los sistemas de aplicación de alguna empresa dada."**

Las bases de datos son importantes para tener una gran cantidad de datos almacenados los cuales sean visualizados, actualizados y modificados en un tiempo prudencial, así mismo nos algunos beneficios o ventajas como lo menciona C. J. Date (introducción a los sistemas de bases de datos 7ma edición)

> **"<u>Compactación</u>: No hay necesidad de archivos en papel voluminosos.**

> **<u>Velocidad:</u> La máquina puede recuperar y actualizar datos más rápidamente que un humano.**
>
> **En particular, las consultas específicas sin mucha elaboración pueden ser respondidas con rapidez, sin necesidad de búsquedas manuales o visuales que llevan tiempo.**
>
> **<u>Menos trabajo laborioso;</u> Se puede eliminar gran parte del trabajo de llevar los archivos a mano. Las tareas mecánicas siempre las realizan mejor las máquinas.**
>
> **<u>Actualidad:</u> En el momento que la necesitemos, tendremos a nuestra disposición información precisa y actualizada. ”**

Existen programas denominados sistema de gestión de bases de datos, abreviado SGB, que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada.

La definición de Olga Pons Capote (Introducción a las bases de datos: el modelo relacional, 2005)

> **“conjunto de elementos software con capacidad de definir, mantener y utilizar una base de datos”**

También se determina las funciones fundamentales de los SGB q son las de crear modificar eliminar obtener la estructura asociada al esquema lógico de una base

de datos, y, instanciar datos operativos en una base de datos, modificar dichas instancias, eliminarlas y recuperarlas bajos diferentes criterios de búsqueda.

Las aplicaciones más usuales son para la gestión de empresas e instituciones públicas. También son ampliamente utilizadas en entornos científicos con el objeto de almacenar la información experimental.

Aunque las bases de datos pueden contener muchos tipos de datos, algunos de ellos se encuentran protegidos por las leyes de varios países.

SISTEMA DE GESTIÓN DE BASES DE DATOS DISTRIBUIDA (SGBD)

La base de datos y el software SGBD pueden estar distribuidos en múltiples sitios conectados por una red. Hay de dos tipos:

1. Distribuidos homogéneos: utilizan el mismo SGBD en múltiples sitios.

2. Distribuidos heterogéneos: Da lugar a los SGBD federados o sistemas multibase de datos en los que los SGBD participantes tienen cierto grado de autonomía local y tienen acceso a varias bases de datos autónomas preexistentes almacenados en los SGBD, muchos de estos emplean una arquitectura cliente-servidor.

Estas surgen debido a la existencia física de organismos descentralizados. Esto les da la capacidad de unir las bases de datos de cada localidad y acceder así a distintas universidades, sucursales de tiendas, etcétera.

Objetivos del sistema de gestión de bases de datos distribuida (SGBD)

Los objetivos que deben tener los sistemas de gestión de bases de datos distribuida son de:

- Diseño y utilización orientada al usuario
- Centralización
- Evitar la redundancia y gestionar la concurrencia
- Mantener la integridad semántica de los datos
- Mantener la seguridad
- Mantener la fiabilidad del sistema

PRODUCTOS SGBD DISPONIBLES EN EL MERCADO

SGBD libres

- PostgreSQL (http://www.postgresql.org Postgresql) Licencia BSD
- Firebird basada en la versión 6 de InterBase, Initial Developer's PUBLIC LICENSE Versión 1.0.
- SQLite (http://www.sqlite.org SQLite) Licencia Dominio Público
- DB2 Express-C (http://www.ibm.com/software/data/db2/express/)
- Apache Derby (http://db.apache.org/derby/)
- MariaDB (http://mariadb.org/)

- MySQL (http://dev.mysql.com/)

SGBD no libres

- MySQL: Licencia Dual, depende del uso. No se sabe hasta cuándo permanecerá así, ya que ha sido comprada por Oracle. Sin embargo, existen 2 versiones: una gratuita que sería equivalente a la edición "express" SQL server de Microsoft Windows, y otra más completa de pago.
- Advantage Database
- dBase
- FileMaker
- Fox Pro
- gsBase
- IBM DB2: Universal Database (DB2 UDB)
- IBM Informix
- Interbase de CodeGear, filial de Borland
- MAGIC
- Microsoft Access
- Microsoft SQL Server
- NexusDB
- Open Access

- Oracle
- Paradox
- PervasiveSQL
- Progress (DBMS)
- Sybase ASE
- Sybase ASA
- Sybase IQ
- WindowBase
- IBM IMS Base de Datos Jerárquica
- CA-IDMS

SGBD no libres y gratuitos

- Microsoft SQL Server Compact Edition Basica
- Sybase ASE Express Edition para Linux (edición gratuita para Linux)
- Oracle Express Edition 10 (solo corre en un servidor, capacidad limitada)

TIPOS DE BASE DE DATOS

Las bases de datos pueden clasificarse de varias maneras, de acuerdo al contexto que se esté manejando, la utilidad de las mismas o las necesidades que satisfagan.

- **Según la variabilidad de los datos almacenados**
    - **Bases de datos estáticas**

      Son bases de datos de sólo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.

    - **Bases de datos dinámicas**

      Éstas son bases de datos donde la información almacenada se modifica con el tiempo, permitiendo operaciones como actualización, borrado y adición de datos, además de las operaciones fundamentales de consulta. Un ejemplo de esto puede ser la base de datos utilizada en un sistema de información de un supermercado, una farmacia, un videoclub o una empresa.

- **Según el contenido**
    - **Bases de datos bibliográficas**

      Sólo contienen un subrogante (representante) de la fuente primaria, que permite localizarla. Un registro típico de una base de datos bibliográfica contiene información sobre el autor, fecha de publicación, editorial, título, edición, de una determinada publicación, etc. Puede contener un resumen o extracto de la

publicación original, pero nunca el texto completo, porque si no, estaríamos en presencia de una base de datos a texto completo (o de fuentes primarias). Como su nombre lo indica, el contenido son cifras o números. Por ejemplo, una colección de resultados de análisis de laboratorio, entre otras.

- **Bases de datos de texto completo**

  Almacenan las fuentes primarias, como por ejemplo, todo el contenido de todas las ediciones de una colección de revistas científicas.

- **Directorios**

  Un ejemplo son las guías telefónicas en formato electrónico.

- **Bases de datos o "bibliotecas" de información química o biológica**

  Son bases de datos que almacenan diferentes tipos de información proveniente de la química, las ciencias de la vida o médicas. Se pueden considerar en varios subtipos:

  - Las que almacenan secuencias de nucleótidos o proteínas.
  - Las bases de datos de rutas metabólicas.
  - Bases de datos de estructura, comprende los registros de datos experimentales sobre estructuras 3D de biomoléculas.

- Bases de datos clínicas.
- Bases de datos bibliográficas (biológicas, químicas, médicas y de otros campos).

MODELOS DE BASE DE DATOS

Además de la clasificación por la función de las bases de datos, éstas también se pueden clasificar de acuerdo a su modelo de administración de datos.

Un modelo de datos es básicamente una "descripción" de algo conocido como *contenedor de datos* (algo en donde se guarda la información), así como de los métodos para almacenar y recuperar información de esos contenedores. Los modelos de datos no son cosas físicas: son abstracciones que permiten la implementación de un sistema eficiente de *base de datos*; por lo general se refieren a algoritmos, y conceptos matemáticos.

Algunos modelos con frecuencia utilizados en las bases de datos:

- **Bases de datos jerárquicas**

  Éstas son bases de datos que, como su nombre indica, almacenan su información en una estructura jerárquica. En este modelo los datos se organizan en una forma similar a un árbol (visto al revés), en donde un *nodo padre* de información puede tener varios *hijos*. El nodo que no tiene padres es llamado *raíz*, y a los nodos que no tienen hijos se los conoce como *hojas*.

Las bases de datos jerárquicas son especialmente útiles en el caso de aplicaciones que manejan un gran volumen de información y datos muy compartidos permitiendo crear estructuras estables y de gran rendimiento.

Una de las principales limitaciones de este modelo es su incapacidad de representar eficientemente la redundancia de datos.

- **Base de datos de red**

  Éste es un modelo ligeramente distinto del jerárquico; su diferencia fundamental es la modificación del concepto de *nodo*: se permite que un mismo nodo tenga varios padres (posibilidad no permitida en el modelo jerárquico).

  Fue una gran mejora con respecto al modelo jerárquico, ya que ofrecía una solución eficiente al problema de redundancia de datos; pero, aun así, la dificultad que significa administrar la información en una base de datos de red ha significado que sea un modelo utilizado en su mayoría por programadores más que por usuarios finales.

- **Bases de datos transaccionales**

  Son bases de datos cuyo único fin es el envío y recepción de datos a grandes velocidades, estas bases son muy poco comunes y están dirigidas por lo general al entorno de análisis de calidad, datos de producción e industrial, es importante entender que su fin único es recolectar y

recuperar los datos a la mayor velocidad posible, por lo tanto la redundancia y duplicación de información no es un problema como con las demás bases de datos, por lo general para poderlas aprovechar al máximo permiten algún tipo de conectividad a bases de datos relacionales.

- **Bases de datos relacionales**

  Éste es el modelo utilizado en la actualidad para modelar problemas reales y administrar datos dinámicamente. Tras ser postulados sus fundamentos en 1970 por Edgar Frank Codd, de los laboratorios IBM en San José (California), no tardó en consolidarse como un nuevo paradigma en los modelos de base de datos. Su idea fundamental es el uso de "relaciones". Estas relaciones podrían considerarse en forma lógica como conjuntos de datos llamados "tuplas". Pese a que ésta es la teoría de las bases de datos relacionales creadas por Codd, la mayoría de las veces se conceptualiza de una manera más fácil de imaginar. Esto es pensando en cada relación como si fuese una tabla que está compuesta por *registros* (las filas de una tabla), que representarían las tuplas, y *campos* (las columnas de una tabla).

  En este modelo, el lugar y la forma en que se almacenen los datos no tienen relevancia (a diferencia de otros modelos como el jerárquico y el de red). Esto tiene la considerable ventaja de que es más fácil de entender y de utilizar para un usuario esporádico de la base de datos. La información

puede ser recuperada o almacenada mediante "consultas" que ofrecen una amplia flexibilidad y poder para administrar la información.

El lenguaje más habitual para construir las consultas a bases de datos relacionales es SQL, *Structured Query Language* o *Lenguaje Estructurado de Consultas*, un estándar implementado por los principales motores o sistemas de gestión de bases de datos relacionales.

Durante su diseño, una base de datos relacional pasa por un proceso al que se le conoce como normalización de una base de datos.

Durante los años 80 la aparición de dBASE produjo una revolución en los lenguajes de programación y sistemas de administración de datos. Aunque nunca debe olvidarse que dBase no utilizaba SQL como lenguaje base para su gestión.

- **Bases de datos multidimensionales**

  Son bases de datos ideadas para desarrollar aplicaciones muy concretas, como creación de **Cubos OLAP**. Básicamente no se diferencian demasiado de las bases de datos relacionales (una tabla en una base de datos relacional podría serlo también en una base de datos multidimensional), la diferencia está más bien a nivel conceptual; en las bases de datos multidimensionales los campos o atributos de una tabla

pueden ser de dos tipos, o bien representan dimensiones de la tabla, o bien representan métricas que se desean estudiar.

- **Bases de datos orientadas a objetos**

  Este modelo, bastante reciente, y propio de los modelos informáticos orientados a objetos, trata de almacenar en la base de datos los *objetos* completos (estado y comportamiento).

  Una base de datos orientada a objetos es una base de datos que incorpora todos los conceptos importantes del paradigma de objetos:

  - Encapsulación - Propiedad que permite ocultar la información al resto de los objetos, impidiendo así accesos incorrectos o conflictos.
  - Herencia - Propiedad a través de la cual los objetos heredan comportamiento dentro de una jerarquía de clases.
  - Polimorfismo - Propiedad de una operación mediante la cual puede ser aplicada a distintos tipos de objetos.

  En bases de datos orientadas a objetos, los usuarios pueden definir operaciones sobre los datos como parte de la definición de la base de datos. Una operación (llamada función) se especifica en dos partes. La interfaz (o signatura) de una operación incluye el nombre de la operación y los tipos de datos de sus argumentos (o parámetros). La implementación

(o método) de la operación se especifica separadamente y puede modificarse sin afectar la interfaz. Los programas de aplicación de los usuarios pueden operar sobre los datos invocando a dichas operaciones a través de sus nombres y argumentos, sea cual sea la forma en la que se han implementado. Esto podría denominarse independencia entre programas y operaciones.

- **Bases de datos documentales**

  Permiten la indexación a texto completo, y en líneas generales realizar búsquedas más potentes. Tesaurus es un sistema de índices optimizado para este tipo de bases de datos.

- **Bases de datos deductivas**

  Un sistema de base de datos deductiva, es un sistema de base de datos pero con la diferencia de que permite hacer deducciones a través de inferencias. Se basa principalmente en reglas y hechos que son almacenados en la base de datos. Las bases de datos deductivas son también llamadas bases de datos lógicas, a raíz de que se basa en lógica matemática. Este tipo de base de datos surge debido a las limitaciones de la Base de Datos Relacional de responder a consultas recursivas y de deducir relaciones indirectas de los datos almacenados en la base de datos.

NORMAS DE SEGURIDAD

NORMAS

El término norma (del latín, norma 'regla'), tiene gran variedad de acepciones:

En Informática, la normalización de una base de datos consiste en aplicar una serie de reglas a las relaciones para evitar la redundancia de los datos y proteger su integridad.

Regla o conjunto de reglas que hay que seguir para llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo.

- Normas de un término que proviene del latín y significa “escuadra”. Una norma es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades.
- Ordenamiento imperativo de acción que persigue un fin determinado con la característica de ser rígido en su aplicación. Regla, disposición o criterio que establece una autoridad para regular acciones de los distintos agentes económicos, o bien para regular los procedimientos que se deben seguir para la realización de las tareas asignadas. Se traduce en un enunciado técnico que a través de parámetros cuantitativos y/o cualitativos sirve de guía para la acción. Generalmente la norma conlleva una estructura de sanciones para quienes no la observen.

Una norma, la norma de América ("cuadrado, el Estado") por lo general se refiere a un estado o una común manera general se considera como una regla a seguir.

Este término genérico se refiere a un conjunto de características que describen un objeto, un ser que puede ser virtuales o no. Todo lo que viene en una norma se considera "normal", mientras que lo que sale es "anormal". Estos términos pueden o no implica juicios de valor.

HISTORIA DE LAS NORMAS

La norma es tradicionalmente uno de los modos preferidos de expresión de la soberanía. Francia en particular, la moneda, el poder soberano de elección, sino también los pesos y medidas, definir el alcance de una de las más antiguas de la normalización.

En su presentación de la norma para el público en general, la Organización Internacional de Normalización (ISO) se refiere a dos fechas: 1906, con la creación de la Comisión Electrotécnica Internacional (IEC) de 1926, el año de creación Federación Internacional de Asociaciones Nacionales de Normalización (ISA , AFNOR). Si esta perspectiva no es incorrecto, es la economía de los acuerdos, concluyó en el último cuarto del siglo XIX, elaboró el enfoque actual de la normalización internacional se aplica a la economía.

Por lo tanto, la firma en 1865 del primer Convenio Telegráfico Internacional y la creación de la Unión del mismo nombre, este año permitió la aplicación de los Reglamentos Telegráfico y, en 1885, el desarrollo de la legislación cooperación en el ámbito de la telefonía y, más adelante, radiocomunicaciones, radiodifusión,

telecomunicaciones espaciales. Del mismo modo, como un producto que requiere el establecimiento de una serie de normas, debido a su utilización transnacional, el sello apareció en su forma moderna en el Reino Unido en 1840 (y aprobada por la década Suiza, Brasil, Estados Unidos, Francia y Bélgica), dio lugar en 1874, mediante convenio, la creación de la Unión General de Correos, que se ha convertido en la Unión Postal Universal. Finalmente, en 1875, la Convención del Metro, firmada en la forma de un tratado diplomático que 51 Estados son ahora parte, es otro ejemplo de una estructura permanente dedicada a la cooperación internacional sobre las normas.

Después de la Segunda Guerra Mundial , el proceso de elaboración de normas ha aumentado considerablemente en la industria, la economía y los sistemas de información . De hecho, a menudo el término se refiere a la estandarización de la estandarización en la industria y los servicios . Debido a su influencia en el ahorro actual, las normas se ve en esta luz puede ser visto como una herramienta de trabajo para extender la influencia del poder económico, utilizando técnicas depresión y redes de organizaciones no gubernamentales por ejemplo, ISO ha publicado más de 16.000 normas desde 1947.

ORIGEN DE LAS NORMAS

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979. Publicación BS 5750 - ahora ISO 9001

1992. Publicación BS 7750 - ahora ISO 14001

1996. Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

- **ISO/IEC 27001:**

  Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En esta norma, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en **AENOR** (también en lengua gallega). En 2009, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2007/1M:2009). Otros países donde también está publicada en español son, por ejemplo, **Colombia** (NTC-ISO-IEC 27001), **Venezuela** (Fondonorma ISO/IEC 27001), **Argentina** (IRAM-

ISO IEC 27001), **Chile** (NCh-ISO27001) o **México** (NMX-I-041/02-NYCE). Fue Publicada a finales del 2012

•ISO/IEC 27002:

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en **AENOR**). Otros países donde también está publicada en español son, por ejemplo, **Colombia** (NTC-ISO-IEC 27002), **Venezuela** (Fondonorma ISO/IEC 27002), **Argentina** (IRAM-ISO-IEC 27002),**Chile** (NCh-ISO27002) o **Perú** (como ISO 17799; descarga gratuita).

• ISO/IEC 27003:

Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el

proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España, esta norma aún no está traducida.

• ISO/IEC 27004:

Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

• ISO/IEC 27005:

Publicada el 4 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

ISO/IEC 27006:

Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

• ISO/IEC 27007:

Publicada en noviembre del 2011. Consiste en una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

• ISO/IEC 27008:

Publicada en noviembre del 2011. Consiste en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

• ISO/IEC 27010:

Publicada en Abril del 2012. Es una norma en 2 partes, que consiste en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.

• ISO/IEC 27011:

Publicada el 15 de Diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.

• ISO/IEC 27012:

Consiste en un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

• ISO/IEC 27013:

Publicada Octubre de 2012. Consiste en una guía de implementación

integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

• ISO/IEC 27014:

Publicada en 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

• ISO/IEC 27015:

Publicada en noviembre del 2012. Consiste en una guía de SGSI para organizaciones del sector financiero y de seguros.

LA ÉTICA NORMATIVA

En la ética , hay una disciplina llamada la ética normativa , que tiene por objeto establecer las normas para el examen crítico de los fundamentos y las formas de la acción correcta. Estos textos fundamentales que pueden aplicarse a áreas más específicas relacionadas con la ética aplicada (por ejemplo, la ética social).

La ética normativa tiene tratos con la ley.

CLASIFICACION DE LAS NORMAS.

Desde el punto de vista de su campo de aplicación las normas de seguridad se pueden clasificar en:

- Normas **GENERALES**, que van dirigidas a todo el centro de trabajo o al menos a amplias zonas del mismo. Marcan o establecen directrices de forma genérica.

- Normas **PARTICULARES o ESPECÍFICAS**, que van dirigidas a actuaciones concretas. Señalan la manera en que se debe realizar una operación determinada.

UTILIDAD Y PRINCIPIOS BÁSICOS DE LA NORMA.

Las normas sirven para: enseñar, disciplinar actuando mejor, complementar la actuación profesional.

Pero no se debe caer en el abuso, ya que un exceso de normas llevaría a la confusión, llegando a producir un efecto negativo y perjudicial. Un exceso de normas contribuye a que no se cumpla ninguna. De ello se desprende la primera condición para que una sea eficaz: Debe ser NECESARIA.

Naturalmente, la norma deberá poder llevarse a la práctica con los medios de que se dispone: Debe ser POSIBLE.

Su contenido será fácilmente comprensible: Debe ser CLARA. Referida a un solo tema: Debe ser CONCRETA. Su lectura deberá ser fácil y no engorrosa: Debe ser BREVE.

Para que una norma sea realmente eficaz debe ser ACEPTADA por quien deba cumplirla y en su caso EXIGIBLE con delimitación precisa de las responsabilidades.

Por último, las técnicas evolucionan, los procesos cambios, una norma que en su momento era perfectamente válida, puede dejar de serlo, quedando anticuada e inservible. Por ello toda norma debe ser renovada y puesta al día: Debe ser ACTUAL.

CONTENIDO DE LAS NORMAS

Para que una norma sea eficaz conviene que disponga de:

- *Objetivo*. Descripción breve del problema esencial que se pretende normalizar (riesgo).
- *Redacción*. Desarrollo en capítulos de los distintos apartados.
- *Campo de aplicación*. Especificación clara del lugar, zona, trabajo y operación a la que debe aplicarse.
- *Grado de exigencia*. Especificación sobre su obligatoriedad o recomendación, indicando, si interesa, la gravedad de la falta.
- *Refuerzo*. Normas legales o particulares que amplíen, mediante su cita el contenido de la norma y a las que debe estar supeditadas.

FASES DE IMPLANTACIÓN DE UNA NORMA

Desde que quienes en la empresa conciben la necesidad de que exista una norma de seguridad hasta que se materializa su implantación debe pasar por las siguientes fases:

Creación

En la elaboración de una norma preventiva deben intervenir todas las partes interesadas ya que de esta manera se consigue el necesario contraste de pareceres y el consenso en su aplicación. Una vez redactada pasará a la dirección de la empresa para su aprobación- la cual indicará si proceden, las correcciones oportunas- y también a los representantes de los trabajadores a través del Comité o Delegado de Seguridad y Salud laboral para ser revisada.

Difusión o Divulgación.

El objeto final de una norma es su aplicación, debiendo por ello ser difundida y comunicada a las personas afectadas para su obligado cumplimiento. Tal difusión podrá hacerse mediante entrega de textos conteniendo las normas y reuniones informativas, o fijación de carteles o avisos, u otros sistemas. Sea cual fuere el sistema empleado, hay que tener garantías de que la norma una vez aprobada es perfectamente conocida por quienes deben aplicarla.

La citada fase se complementará con otras dos:

- Vigilar el cumplimiento de las normas, debiéndose en caso contrario analizar las causas de incumplimiento para tomar las medidas correctoras oportunas.

- Vigilar la posible variación en los métodos de trabajo, llevándose a cabo la actualización de las normas.

SEGURIDAD

La seguridad es el estado de estar "seguro" (del francés sauf),la condición de protegerse contra los tipos físicos, sociales, espirituales, económicos, políticos, emocionales, laborales, psicológicas, educativas o de otra índole o consecuencias de la falta, daño, error , accidentes ,daños o cualquier otro suceso que pueda ser considerado no deseable. La seguridad también se puede definir como el control de los riesgos reconocidos para lograr un nivel aceptable de riesgo. Esto puede tomar la forma de estar protegido de caso o de la exposición a algo que causa pérdidas de salud o económicos. Se puede incluir la protección de las personas o los bienes.

La seguridad es la condición de un "estado estable" de una empresa o lugar de hacer lo que se supone que debe hacer. "Lo que tiene que hacer" se define en términos de los códigos y las normas públicas, asociados arquitectónicos y diseños de ingeniería, la visión y misión corporativa, y de funcionamiento y las políticas de personal. Para cualquier empresa ya sea grande o pequeña, la seguridad es un concepto normativo. Cumple con las definiciones de la situación específica de lo que se espera.

La seguridad es generalmente interpretada en el sentido de un impacto real y significativo en el riesgo de muerte, lesiones o daños a la propiedad. En respuesta a los riesgos percibidos muchas intervenciones pueden ser propuestos con las respuestas de la ingeniería y la regulación son dos de los más comunes.

Probablemente, la respuesta individual más común de los problemas de seguridad que se percibe es de seguro que compensa o prevé la devolución en el caso de daño o pérdida.

La seguridad es la capacidad del sistema de proteger datos, servicios y recuersos de personas nos autorizados, la seguridad debe garantizar la protección de cualquier daño y que de cierta manera es infalible.

La seguridad de los sistemas de información es un valor particularmente estratégico, ya que, a través de los sistemas de control , sistemas de gestión, y en general a través de la ingeniería de sistemas , se debe abordar la interoperabilidad de los sistemas , y garantizar que la seguridad se logra a través de normas y estándares para la descripción de las estructuras de datos.

La seguridad se puede evaluar de acuerdo a varios criterios:

Disponibilidad: asegurar que estos elementos se consideran accesibles cuando sea necesario por las personas autorizadas.

Integridad: la seguridad de que el tema sea exacta y completa.

Confidencialidad: garantizar que sólo las personas autorizadas tengan acceso al material.

Otros aspectos que posiblemente pueden ser considerados como criterios (a pesar de que hace las funciones de seguridad), tales como:

Trazabilidad (o " prueba "): asegurar que los intentos de acceso y el acceso se registran en los elementos considerados y de que esos restos se conservan y explotados.

Una vez que los elementos sensibles, el riesgo de cada uno de estos elementos se puede estimar sobre la base de la amenaza que enfrentan los elementos a proteger. Esto implica la estimación:

La gravedad de los impactos que el riesgo se materializa,

La probabilidad de riesgo (o potencial, o la probabilidad de ocurrencia).

En el método EBIOS , estos niveles representan el nivel de cada riesgo que les permite evaluar (comparar).

En el Mehari método, el producto del impacto y el potencial que se llama "la gravedad". Otros métodos utilizan el concepto de "nivel de riesgo" o "grado de riesgo."

Elementos que pueden ser amenazas a un sistema son:

- Personas
  - ✓ Pasivos: aquellos que husmean por el sistema pero no lo modifican/ destruyen.
  - ✓ Activos: aquellos que dañan el objetivo atacado o lo modifican en su favor.

    Describiremos algunos de ataques que realizan las personas:
    - ✓ Personal
    - ✓ Ex-empleados
    - ✓ Curiosos
    - ✓ Hackers
    - ✓ Terroristas

- Amenazas Lógicas
  - ✓ Software incorrecto
  - ✓ Herramientas de seguridad
  - ✓ Puertas traseras
  - ✓ Canales cubiertos
  - ✓ Virus
  - ✓ Gusanos
  - ✓ Caballos de Troya

NORMAS DE SEGURIDAD

Se refieren al conjunto de reglas e instrucciones detalladas a seguir para la realización de una labor segura, las precauciones a tomar y las defensas a utilizar de modo que las operaciones se realicen sin riesgo, o al menos con el mínimo posible, para el trabajador que la ejecuta o para la comunidad laboral en general. Estas deben promulgarse y difundirse desde el momento de la inducción o reinducción del trabajador al puesto de trabajo, con el fin de evitar daños que puedan derivarse como consecuencia de la ejecución de un trabajo. Por lo tanto se deben hacer controles de ingeniería que sirven para rediseñar los procesos, la buena distribución de los puestos de trabajo y procurar instalaciones adecuadas.

En la realización de los trabajos pueden concurrir una gran variedad de posibles situaciones y circunstancias que las reglamentaciones oficiales no pueden abarcar. Lo que hace que la normativa legal, en muchos casos, es regular de manera general, ya que no puede descender a las condiciones de trabajo concretas que se dan en cada industria, o en cada puesto de trabajo en particular.

CONCEPTO DE NORMA DE SEGURIDAD.

Para la realización de cualquier trabajo que puede entrañar riesgo existen recomendaciones preventivas. Cuando estas son recogidas formalmente en un documento interno que indica una manera obligada de actuar, tenemos las normas de seguridad.

Las normas de seguridad van dirigidas a prevenir directamente los riesgos que puedan provocar accidentes de trabajo, interpretando y adaptando a cada necesidad las disposiciones y medidas que contienen la reglamentación oficial. Son directrices, órdenes, instrucciones y consignas, que instruyen al personal que trabajan en una empresa sobre los riesgos que pueden presentarse en el desarrollo de una actividad y la forma de prevenirlos mediante actuaciones seguras.

Se puede definir también la **NORMA DE SEGURIDAD** como la regla que resulta necesario promulgar y difundir con la anticipación adecuada y que debe seguirse para evitar los daños que puedan derivarse como consecuencia de la ejecución de un trabajo.

Las normas no deben sustituir a otras medidas preventivas prioritarias para eliminar riesgos en las instalaciones, debiendo tener en tal sentido un carácter complementario.

SEGURIDAD DE INFORMACIÓN

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{RIESGO} = \frac{\text{AMENAZA} \quad X \quad \text{VULNERABILIDAD}}{\text{CONTRAMEDIDA}}$$

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como falencias (flaws) o brechas (breaches)) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo. Por tanto, el objetivo de este informe es brindar una perspectiva general de las posibles motivaciones de los hackers, categorizarlas, y dar una idea de cómo funciona para conocer la mejor forma de reducir el riesgo de intrusiones.

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

Integridad: Garantizar que los datos sean los que se supone que son.

Confidencialidad: Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.

Disponibilidad: Garantizar el correcto funcionamiento de los sistemas de información.

Evitar el rechazo: Garantizar de que no pueda negar una operación realizada.

Autenticación: Asegurar que sólo los individuos autorizados tengan acceso a los recursos.

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente, la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias.

Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.

Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan.

Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de

acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Es más, dado que el/la administrador/a es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concientización. Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados.

Un procedimiento para administrar las actualizaciones.

Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente.

Un plan de recuperación luego de un incidente.

Un sistema documentado actualizado.

SEGURIDAD EN BASE DE DATOS

El objetivo principal es de proteger la base de datos de ataques maliciosos, sean estos internos o externos.

La causa por lo que se producen los errores en la seguridad de base de datos aun con el avance tecnológico tiende a producirse por la falla de procedimientos sencillos que a pasar el tiempo se convierten en grandes inconvenientes que afectan en lo concerniente a la seguridad, todo tiene que quedar de acuerdo con lo planteado sin ninguna omisión por más mínima que sea, así como en la instalación, en el diseño o en el desarrollo, cualquier punto que se deje sin la preocupación debida que no puede afectar en nada puede ser la entrada para los ataques.

Un caso en que ponemos ponerlo a la vista es cuando un administrador de sistema o redes no se preocupe por técnica de seguridad porque asume que el desarrollo de una aplicación Web ya se ha encargado de este proceso y a su vez el desarrollo piensa lo mismo por parte del administrador del sistema. En cambio el administrador de base de dato estará más preocupado por el correcto funcionamiento del servicio de la base de datos.

Se puede determinar que el problema de seguridad se produce principalmente por la falta de preocupación en primer lugar de la empresa, luego de la ausencia de

comunicación entre los encargados de cada proceso y por último la falla de capacitación o conocimiento sobre las técnicas de seguridad

NORMALIZACIONES

ISO

ISO es el acrónimo de International Organization for Standardization. Aunque si se observan las iniciales para el acrónimo, el nombre debería ser IOS, los fundadores decidieron que fuera ISO, derivado del griego "*isos"*, que significa "igual". Por lo tanto, en cualquier país o en cualquier idioma, el nombre de la institución es ISO, y no cambia de acuerdo a la traducción de "International Organization for Standardization" que corresponda a cada idioma. Se trata de la organización desarrolladora y publicadora de Estándares Internacionales más grande en el mundo. ISO es una red de instituciones de estándares nacionales de 157 países, donde hay un miembro por país, con una Secretaría Central en Geneva, Suiza, que es la que coordina el sistema.

ISO es una organización no gubernamental que forma un puente entre los sectores públicos y privados.

Respecto al origen de la organización ISO, oficialmente comenzó sus operaciones el 23 de febrero de 1947 en Geneva, Suiza. Nació con

el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

IEC

IEC es el acrónimo de International Electrotechnical Commission. Esta es una organización sin fines de lucro y también no gubernamental. Se ocupa de preparar y publicar estándares internacionales para todas las tecnologías eléctricas o relacionadas a la electrónica.

IEC nace en 1906 en London, Reino Unido, y desde entonces ha estado proporcionando estándares globales a las industrias electrotécnicas mundiales. Aunque como se acaba de decir, IEC nació en el Reino Unido, en el año de 1948 movieron su sede a Geneva, Suiza, ciudad en la que también se encuentra la sede de ISO.

ISO/IEC JTC1

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de la información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información. Dicho subcomité ha venido desarrollando una familia de Estándares Internacionales para el

Sistema Gestión y Seguridad de la Información. La familia incluye Estándares Internacionales sobre requerimientos, gestión de riesgos, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. Esta familia adoptó el esquema de numeración utilizando las series del número 27000 en secuencia, por lo que a partir de julio de 2007, las nuevas ediciones del ISO/IEC 17799 se encuentran bajo el esquema de numeración con el nombre ISO/IEC 27002.

COBIT

Marco de referencia para objetivos de control sobre la información y recursos tecnológicos asociados. Cobit fue creado por ISACA (Information System Control Standard) la cual es una organización sin ánimo de lucro enfocada en el Gobierno y control de IT. La función principal de CobiT es ayudar a las Organizaciones a mapear sus procesos de acuerdo a las mejores prácticas recopiladas por ISACA. Cobit usualmente es implementado por compañías que realizan auditorías de sistemas de información, ya sea relacionadas con la auditoría financiera o auditoría de TI en general.

ITIL

Marco de referencia para Infraestructura de Tecnologías de Información. ITIL fue creado por la OGC (Office of Government Commerce), y es un marco de referencia para gestionar los diferentes niveles de servicios IT. Aunque ITIL es

similar a CobiT en muchos aspectos, CobiT se enfoca en los procesos base y en riesgos, mientras que ITIL se enfoca en los servicios IT.

ISO 27000

Estándar enfocado exclusivamente en la seguridad, lo cual le hace muy diferente a los estándares manejados por CobiT o ITIL. Esta diferencia hace que la ISO 27000 tenga un alcance menor pero más profundo en el tema obviamente de seguridad comparándole con ITIL o CobiT.

NORMALIZACIÓN Y NORMAS ISO

La estructura de las sociedades y del comercio a nivel mundial, ha planteado a lo largo de su historia la necesidad del mejoramiento continuo en lo referente a los productos, bienes de servicios, que tienen un destino común cual es la inmensa cantidad de consumidores. Esta necesidad se basa primordialmente en lo referente al mejoramiento de los procesos tecnológicos y productivos, con la finalidad de optimizar los recursos disponibles, que pueden ser materiales, equipos y maquinaria, humanos.

El instrumento fundamental para lleva a cabo estas políticas, es la creación de una nueva estructura organizativa a nivel internacional, cuyo fin principal es la adopción de la cultura empresarial dedicada al cumplimiento de la normalización y su finalidad es la de homogenizar la producción, para hacer de los estándares de calidad una filosofía en todas las organizaciones productivas.

1. · NORMALIZACIÓN.-

La normalización hoy en día juega un papel importante en la mayoría de las actividades de los seres humanos, en el campo del sector privado es un soporte muy efectivo al impulsar a constituir estándares internacionales de calidad, a nivel público o estatal su desempeño es de vital importancia al dotar al estado de suficientes instrumentos de control en las políticas relacionadas con el medioambiente, la salud, la agricultura y particularmente el sector dé los consumidores.

Por normalización se entiende el proceso de formulación, elaboración, la aplicación y mejoramiento de las normas existentes que se aplican a las diversas actividades económicas, industriales o científicas, con el objeto de ordenarlas y mejorarlas. Los propósitos principales de la normalización son la simplificación, la unificación y la especificación.

1.1.- RESEÑA HISTÓRICA.- Por los años de 1906 se inicia la normalización internacional en el campo de la electrotecnia, mediante la creación de la lnternational Electrotechnique Committee (IEC), Comisión Internacional de Electrotécnica. Posteriormente en 1926 se crea la Intemational Standardization Associates (ISA), Federación Internacional de Asociaciones Nacionales de Normalización, pero fue disuelta en 1942 por la amenaza de guerra circundante en Europa.

El 14 de octubre de 1948 se reunieron en Londres los sesenta y cuatro (64) delegados de veinticinco (25) países, con la finalidad de crear una nueva organización de normalización con carácter internacional, creando la International Organization for Standardization (ISO), Organización Internacional de Normalización. La palabra ISO no es un acrónimo de su nombre en ingles, proviene de la raíz griega ισο (iso), que significa igual, razón suficiente para que los fundadores de la organización escogieran su nombre para ser utilizado universalmente.

1.1.1.- ORGANISMOS DE NORMALIZACION INTERNACIONAL.- Los organismos encargados de la Normalización Internacional son los siguientes:

- ASME (American Society of Mechanical Engineers): Sociedad Americana de Ingenieros Mecánicos.
- CEE: Comisión de reglamentación para Equipos Eléctricos.
- CENELEC (Comité Européen de Normalisation Electrotechnique): Comité Européo de Normalización Electrotécnica.
- COPANT: Comisión Panamericana de Normas Técnicas.
- EURONORM: Organismo de normalización de la Comunidad Europea.

- IEC (Internacional Electrotechnical Comisión): Comisión Internacional de Electrotécnica.
- ISO (Internacional Organization for Standardization): Organización Internacional de Normalización.
- ITU (Internacional Telecomunications United): Unión Internacional de Telecomunicaciones.

1.2.- LA ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN.- La ISO es un organismo internacional compuesta por los representantes de los cuerpos normativos nacionales (Organismos de Normalización), compuesta por noventa (90) países, con un perfil administrativo de carácter no gubernamental. Esta federación de representantes nacionales actúa con oficinas delegadas de la ISO y son las encargadas de la normalización en cada país, en la Tabla No. 1 se presentan algunos Organismos Nacionales de Normalización.

La ISO es un órgano consultivo de la Organización de las Naciones Unidas (ONU), que tiene su sede en Ginebra (Suiza), cuya función principal es la de contribuir al fomento y desarrollo internacional de la normalización, para facilitar el intercambio mundial de productos, bienes y servicios, mediante la colaboración científica, tecnológica y técnica en el campo administrativo,

industrial y económico, manteniendo La ISO contacto con las universidades, centros científicos y tecnológicos.

TABLA No. 1

ORGANISMOS NACIONALES DE NORMALIZACIÓN

PAÍS	**ORGANISMO**	**PAGINA WEB**
Alemania	Deutsches Institut für Normung - DIN	www2.din.de
Argentina	Instituto Argentino de Normalización - IRAM	www.iram.com.ar
Bolivia	Instituto Boliviano de Normalización y Calidad - IBNORCA	www.ibnorca.org
Chile	Instituto Nacional de Normalización - INN	www.inn.cl
Colombia	Instituto Colombiano de Normas Técnicas - ICONTEC	www.icontec.org.co
Costa Rica	Instituto de Normas Técnicas de Costa Rica - INTECO	www.inteco.or.cr
Cuba	Oficina Nacional de Normalización - NC	www.nc.cubaindustria.cu
Ecuador	Instituto Ecuatoriano de Normalización - INEN	www.inen.gob.ec
El Salvador	Consejo Nacional de Ciencia y Tecnología - CONACYT	www.conacyt.gob.sv
España	Asociación Española de Normalización y Certificación - AENOR	www.aenor.es
Estados Unidos	American Nacional Standards Institute - ANSI	www.ansi.org
Filipinas	Bureau of Product Standards - BPS	www.dti.gov.ph/bps
Francia	Association Française de Normalisation - AFNOR	www.afnor.fr/portail/asp
Guatemala	Comisión Guatemalteca de Normas - COGUANOR	www.mineco.gob.gt
Honduras	Consejo Hondureño de Ciencia y Tecnología - COHCIT	www.cohcit.gob.hn

México	Dirección General de Normas - DGN	www.economia-normas.gob.mx
Nicaragua	Dirección de Tecnología, Normalización y Metrología - DTNM	www.mific.gob.ni
Panamá	Comisión Panameña de Normas Industriales y Técnicas - COPANIT	www.mici.gob.pa
Paraguay	Instituto Nacional de Tecnología y Normalización - INTN	www.intn.gob.py
Perú	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI	www.indecopi.gob.pe
Reino Unido	British Standards Institute - BS	www.bsi-global.com/index.xalter
Republica Dominicana	Dirección General de Normas y Sistemas de Calidad - DIGENOR	www.seic.gov.do/digenor/default.htm
Rusia	Agencia Federal para la Regulación Técnica y la Metrología - GOST	www.gost.ru/wps/portal
Suiza	Swiss Association for Standardization - SNV	www.snv.ch
Uruguay	Instituto Uruguayo de Normas Técnicas - UNIT	www.unit.org.uy
Venezuela	Fondo para la Normalización y Certificación de la Calidad - FONDONORMA	www.fondonorma.org.ve

Fuente: Monografias.com

1.2.1.- CLASES DE MIEMBROS DE LA ISO.- Este organismo lo componen tres clases de miembros:

- MIEMBROS NATOS.- Es la representación unitaria de los Organismos Nacionales de Normalización de cada país, con derecho a voz y voto.
- MIEMBROS CORRESPONDIENTES.- Es la representación de los países en vías de desarrollo y que no poseen un comité nacional de normalización, no conforman la parte activa en el proceso de

normalización pero se encuentran permanentemente informados acerca de todos los procesos en desarrollo.

- MIEMBROS SUSCRITOS.- Lo conforman los países con reducidas economías, que contribuyen con unas tasas menores de pago.

1.2.2.- ESTRUCTURA INTERNA DE LA ISO.- Su estructura interna está compuesta por un Consejo de la Organización encargado de la aprobación de los proyectos de normas, subordinados a éste se han creado ciento setenta y seis (176) comités permanentes llamados Comités Técnicos ISO (ISO/TC) cuya función es la de estudiar los principios científicos de la normalización, a cada Comité Técnico se le adjudica un número de orden y un nombre que refleja el perfil y la especialización a que se dedica.

En los comités técnicos se encuentran subordinados seis cientos treinta y un (631) Subcomités Técnicos (ISO/TCSC) creados según la especialización específica de cada disciplina, estos subcomités están divididos en mil ochocientos treinta (1 830) Grupos de Trabajo de acuerdo a cada especialidad.

En los Comités y Subcomités Técnicos tienen asiento cada uno de los países que conforman esta organización, y representan el punto de vista de los fabricantes, vendedores, profesionales de la ingeniería, laboratorios de pruebas, servicios públicos, gobierno, organizaciones científicas de investigación, grupos de usuarios y consumidores, en todo el mundo.

1.2.3.- FUNCIONES Y OBJETIVOS.- Las funciones y objetivos de la ISO son las siguientes:

- La elaboración, discusión y presentación de los proyectos de normas técnicas internacionales.
- Facilitar la utilización de las nuevas normas para ser empleadas internacionalmente y en la esfera local de. cada nación.
- Coordinar para los países miembros as recomendaciones necesarias para la unificación de criterios de las normas ISO nacionales en cada país.
- Elaboración de las normas internacionales con el apoyo, participación y aceptación de todos sus miembros.
- Colaborar activamente con organizaciones internacionales dedicadas a la promulgación de la normalización.

NORMALIZACION DE BASE DE DATOS

El proceso de **normalización de bases de datos** consiste en aplicar una serie de reglas a las relaciones obtenidas tras el paso del modelo entidad-relación al modelo relacional.

Las bases de datos relacionales se normalizan para:

- Evitar la redundancia de los datos.

- Evitar problemas de actualización de los datos en las tablas.
- Proteger la integridad de los datos.

En el modelo relacional es frecuente llamar *tabla* a una relación, aunque para que una tabla sea considerada como una relación tiene que cumplir con algunas restricciones:

- Cada tabla debe tener su nombre único.
- No puede haber dos filas iguales. No se permiten los duplicados.
- Todos los datos en una columna deben ser del mismo tipo.
- Relación = tabla o archivo.
- Registro = registro, fila, renglón o tupla.
- Atributo = columna o campo.
- Clave = llave o código de identificación.
- Clave Candidata = superclave mínima.
- Clave Primaria = clave candidata elegida.
- Clave Ajena (o foránea) = clave externa o clave foránea.
- Clave Alternativa = clave secundaria.
- Dependencia Multivaluada = dependencia multivalor.
- RDBMS = Del inglés *Relational Data Base Manager System* que significa, *Sistema Gestor de Bases de Datos Relacionales*.

- 1FN = Significa, *Primera Forma Normal* o 1NF del inglés *First Normal Form*.

Los términos Relación, Tupla y Atributo derivan del álgebra y cálculo relacional, que constituyen la fuente teórica del modelo de base de datos relacional.

Todo atributo en una tabla tiene un dominio, el cual representa el conjunto de valores que el mismo puede tomar. Una instancia de una tabla puede verse entonces como un subconjunto del producto cartesiano entre los dominios de los atributos. Sin embargo, suele haber algunas diferencias con la analogía matemática, ya que algunos RDBMS permiten filas duplicadas, entre otras cosas. Finalmente, una tupla puede razonarse matemáticamente como un elemento del producto cartesiano entre los dominio.

RIESGOS

La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra una perdida permanente de la información.

El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular (Peltier, 2001).

Aclaración del significado: Cuanto mayor es la vulnerabilidad mayor es el riesgo (e inversamente), pero cuanto más factible es el perjuicio o daño mayor es el

peligro (e inversamente). Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere sólo a la teórica "probabilidad de daño" bajo determinadas circunstancias. Por ejemplo, desde el punto de vista del riesgo de daños a la integridad física de las personas, cuanto mayor es la velocidad de circulación de un vehículo en carretera mayor es el "riesgo de daño" para sus ocupantes, mientras que cuanto mayor es la imprudencia al conducir mayor es el "peligro de accidente" (y también es mayor el riesgo del daño consecuente).

ANÁLISIS DE LOS RIESGOS

La etapa de análisis de riesgos consiste en detallar los diferentes riesgos que se advierten en la forma como se manipula la de información dentro de las empresas, estimando sus probabilidades de ocurrencia y, por último, analizar su impacto mediante la valoración y aplicación las clausulas de la norma ISO27002.

Una de las formas de analizar el impacto de una amenaza consiste en estimar los daños que se podrían dar por falta de seguridad de información normalizada (por ejemplo, un ataque a un servidor o un daño y/o perdida de los datos de vital importancia de la compañía).

Partiendo de esta base, se debe elaborar una tabla donde contenga los riesgos (incumplimiento de clausulas y controles) y sus potencialidades (es decir, la

probabilidad de que existan) dándoles niveles de calificación que en nuestro caso esta determinado en procesos de la norma.

RIESGOS DE LA INFORMACIÓN DE LAS BASES DE DATOS

Cuando nuestros datos son almacenados en bases de datos, con independencia de que sean bases del Estado o privadas, siempre surgen riesgos:

- Riesgo de que sean utilizados comercialmente para beneficio ajeno y encima seamos molestados con publicidad a nuestro nombre.
- Riesgo de uso delictivo para estafas bancarias, suplantación de identidad, chantaje, secuestro por mafias.
- Riesgo de que sean utilizados en nuestra contra por la policía o servicios de inteligencia que nunca tendrán suficiente control democrático y riesgo de su utilización por un futuro gobierno antidemocrático.

A la hora de ceder nuestros datos tenemos que tener muy claro que nunca tendremos la seguridad total de a donde acabarán yendo a parar, ni para qué acabarán siendo utilizados, por lo que siempre hay un riesgo potencial que nos obliga a valorar suficientemente si con ello obtenemos algún beneficio que nos compense y si podemos recuperar su control. Esto no debe volvernos paranoicos pero si prudentes.

Los datos que damos pueden ser robados o vendidos por un funcionario o

empleado infiel o ser utilizados con una finalidad diferente. Cuando entregamos nuestros datos nos han de ofrecer suficiente confianza de que serán tratados en nuestro beneficio y almacenados con suficiente seguridad. La tecnología moderna facilita la suplantación electrónica de nuestra identidad, también la difusión de información perjudicial.

EVALUACIÓN DE RIESGOS

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos, y por ello han surgido una multitud de guías informales, aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están dichos activos y no llamarse a engaño (MAGERIT, 2005).

Entre las múltiples metodologías y estándares que han surgido para manejar la seguridad se pueden mencionar: ISO 27001:2005, SEE_CMM, Cobit, ITIL, ISM3, entre otros. Sin embargo, se requiere incorporar los cambios necesarios para que se ajusten a los requerimientos particulares de cada empresa.

En los actuales momentos la norma ISO 27001:2007, presenta un compendio que proporciona una base común para la elaboración de reglas, un método de gestión eficaz de la seguridad y permite establecer informes de confianza en las transacciones y las relaciones entre empresas. La norma ha sido publicada en dos partes:

- ISO/IEC 27002:2007: Código de buenas prácticas para la Gestión de la seguridad de la información;
- ISO/IEC 27001:2007 - BS 7799 Parte 2: Especificaciones relativas a la gestión de la seguridad de la información.

Lo relacionado con la gestión del riesgo es una parte esencial del ISO 27001:2007. En el Anexo A de esta norma se propone una tabla detallada de los controles (Alexander, 2007), controles que deben ser seleccionados en base a los resultados de la evaluación del riesgo y a las decisiones tomadas concernientes al tratamiento de dicho riesgo.

La gestión del riesgo, generalmente, contempla el cálculo del riesgo, la apreciación de su impacto en el negocio y la probabilidad de ocurrencia (Hiles, 2004). Luego se derivan pasos para reducir la frecuencia a un nivel considerado aceptable.

Si la empresa no conoce sobre el riesgo que corren sus activos de información, difícilmente llegará a estar preparada para evitar su posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminar su posible ocurrencia.

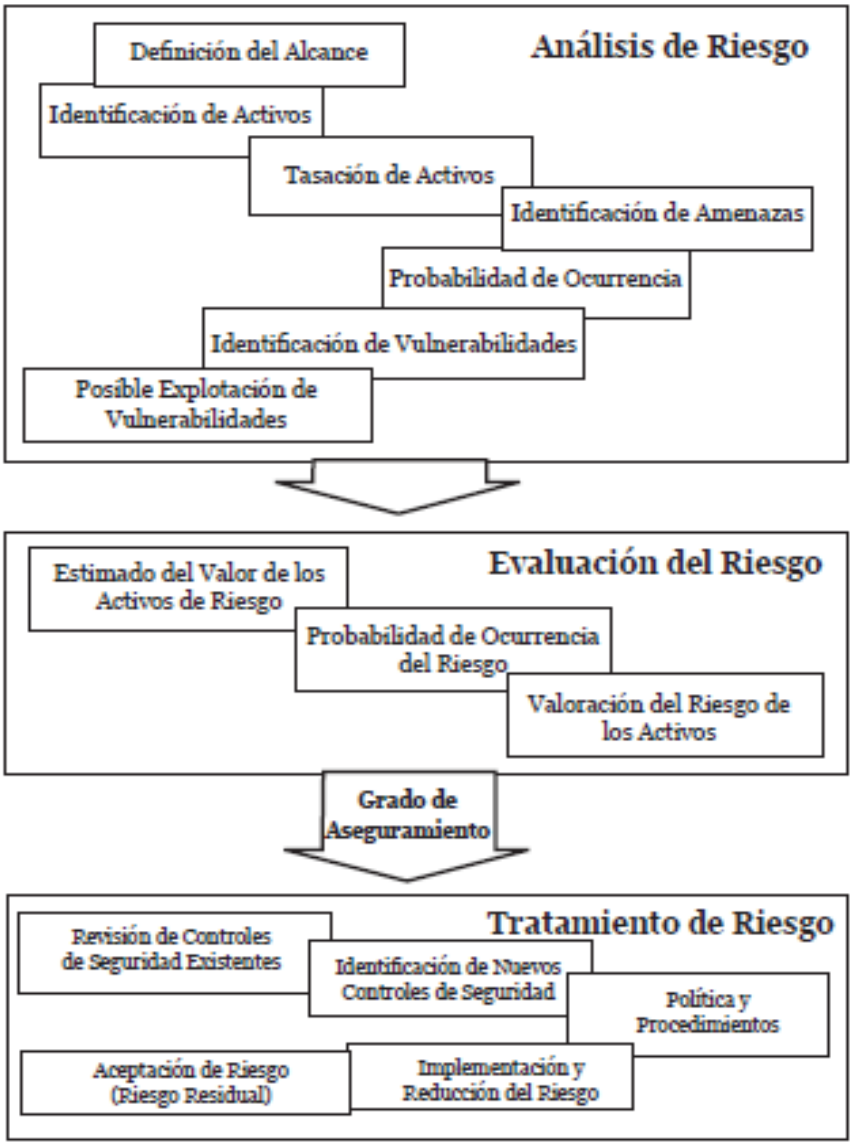
La ISO 27001:2007 recomienda para llevar a cabo una gestión de riesgo, que se defina primero el alcance del estándar en la empresa, y con base en ello, identificar todos los activos de información.

Los activos de información deben ser tasados para identificar su impacto en la organización.

Luego se debe realizar un análisis para determinar qué activos están bajo riesgo. Es en ese momento que se deben tomar decisiones en relación a qué riesgos aceptará la organización y qué controles serán implantados para mitigar el riesgo (Alberts y Dorofee, 2003). A la gerencia le corresponde revisar los controles implantados a intervalos de tiempo regular para asegurar su adecuación y eficacia. Se le exige a la gerencia que controle los niveles de riesgos aceptados y el estado del riesgo residual (que es el riesgo que queda después del tratamiento del riesgo). El objetivo final de la evaluación de riesgos es realizar un cálculo de las amenazas a los activos de información, con vistas a seleccionar los controles ISO 27002:2007 o ISO 17799:2005 adecuados para mitigar ese riesgo.

Después de revisar los diferentes métodos, metodologías y herramientas existentes, la Revista Venezolana de Información, Tecnología y Conocimiento Año 6: No. 1, Enero-Abril 2009, se propone el esquema que se puede observar en la Figura 1 para llevar a cabo el mencionado análisis y evaluar su riesgo.

Figura 1
Esquema del Análisis y Evaluación de Riesgo



FUNDAMENTACIÓN LEGAL

LEY DEL SISTEMA NACIONAL DE REGISTROS DE DATOS PÚBLICOS

Artículo 5.- Responsabilidad de la información.- El Estado es responsable de la administración y control de los registros y bases de datos públicos. Los funcionarios a cargo del manejo de los registros responderán por la veracidad, autenticidad y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva del declarante cuando éste provee toda la información.

Sin perjuicio del derecho de repetición, los registradores de datos públicos indemnizarán a quienes sufran daños o lesiones en sus derechos o bienes, como consecuencia de un manejo negligente o doloso de la información que genere falsedad o imprecisión de la información que difundan y certifiquen.

Articulo 25.- Sistema Informático.- El sistema informático tiene como objetivo la tecnificación y modernización de los registros empleando tecnologías de información, bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive, codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados.

El sistema informático utilizado para el funcionamiento e interconexión de los registros y entidades, es de propiedad estatal y del mismo se podrán conceder licencias de uso limitadas a las entidades, oficinas y personas que correspondan, de acuerdo a lo establecido en el Reglamento.

Articulo 26.- Interconexión.- Para la debida implementación del sistema de control cruzado nacional, los registros y bases de datos deberán obligatoriamente interconectarse buscando la simplificación de procesos y el debido control de la información de las instituciones competentes.

Artículo 27.- Información física y digital.- Sin perjuicio de llevar la información con soporte físico como determina la Ley de Registro y reglamentos aplicables, los registros cantonales deberán llevar la información, como regla general, de manera digitalizada para efectos de la sistematización e interconexión del registro de datos.

La Dirección Nacional de Registros de Datos Públicos proporcionará los sistemas informáticos necesarios para la administración de los registros y las bases de datos, sistema informático único a ser utilizado en todos los registros cantonales del país.

Artículo 28.- Seguridad. Toda base informática de datos debe contar con su respectivo respaldo y mantener estándares técnicos que permitan la continuidad del sistema informático y la protección de los datos.

Ley 83 de Propiedad Intelectual, de 1998

Artículo 10. El derecho de autor protege también la forma de expresión mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas a las obras.

(…) Protección de datos:

La doctrina utiliza la expresión "protección de datos" en lo referente a la protección jurídica de la persona frente a la tecnología que automatiza sus datos. Pero que es lo que se protege, al respecto la mayoría de autores coinciden en los siguientes aspectos:

Proteger al individuo ante el "manejo o manipulación, no autorizada, de sus datos personales" que se encuentren en medios o formas electrónicas.

Los resultados de procesamientos informáticos, "deben ser identificable con el titular de los mismos" puesto que es muy fácil conocer características de la personalidad y de la intimidad de las personas.

Y, por último, el consentimiento no autorizado del uso de los datos, para fines en los que el titular no autorizo o fue obligado a darlos.

SEGÚN LA CONSTITUCIÓN DEL ECUADOR:

Artículo. 349. El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo.

Art. 386. Será responsabilidad del Estado:

Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kausay.

Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

Reconocer la condición de investigador de acuerdo a la Ley.

SEGÚN EL REGLAMENTO DE LA INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA DE LA UNIVERSIDAD DE GUAYAQUIL:

Artículo. 1.- Los objetivos de la investigación en la Universidad de Guayaquil están concebidos como parte de un proceso de enseñanza único, de carácter docente investigativo, orientado según norma el Estatuto Orgánico, para permitir el conocimiento de la realidad nacional y la creación de ciencia y tecnología, capaces de dar solución a los problemas del país. Las investigaciones dirigidas a la comunidad tienen por finalidad estimular las manifestaciones de la cultura popular, mejorar las condiciones intelectuales de los sectores que no han tenido acceso a la educación superior; la orientación del pueblo frente a los problemas que lo afectan; y la prestación de servicios, asesoría técnica y colaboración en los planes y proyectos destinados a mejorar las condiciones de vida de la comunidad.

Artículo 14.- Las unidades académicas son responsables de la labor investigativa de sus Profesores (as) e Investigadores (as), y trabajarán por lograr la mayor integración posible de los proyectos de investigación a las necesidades del desarrollo científico y metodológico del pregrado y el posgrado, y a los fines de la formación integral y profesional de sus docentes y alumnos.

SEGÚN LA LEY DE EDUCACIÓN SUPERIOR:

Artículo 3.- Las instituciones del Sistema Nacional de Educación Superior ecuatoriano, en sus diferentes niveles, tienen los siguientes objetivos y Estrategias fundamentales:

Desarrollar sus actividades de investigación científica en armonía con la legislación nacional de ciencia y tecnología y la Ley de Propiedad Intelectual.

Artículo 80.- El Estado fomentará la ciencia y la tecnología, especialmente en todos los niveles educativos, dirigidos a mejorar la productividad, la competitividad, el manejo sustentable de los recursos naturales y a satisfacer las necesidades básicas de la población. La investigación científica y tecnológica se llevará a cabo en las universidades, escuelas politécnicas, institutos superiores técnicos y tecnológicos y centros de investigación científica, en coordinación con los sectores productivos cuando sea pertinente, y con el organismo público que establezca la ley, la que regulará también el estatuto del investigador científico.

HIPÓTESIS PREGUNTAS A CONTESTARSE

El cumplimiento de normas de seguridad de la información logra aumentar los estándares de calidad con lo cual se aumenta continuamente la satisfacción de la empresa y sus clientes, logrando el crecimiento de la empresa.

Los riesgos de robo y/o pérdida de información disminuyen cuando se aplican normas de seguridad.

VARIABLES DE LA INVESTIGACIÓN

Variable Independiente: Cumplimiento de las normas de seguridad de las bases de datos (en su actualidad).

Variable Dependiente: El efecto en el riesgo que causa la seguridad de la información de las empresas de Guayaquil.

Variable Dependiente: Propuesta para reducir el riesgo asociado al uso de bases de datos que no cumplen con las normas de seguridad.

DEFINICIONES CONCEPTUALES

POLITICAS

El concepto de políticas según Víctor Manuel Gonzales P. es: **"Lineamientos generales que orienten las actividades que habrán de realizar los trabajadores involucrados en sus aéreas de trabajo. Precisando de antemano la mayor parte de las situaciones que pudieran presentarse o que propicien la toma de decisiones de las autoridades superiores.**

Está definido como la acción de establecer planes de contingencia frente algún problema, es un conjunto de requisitos definidos por los responsables de un área,

sistema de información, etc., indicando en términos generales que esta y que no está permitido hacer, como se debe hacer.

Una política puede prohibir o permitir acceder, elaborar, adjudicar, etc., contemplando los siguientes elementos clave de un sistema informático.

Debe brindar beneficios a los recursos del sistema y la información que se maneja.

Autenticidad: Es la adecuación entre lo que se piensa, dice, hace y lo que se debe hacer, frente a un problema.

Posesión: Debe ser aprobado y legalizado por las entidades pertinentes, además que deben ser capaces de controlar en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Existen estándares para elaborar políticas de seguridad pero eso no garantiza que tu sistema sea 100% seguro, estos estándares en algunos casos son el aval de las empresas para ofrecer algún producto o servicio al mercado.

Las políticas según José Manuel Ajhuacho Vargas **“Las políticas de seguridad por lo general están en base a un análisis de riesgo al que está expuesto la empresa o el sistema, basándose en lo siguiente**

¿Que proteger?

¿De qué o quien proteger?

¿Cómo proteger? ”

NORMAS

Lineamientos imperativos y específicos de acción que persiguen un fin determinado con mayor obligatoriedad en sus interpretaciones y aplicación.

Víctor González Peláez nos dice **“Las Políticas y normas deberán de elaborarse clara y concisamente a fin de que sean comprendidas incluso por aquellas personas no familiarizadas con los aspectos administrativos o con el procedimiento mismo.”**

Es la documentación de las políticas de seguridad, previa aprobación de las entidades correspondientes además competentes al área jurídica, aplicándolo y haciendo cumplir dichas políticas.

Las normas de carácter general, son universalmente aceptadas y las normas de carácter específico son las que regulan una función, trabajo u operación específica, representando un elemento de sistematización de seguridad, facilitando la comprensión y ejecución de las tareas de seguridad de forma clara y precisa.

José Manuel Ajhuacho Vargas manifiesta que **“Permite la dirección eficaz del sistema de seguridad, impiden que existan vacíos acerca de la seguridad, facilitan la rápida formación y concientización del personal, permiten un**

manejo excelente de las instalaciones y equipos, homogenizan medios y procedimientos, además de facilitar la comunicación y la seguridad, aumentan el sentido de seguridad en el usuario"

SEGURIDAD

La seguridad según Gonzalo Álvarez Marañón y Pedro Pablo Fábrega Martínez es: "un proceso continuo, que requiere tener previsto hasta lo imprevisible."

NORMAS DE SEGURIDAD

Se entiende por Norma a una regla a la que se debe ajustar la puesta en marcha de una operación. También se puede definir como una guía de actuación por seguir o como un patrón de referencia.

Las normas de seguridad se pueden considerar prácticamente como:

a. Normas de carácter general: son las universalmente aceptadas.

b. Normas de carácter específico: las que regulan una función, trabajo u operación específica.

La Unidad de Gestión de Riesgos - Universidad Nacional de San Luis da a conocer las ventajas de las normas se reducen, entre otras, a lo siguiente:

• **Representan un elemento de sistematización de seguridad.**

• Facilitan la comprensión y ejecución de las tareas de seguridad de forma clara y precisa.

• Permiten la dirección eficaz del sistema de seguridad.

• Impiden que existan vacíos acerca de la seguridad.

• Facilitan la rápida formación y concientización del personal.

• Permiten un manejo excelente de las instalaciones y equipos.

• Homogenizan medio y procedimientos, además de facilitar la comunicación y la seguridad.

• Aumentan el sentido de seguridad en el usuario.

SEGURIDAD DE LA INFORMACIÓN:

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad de Integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

CAPÍTULO III

METODOLOGÍA

DISEÑO DE LA INVESTIGACIÓN

MODALIDAD DE LA INVESTIGACIÓN

Mi proyecto: "Cumplimiento de normas de seguridad de las bases de datos y su efecto en el riesgo de la información de las empresas de Guayaquil. Propuesta para reducir el riesgo de las bases de datos que no cumplen las normativas" tiene como modalidad la investigación de campo en un 30% y la investigación bibliográfica en un 70%.

INVESTIGACIÓN BIBLIOGRÁFICA

Constituye una excelente introducción a todos los otros tipos de investigación, además de que constituye una necesaria primera etapa de todas ellas, puesto que ésta proporciona el conocimiento de las investigaciones ya existentes, teorías, hipótesis, experimentos, resultados, instrumentos y técnicas usadas acerca del tema o problema que el investigador se propone investigar o resolver.

Se puede decir que un factor importante en este tipo de investigación es la utilización de la biblioteca y realizar búsquedas bibliográficas. La habilidad del investigador se demostrará en la cuidadosa indagación de un tema, de la habilidad

para escoger y evaluar materiales, de tomar notas claras bien documentadas y depende además de la presentación y el orden del desarrollo en consonancia con los propósitos del documento.

TIPO DE INVESTIGACIÓN

Para el desarrollo de este proceso de investigación se van a tomar en cuenta dos tipos lo que es la investigación explorativa y la descriptiva.

El tipo de investigación es explorativa ya que recoger e identificar antecedentes generales, números y cuantificaciones, temas y tópicos respecto del problema investigado, sugerencias de aspectos relacionados que deberían examinarse en profundidad en futuras investigaciones. Siendo el objetivo documentar ciertas experiencias, examinar temas o problemas poco estudiados o que no han sido abordadas antes. Por lo general investigan tendencias, identifican relaciones potenciales entre variables para investigaciones posteriores más rigurosas.

Los estudios exploratorios nos sirven para aumentar el grado de familiaridad con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular de la vida real, investigar problemas de comportamiento humano que consideren cruciales los profesionales de determinada área, identificar conceptos o variables promisorias, establecen prioridades para investigaciones posteriores o sugerir afirmaciones (postulados) verificables.

El tipo de investigación es descriptiva. Comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o procesos de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre como una persona, grupo o cosa se conduce o funciona en el presente.

La investigación descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentarnos una interpretación correcta.

La tarea de investigación en este tipo de investigación tiene las siguientes etapas:

Descripción del Problema.

Definición y Formulación de la Hipótesis.

Supuestos en que se basa la Hipótesis.

Marco Teórico.

Selección de Técnicas de Recolección de Datos.

Categorías de Datos, a fin de facilitar relaciones.

Verificación de validez del instrumento.

Descripción, Análisis e Interpretación de Datos.

POBLACIÓN Y MUESTRA

POBLACIÓN:

El desarrollo de esta investigación va dirigido a los fejes de departamento de cómputos o a los administradores de bases de datos.

Lo tomamos como muestra población es porque las personas mencionadas anteriormente son las responsables de salvaguarda a integridad de la información y datos que de asigna una empresa.

MUESTRA:

Una cuestión que uno puede plantearse es la relacionada con el tamaño idóneo de la población. Parece intuitivo que las poblaciones pequeñas corren el riesgo de no cubrir adecuadamente el espacio de búsqueda, mientras que el trabajar con poblaciones de gran tamaño puede acarrear problemas relacionados con el excesivo costo computacional.

La muestra se va a determinar para este estudio en la fórmula para aplicar:

$$n = \frac{m}{e^2 (m-1) + 1}$$

INTRODUCCIÓN.-

La muestra va a ser enfocada a ver en qué población va a ser efectuada el estudio la cual nos con lleva a saber que necesitamos o cuantas personas se va a identificar como necesarias para la investigación en ello vamos a saber el tamaña de nuestra población; así mismo el porcentaje de error que podemos tener en la aplicación de este muestreo buscando al fin el objetivo de saber de qué tamaño va hacer muestra.

TÍTULO – POBLACIÓN.-

A la población se la llamará “Autorizados de bases de datos”

DESCRIPCIÓN A LA (S) POBLACIÓN (S) QUE SERÁN UTILIZADAS EN LA INVESTIGACIÓN

Los “Autorizados de bases de datos” son personas responsables de los aspectos ambientales de una base de datos. En general esto incluye lo siguiente:

Recuperabilidad - Crear y probar Respaldos.

Integridad - Verificar o ayudar a la verificación en la integridad de datos.

Seguridad - Definir o implementar controles de acceso a los datos.

Disponibilidad - Asegurarse del mayor tiempo de encendido.

Desempeño - Asegurarse del máximo desempeño incluso con las limitaciones.

Desarrollo y soporte a pruebas - Ayudar a los programadores e ingenieros a utilizar eficientemente la base de datos.

El diseño lógico y físico de las bases de datos a pesar de no ser obligaciones de un administrador de bases de datos, es a veces parte del trabajo. Esas funciones por lo general están asignadas a los analistas de bases de datos o a los diseñadores de bases de datos.

Los deberes de un administrador de bases de datos dependen de la descripción del puesto, corporación y políticas de Tecnologías de Información (TI). Por lo general se incluye recuperación de desastres (respaldos y pruebas de respaldos), análisis de rendimiento y optimización, y cierta asistencia en el diseño de la base de datos.

Debe incorporarse una metodología basada en calidad y administración de riesgos al proceso de la administración de bases de datos.

La disponibilidad significa que los usuarios autorizados tengan acceso a los datos cuando lo necesiten para atender a las necesidades del negocio. De manera incremental los negocios han ido requiriendo que su información esté disponible todo el tiempo (7x24", o siete días a la semana, 24 horas del día). La industria de TI ha respondido a estas necesidades con redundancia de red y hardware para incrementar las capacidades administrativas en línea siempre y cuando estés en la administración de la TI.

CUADRO ESTADÍSTICO EN EL QUE CONSTE: LA POBLACIÓN Y SU NÚMERO DE ELEMENTOS TOTAL

POBLACIÓN DE autorizados de base de datos	N
Administrador de base de datos	52
Jefe de departamento de computo	25
TOTAL	77

TÍTULO – MUESTRA.

"Población de Base de datos"

INTRODUCCIÓN.

Para calcular la población vamos a utilizar la siguiente fórmula que no ayudara a saber cuál es el porcentaje de la población vamos a utilizar para el estudio

$$n = \frac{m}{e^2 (m-1) + 1}$$

m= Tamaño de la población (77)

E= error de estimación

(Valor constate para formula) (6%)

n = Tamaño de la muestra (60)

$$n = \frac{77}{(0.06)2(77-1)+1}$$

$$n = \frac{77}{(0.0036)\,(76)+1}$$

$$n = \frac{77}{0.2736+1}$$

$$n = \frac{77}{1.2736}$$

$$n = 60$$

Esto nos da que teniendo una población de 77 con un error de estimación del 6% demostrando que el tamaño de nuestra será de 60

OPERACIONALIZACIÓN DE VARIABLES

Variable Independiente: Cumplimiento de las normas de seguridad de las bases de datos (en su actualidad).

Variable Dependiente 1: El efecto del incumplimiento en la seguridad de información de las empresas de Guayaquil.

Variable Dependiente 2: Reducir el riesgo asociado al uso de bases de datos que no cumplen con dichas normas.

CUADRO No. 24

MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

Variables	Dimensiones	Indicadores	Técnicas y/o Instrumentos
V. I. Cumplimiento de las normas de seguridad	Normas 27001	Conocimiento de normas de seguridad 60%	Pruebas de cumplimiento

V.D. 1 Efecto en la seguridad de información	Confidencialidad Disponibilidad Recuperación Normas 27002	Aplicación de normas y políticas de seguridad 80%	Manuales de funciones del área de base de datos, consulta a expertos.
V.D. 2 Reducir el riesgo asociado al uso de bases de datos que no cumplen con dichas norma	Normas 27005	Metodología	Pruebas sustantivas

Elaboración: Sharon Estrada Rojas

Fuente: Sharon Estrada Rojas

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Las técnicas de recolección de datos para la investigación que se desarrollaron son el análisis del contenido de la información a investigar, la cual nos proporciona conocimientos y los resultados del análisis de contenido es con el objetivo de reproducirlos ya que son fiables, también se llegara a recolectar más datos de la investigación mediante libros, sitios web, información de ley.

Otra técnica que se utilizo es la de campo que se utilizó para y la encuesta sobre el tema a desarrollarse, ya que con esta técnica no se modifica el entorno, ya que se puede obtener también mayor rapidez en la obtención de resultados.

Los instrumentos que se utilizaron según la técnica antes mencionada es la de cuestionario ya que este es un documento básico de la encuesta para la obtención de información, ya que es un conjunto de preguntas que debe estar redactadas de forma coherente, y organizadas, secuenciadas y estructuradas de acuerdo con el objeto de la investigación, para así obtener las repuestas con toda la información precisa.

Para el cuestionario fue recomendable utilizar un lenguaje apropiado según el ambiente profesional que vamos a llegaban a cago la investigación, la cuales también tienen que ser claras y directas apuntando al tema netamente de la investigación para así obtener resultado eficientes.

INSTRUMENTOS DE LA INVESTIGACIÓN

De acuerdo a las técnicas mencionadas anteriormente, los instrumentos utilizados fueron, básicamente, fuentes bibliográficas en internet y un cuestionario corto y en conceptos básicos en libros.

Las bibliográficas consultadas son de varias fuentes, estas son artículos o capítulos de algún libro citado en internet y conceptos modernos de seguridad

informática, todos escritos por profesionales y expertos en su respectiva área como por ejemplo Sistemas de bases de datos: diseño, implementación y administración Escrito por Peter Rob, Carlos, y le paginas directas como las ISO2700 y Oracle, etc.

DETALLE DE LA ENCUESTA REALIZADA

Encuesta sobre las Normas de Seguridades de Bases de Datos

¿Conoce usted acerca de las normas de Seguridades de las bases de datos?

SI

NO

NO SABE

¿Se cumple las Normas de Seguridad en la empresa que labora?

SI

NO

NO SABE

¿Conoce en que ayuda a una empresa un Sistema de Gestión de Seguridad de la Información (SGSI)?

SI

NO

NO SABE

¿Qué base de datos utiliza la empresa?

ORACLE

SQLSERVER

MYSQL

INFORMIX

OTRAS _____

¿Existen políticas de seguridad en la empresa que labora?

SI

NO

NO SABE

¿Existe asignación de funciones y /o roles para el personal esta encargado de la información en la empresa?

SI

NO

NO SABE

¿A consideran como activos importantes en la empresa que labora?

EQUIPOS

PERSONAL

INFORMACIÓN

OTROS _____

¿Realizan respaldo de la información en la empresa que labora?

SI

NO

NO SABE

¿Que controles de seguridad tiene en la empresa que labora?

SEGURIDAD FÍSICA

SEGURIDAD AMBIENTAL

MANTENIMIENTOS Y CONTROLES DE EQUIPO

OTROS _____

¿Que riesgo de mayor importancia se debe evitar y /o reducir en la empresa?

Accesos indebidos

Divulgación no autorizada

Modificación indebida

Destrucción de los soportes

Robo de la información

Interrupción de los servicios

Introducción de códigos maliciosos

Intercepción de comunicaciones

Alteración de funcionamiento en la red

Alteración de funcionamiento en equipo de cómputo

OTROS _____

PROCEDIMIENTOS DE LA INVESTIGACIÓN

EL PROBLEMA

Planteamiento del problema

El problema surge que hay empresas que pueden estar usando bases de datos que no cumplan con las normas de seguridad que debería.

INTERROGANTES DE LA INVESTIGACIÓN

Las interrogantes que se pueden presentar en la propuesta ¿Para qué nos sirven cumplir las normas de seguridad? ¿En que afectaría a la empresa en no cumplir con las normas de seguridad de base de datos?

OBJETIVOS DE LA INVESTIGACIÓN

El objetivo de la investigación es saber que bases de datos cumplen con las normas de seguridad correspondientes para ver cuál sería su efecto para las empresas que la utilizan.

JUSTIFICACIÓN O IMPORTANCIA DE LA INVESTIGACIÓN

Es importante el proyecto ya que la actividad económica de algunas empresas se basa en sus datos y tendrían que ver cuál es el riesgo que causa si no tiene una base de dato.

MARCO TEÓRICO:

FUNDAMENTACIÓN TEÓRICA

Realizar el estudio sobre cuáles son las normas de seguridad de las bases de datos.

FUNDAMENTACIÓN LEGAL

Son Los decretos o leyes que establece nuestra máxima autoridad del país el cual nos ayuda a la compresión de que puntos podemos observar si estamos en lo correcto o no según las leyes que rigen en el país

PREGUNTAS A CONTESTARSE

Pueden surgir algunas pero la más relevante es en que puede o no afectar en no cumplimiento de normas para la empresa.

DEFINICIÓN DE TÉRMINOS

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.

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.

Pruebas de cumplimiento: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Pruebas sustantivas: Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

RECOLECCIÓN DE LA INFORMACIÓN

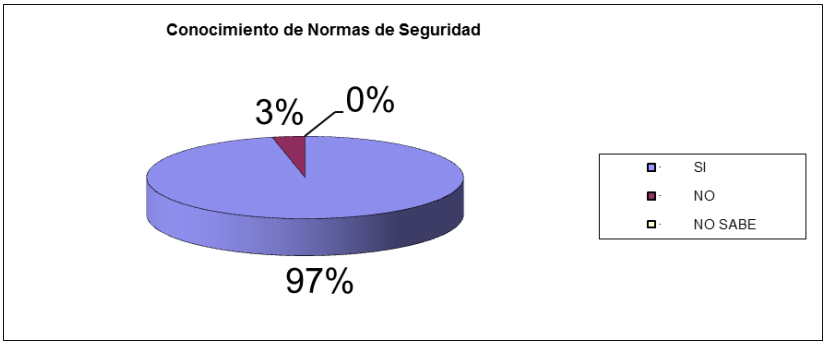
El proceso de recolección de información se realizó utilizando las herramientas antes ya mencionadas; las que conllevan en si las actividades de búsqueda de información relevante en páginas web, libros en formato digital y consultas hechas a personas expertas.

PROCESAMIENTO Y ANÁLISIS

Se procedió a realizar las respectivas encuestas a la población que se indico posteriormente la cuales las preguntas nos con llevan a la verificación de conocimiento que posee la persona encargada de la área netamente de base de datos o mejor dicho de la persona que está en mayor contacto con los datos de la empresa la cuales no dieron los siguiente resultados.

GRAFICO N ° 1

CONOCIMIENTO DE NORMAS DE SEGURIDAD



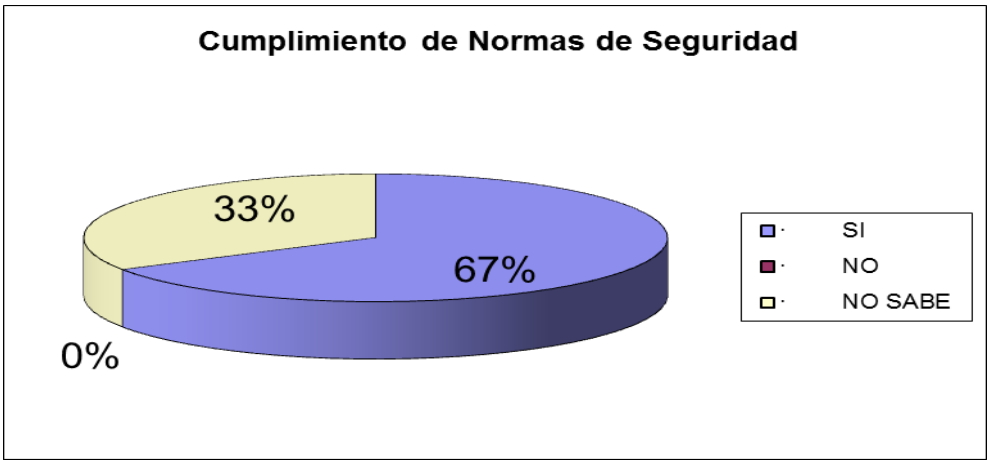
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

En el grafico nos podemos darnos cuenta que la mayoría de nuestra población si tiene conocimiento en su totalidad de las normas de seguridad.

GRAFICO N ° 2

CUMPLIMIENTO DE NORMAS DE SEGURIDAD



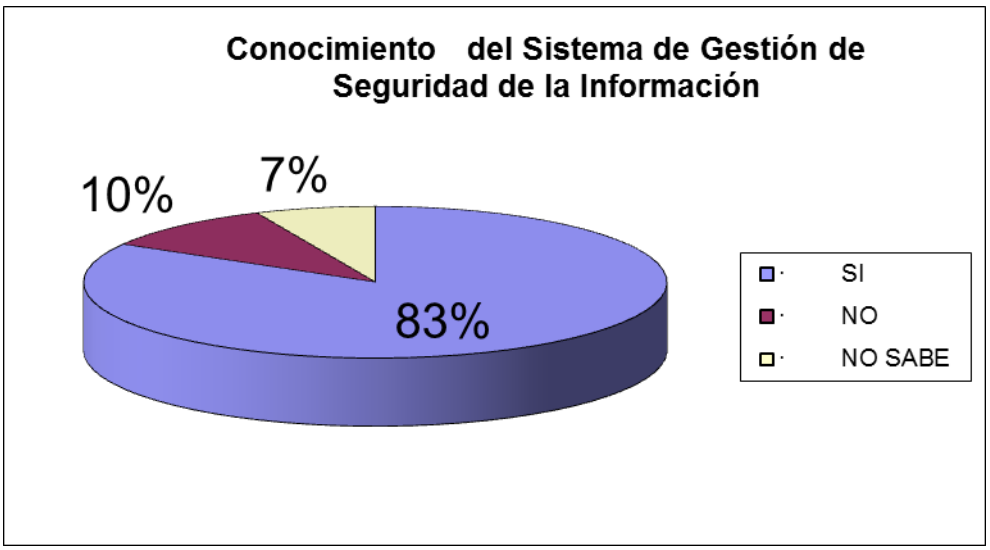
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

Nuestra población en el grafico Nº2 nos da a conocer que un 67% cumple con normas de seguridad, y un 33% no sabe si cumple o no, este porcentaje puede varias ya que empresas llevan un control y /o procedimientos en su información, los cuales pueden estar detallados en las normas de seguridad y por lo tanto las están cumpliendo.

GRAFICO N ° 3

CONOCIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



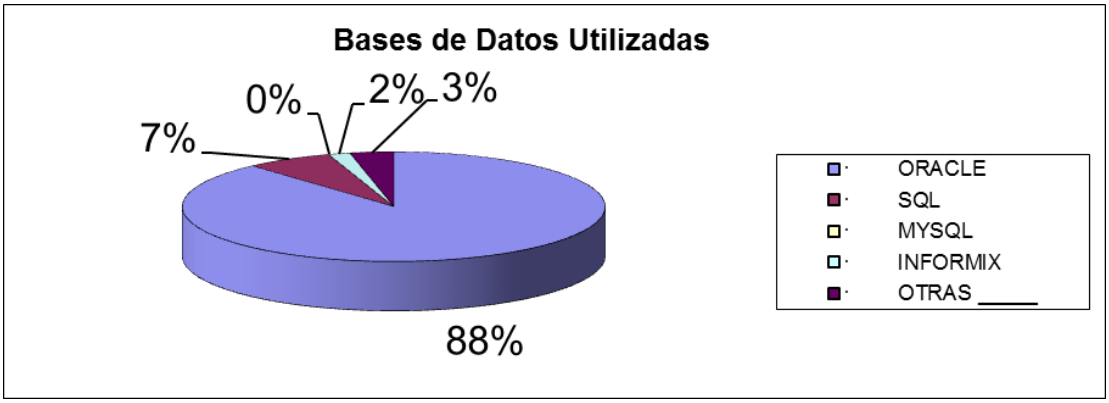
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

Témenos que la mayoría de los encuestados tiene conocimientos de un SGSI, y un mínimo del 17% no tiene conocimiento de como se pueda llegar a implementar o no sabes que es un SGSI.

GRAFICO N ° 4

BASES DE DATOS UTILIZADAS



Elaborado por: Sharon Estrada Rojas

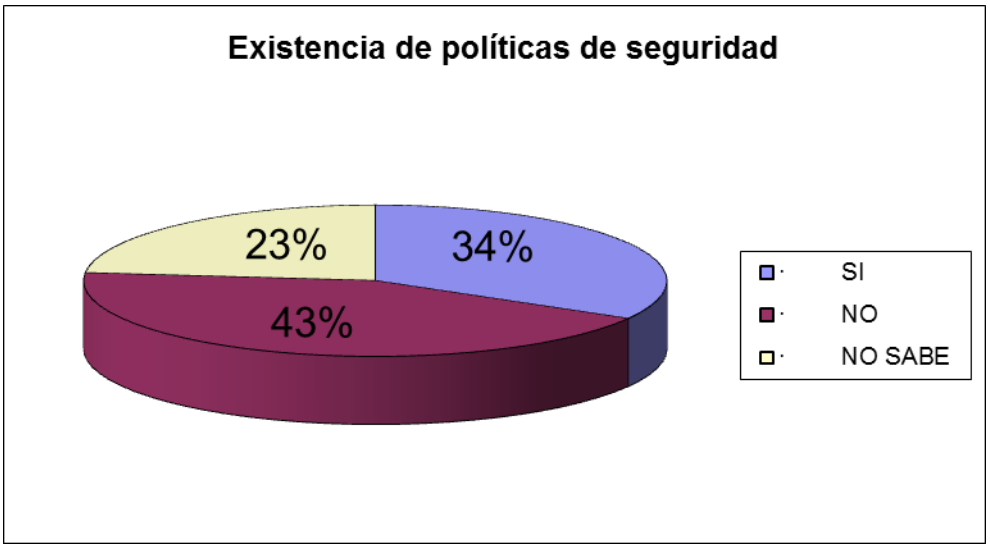
Fuente: Procesamiento y análisis

Para poder determinar cuáles de las bases de datos son las utilizadas en Guayaquil en el sector las consultoras y constructoras de obras civiles, escogimos cuatro bases de datos dándonos como resultado que el 88% conoce Oracle, un 7% conoce SQL, un 2% conoce Informix, y una pequeña parte teniendo un 3% utilizan como bases de datos Access, Visual FoxPro. Cabe destacar que los encuestadores determinaron que las tres bases de datos más conocidas para la seguridad de la información no se cuenta con licencias respectivas o no son utilizadas de una manera eficientes por falta de técnicos o profesionales capacitados para tal ejecuto por lo tanto para la evaluación estadística se

determino que el 81.67% de las empresas no cuentan con una base de datos legalmente determinada y/o mantenida y aplicada eficientemente.

GRAFICO N ° 5

EXISTENCIA DE POLITICAS DE SEGURIDAD



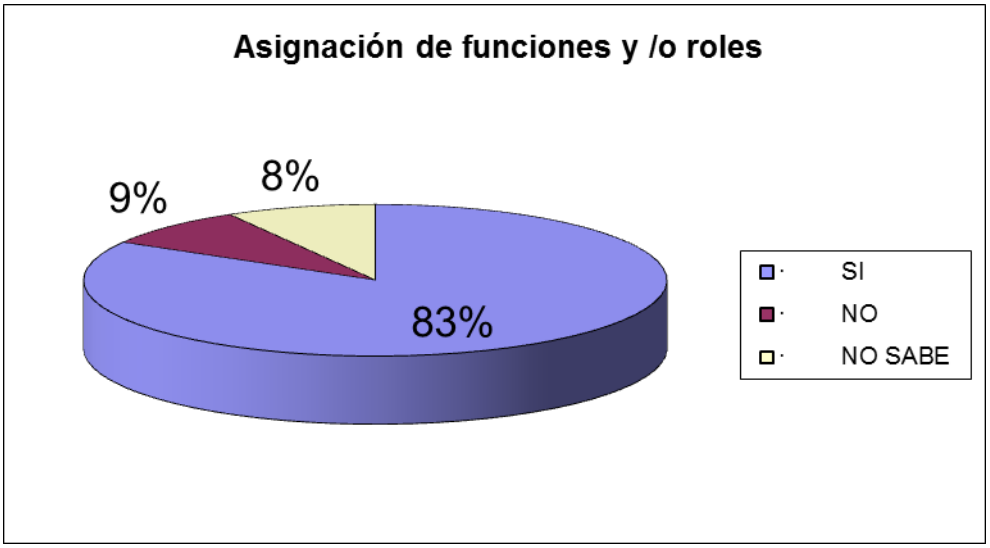
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

En el grafico N° 5 podemos observar que tenemos un 43 % de muestra población que no aplican políticas de seguridad, un 34% que si tienen las políticas y un 23% de no conocen si existen políticas de seguridad en su empresa. Se considero no las empresa que determinaron no saber por lo tanto se determino un 66.67% de incumplimiento.

GRAFICO N ° 6

ASIGNACION DE FUNCIONES Y /O ROLES



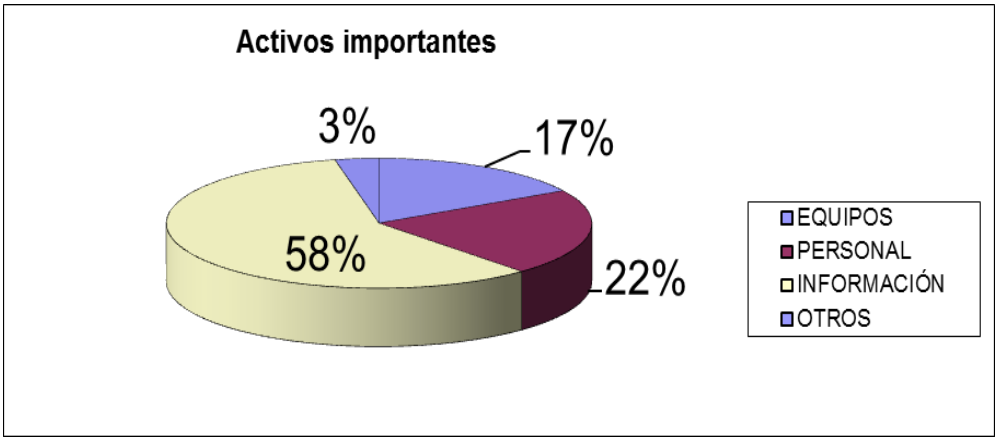
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

En el grafico N° 6 podemos encontrar que la asignación de funciones y/o roles si son aplicadas ya que un 83% nos dice que si cumplen con la asignación. Sin embargo se determino que las asignación de funciones y/o roles del personal solo fueron transmitidas directamente por el superior inmediato, la cual no están definidas en los contratos legalizados en el ministerio de relaciones laborables y manuales de control de seguridad interno de las empresas. Por lo tanto se determino que existe un incumplimiento del 63.33%

GRAFICO N ° 7

ACTIVOS IMPORTANTES



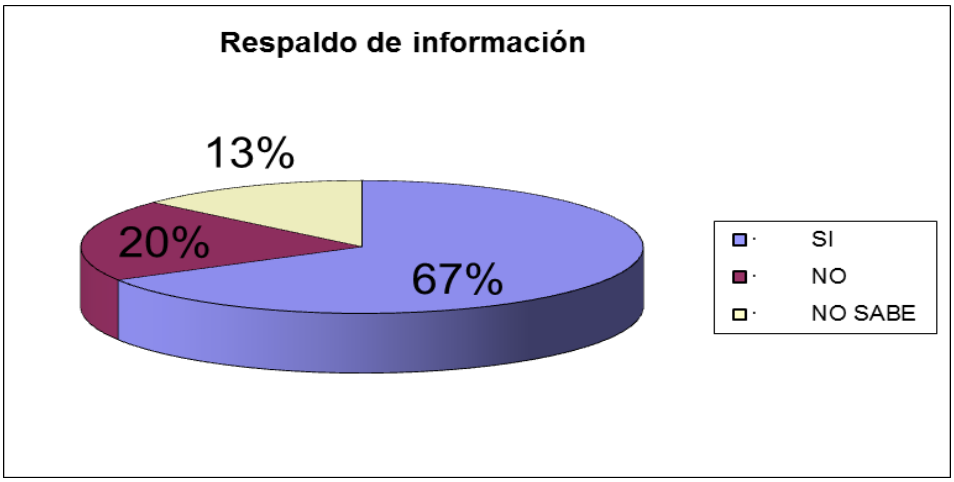
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

Para determinar cuales son activos importantes en las empresas nos podamos dar cuenta que en su mayoría es la información, siguiendo con el personal y equipo. Por lo expuesto se considera un 97% de cumplimiento, ya que existe un 3% de las empresas que consideran otros activos.

GRAFICO N ° 8

RESPALDO DE INFORMACION



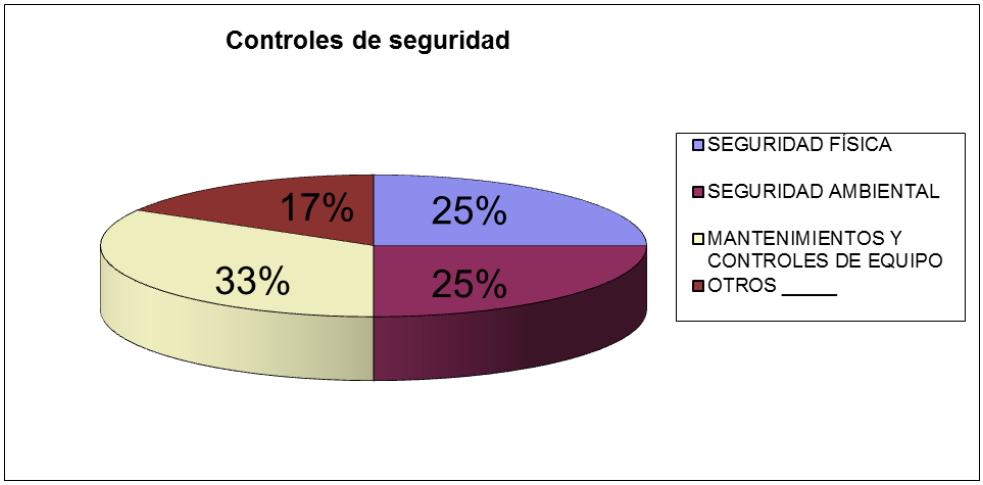
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

Si en el grafico N°7 fue demostrado que el activo importante es la información para muchos, así mismo témenos que respaldarla la cual la cumple un 67%. Se ha considerado que la información respaldada mediante medios físicos (impresos) debe ser respaldada en forma magnética para evitar daños, deterioro, perdidas y/o robo, por lo tanto se determino un incumplimiento del 33.33%

GRAFICO N ° 9

CONTROLES DE SEGURIDAD



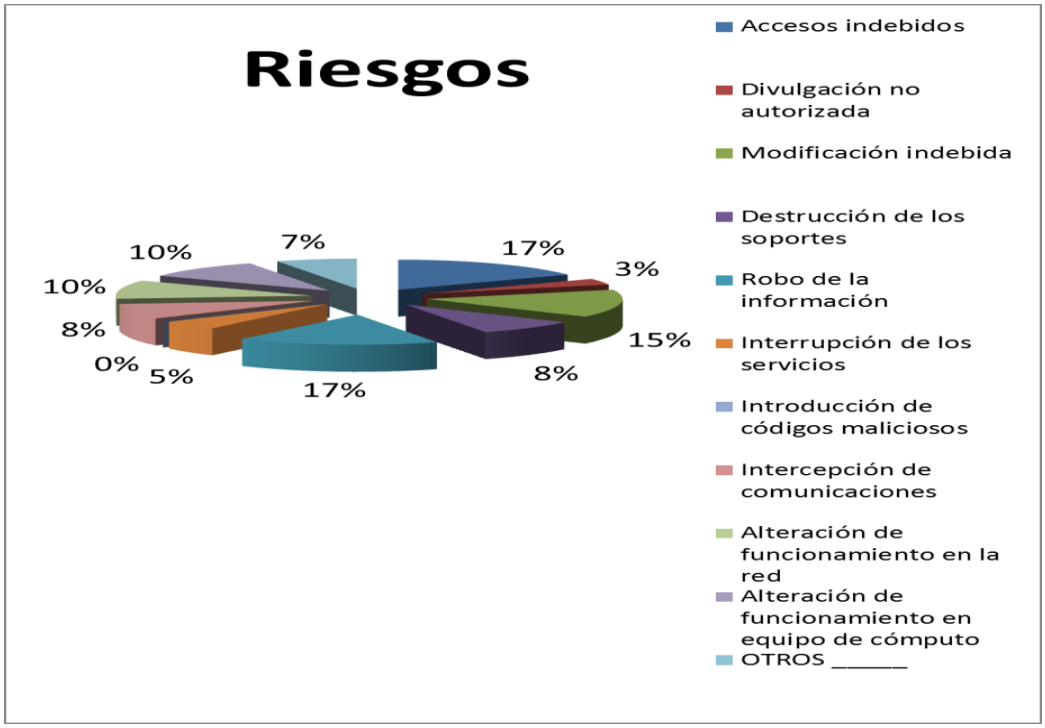
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

Nuestra población muestra que controles de seguridad aplica a sus activos, lo cual nos da como resultados que tienen controles de seguridad en: Mantenimiento y control de equipos; ambiental y física; técnico; administrativos entre otros. Sin embargo se considero como un no incumplimiento a los procesos de mantenimiento y control de equipo y otros, obteniéndose un valor del 50%

GRAFICO N ° 10

RIESGOS



Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

En este ultimo cuadro nos podemos dar cuenta que la mayoría de nuestra población sabe en que riesgo puede incurrir, o en que riesgo se encuentra si este que no cumple con normas de seguridad. Se determino que el 93.33% de la población no mantienen normas de control de la aseguración de la información, determinándose que solo 4 empresas cumplen normas de control de la calidad incluida la información.

Observaciones de las encuestas y estadísticas:

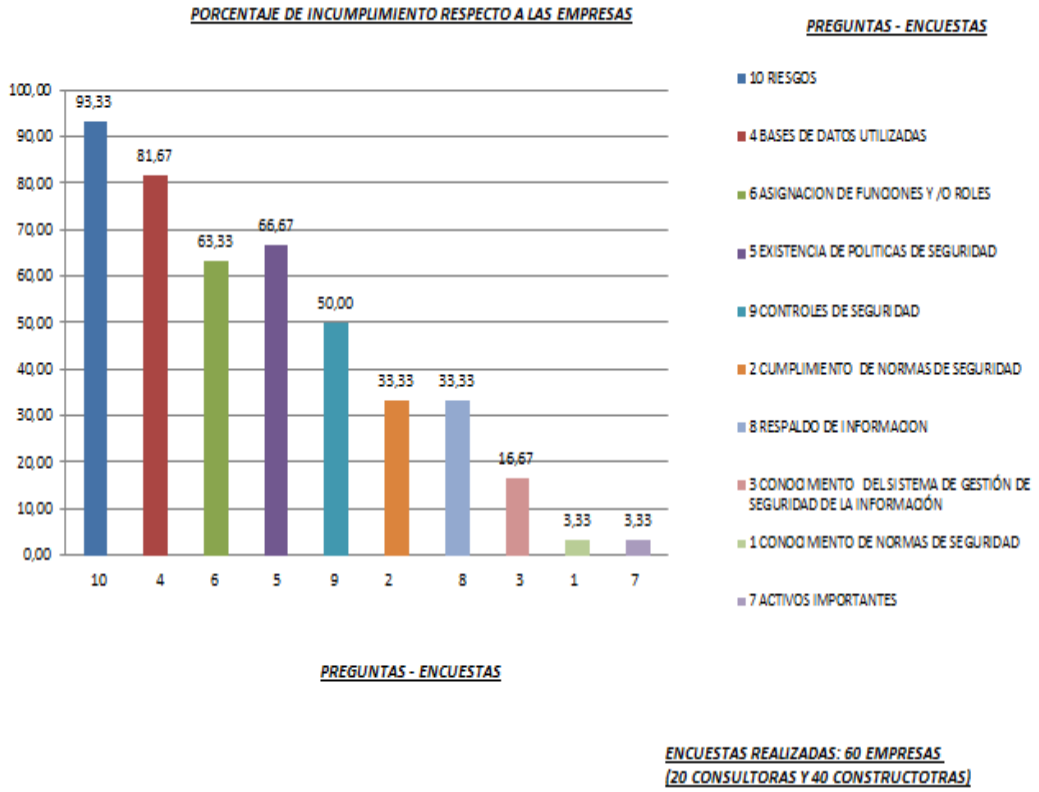
Por medio de este método de la encuesta se determino:

- Las empresas conocen las normas de seguridad y los riesgos que pueden incurrir si no cumplen o aplican normas.
- Las empresas no mantienen software legales y muchos casos no mantiene personal calificados para la ejecución de dichos programas.
- Se estableció que la mayoría de las empresas no mantienen las normas de control y asignación debidamente legalizadas, distribuidas y entendidas por el personal asignado a la seguridad de información.
- El respaldo de información no se lleva de una manera eficiente utilizando la tecnología existente.

Se anexa a la presente el cuadro de incumplimiento respecto a las empresas encuestadas:

GRAFICO N ° 11

INCUMPLIMIENTOS - EMPRESAS



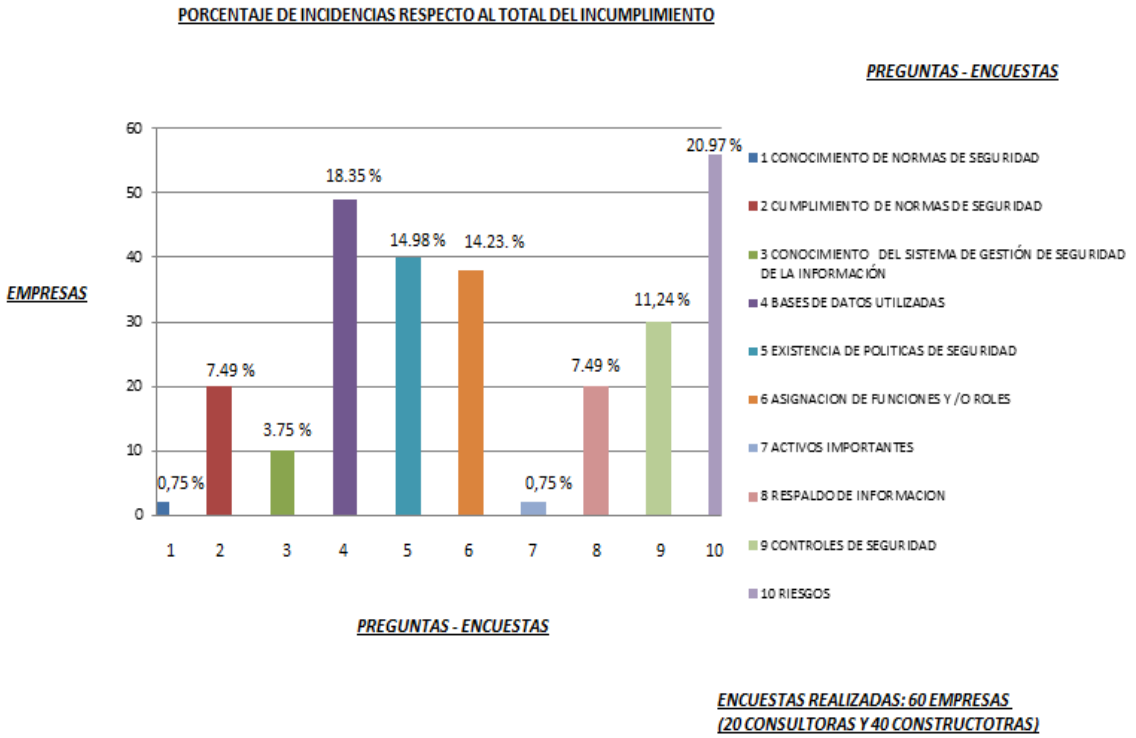
Elaborado por: Sharon Estrada Rojas

Fuente: Procesamiento y análisis

Con la finalidad de poder determinar el porcentaje de incidencia respecto a todo los incumplimientos, en base a la estadística realizada a las 60 organizaciones (consultoras o constructoras) se presenta el siguiente cuadro en donde se le ha asigna los pesos o porcentajes de incidencia aplicables a las 11 clausulas de la normas ISO 27002.

GRAFICO N ° 12

INCUMPLIMIENTOS – PREGUNTAS DE ENCUESTAS



Elaborado por: Sharon Estrada Rojas

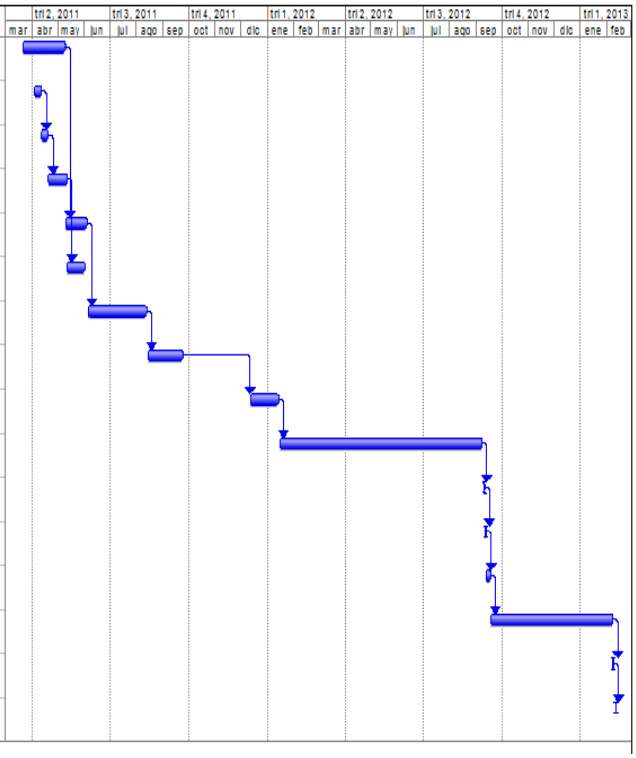
Fuente: Procesamiento y análisis

CAPÍTULO IV

MARCO ADMINISTRATIVO

CRONOGRAMA

Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	Inicio de clases de tesis	36 días	lun 21/03/11	lun 09/05/11	
2	Elaboración de Capítulo I	6 días	lun 04/04/11	lun 11/04/11	
3	Elaboración de Capítulo II	6 días	mar 12/04/11	mar 19/04/11	2
4	Elaboración de Capítulo III	16 días	mié 20/04/11	mié 11/05/11	3
5	Clases Individuales	19 días	mar 10/05/11	vie 03/06/11	1
6	Elaboración de Capitulo IV	15 días	jue 12/05/11	mié 01/06/11	4
7	Revisión de todos los capítulos	50 días	lun 06/06/11	vie 12/08/11	5
8	Aprobación de Capítulos de tesis	30 días	lun 15/08/11	vie 23/09/11	7
9	Asignación de Tutor	25 días	lun 12/12/11	vie 13/01/12	8
10	Revisión y corrección de tesis	170 días	lun 16/01/12	vie 07/09/12	9
11	Aprobación de tesis por tutor	1 día	lun 10/09/12	lun 10/09/12	10
12	Entrega de solicitud para sustentar	2 días	mar 11/09/12	mié 12/09/12	11
13	Notificación de tribunal	3 días	jue 13/09/12	lun 17/09/12	12
14	Revisión y corrección por tribunal	103 días	mar 18/09/12	jue 07/02/13	13
15	Aprobación	1 día	vie 08/02/13	vie 08/02/13	14
16	Fin de Tesis	1 día	lun 11/02/13	lun 11/02/13	15



PRESUPUESTO

Comprende los diferentes gastos que se llevaran a efecto, para el cumplimiento del objetivo del proceso de la investigación.

INGRESOS

Para la realización del proyecto de tesis he tenido un autofinanciamiento, todos los gastos que conllevan la realización del proyecto los he solventado con el sueldo de mi trabajo dando un total del $520.00.

CUADRO # 4

Detalle de egresos del proyecto

EGRESOS	DÓLARES
Impresiones	$ 90.00
Fotocopias	$ 30.00
Computadora y servicios de Internet	$ 50.00
Energía eléctrica	$100.00
Transporte	$ 55.00
Refrigerio	$ 45.00
Empastado, anillado de tesis de grado	$ 150.00
TOTAL……	$520.00

PROPUESTA

1. POLÍTICAS DE SEGURIDAD

Esta primera cláusula va netamente acorde con la parte administrativa de la empresa de quien o quienes deben autorizar y realizar las políticas de seguridad; la cual no se puede demostrar en ninguna base de dato pero si influye al seguir los procesos de seguridad de la información en las bases de datos.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En esta cláusula hace referencia a gestionar la seguridad de la información dentro de la Organización, lo cual se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.

El órgano de dirección debería aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización.

Así mismo Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

3. Gestión de activos

En esta cláusula se puede entender que la información es un activo importante para una organización, el objetivo es alcanzar y mantener una protección adecuada de los activos de la Organización; Asegurar que se aplica un nivel de protección adecuado a la información.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

4. Seguridad de recursos humanos

En esta cláusula nos da a conocer que se debe tener un control de quienes pueden acceder a nuestra información así mismo que en las políticas de seguridad se

encuentren definido como calificar al personal adecuado.

Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

ORACLE: Cumple si es que tiene una tabla (bitácora) donde detalle los datos de los empleados y/o contratistas

SQL SERVER: Cumple si es que tiene una tabla (bitácora) donde detalle los datos de los empleados y/o contratistas

INFORMIX: Cumple si es que tiene una tabla (bitácora) donde detalle los datos de los empleados y/o contratistas

ACCESS: Cumple si es que tiene una tabla (bitácora) donde detalle los datos de los empleados y/o contratistas

5. Seguridad física y ambiental

Esta cláusula nos menciona la seguridad física y ambiental que debemos tener en nuestra información, tanto en controles de ingreso físico, equipo de seguridad su manteniendo y la seguridad cuando este esta fuera de la organización.

Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.

Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

6. Gestión de las comunicaciones y operaciones

La cláusula nos menciona como

- Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.
- Minimizar el riesgo de fallos en los sistemas.
- Proteger la integridad del software y de la información.
- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- Asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo.
- Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.
- Mantener la seguridad de la información y del software que se

intercambian dentro de la organización o con cualquier entidad externa.

- Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.
- Detectar actividades de procesamiento de la información no autorizadas.

INTEGRIDAD: Es importante, al diseñar una base de datos y las tablas que contiene, tener en cuenta la integridad de los datos, esto significa que la información almacenada en las tablas debe ser válida, coherente y exacta.

Se debe controlar y restringir la entrada de valores a un campo mediante el tipo de dato que le definimos (cadena, numéricos, etc.), la aceptación o no de valores nulos, el valor por defecto. También cada registro de una tabla sea único definiendo una clave primaria y empleando secuencias.

RESPALDOS: Para conseguir un funcionamiento seguro de la BD y una pronta recuperación ante fallos se necesita planear una estrategia de copias de seguridad, backup, y de recuperación

REDES: es importante determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura

ORACLE: Si cumple

INTEGRIDAD: Las restricciones (constraints) son un método para

mantener la integridad de los datos, asegurando que los valores ingresados sean válidos y que las relaciones entre las tablas se mantengan.

Las restricciones pueden establecerse a nivel de campo o de tabla.

Pueden definirse al crear la tabla ("create table") o agregarse a una tabla existente (empleando "alter table") y se pueden aplicar a un campo o a varios. También es posible habilitarlas y deshabilitarlas.

Tipos de restricciones:

- not null: a nivel de campo.

- primary key: a nivel de tabla. Es un campo o varios que identifican cada registro de una tabla.

- foreign key: a nivel de tabla. Establece que un campo (o varios) relacione una clave primaria de una tabla con otra.

- check: a nivel de tabla. Restringe los valores que pueden ingresarse en un campo específico.

- unique: a nivel de tabla.

Se pueden crear, modificar y eliminar las restricciones sin eliminar la tabla y volver a crearla.

RESPALDOS:

- Backups del SO

  Este tipo de backup es el más sencillo de ejecutar, aunque consume

mucho tiempo y hace inaccesible al sistema mientras se lleva a cabo. Aprovecha el backup del SO para almacenar también todos los ficheros de la BD. Los pasos de este tipo de backup son los siguientes:

- Parar la BD y el SO
- Arrancar en modo superusuario.
- Realizar copia de todos los ficheros del sistema de ficheros
- Arrancar el sistema en modo normal y luego la BD.

- Backups de la BD en Frio

  Los backups en frio implican parar la BD en modo normal y copiar todos los ficheros sobre los que se asienta. Antes de parar la BD hay que parar también todas las aplicaciones que estén trabajando con la BD. Una vez realizada la copia de los ficheros, la BD se puede volver a arrancar.

  El primer paso es parar la BD con el comando shutdown normal. Si la BD se tiene que parar con inmediate o abort debe rearrancarse con el modo RESTRICT y vuelta a parar en modo normal. Después se copian los ficheros de datos, los de redo log y los de control, además de los redo log archivados y aún no copiados.

Una buena idea es automatizar todo este proceso con los scripts correspondientes, de modo que no nos olvidemos de copiar ningún fichero.

Como este tipo de backup es una copia de los ficheros de la BD, si estos contienen algún tipo de corrupción, la traspasaremos a la copia de seguridad sin detectarla. Por esto es importante comprobar las copias de seguridad.

- Backups de la BD en Caliente

  El backup en caliente se realiza mientras la BD está abierta y funcionando en modo ARCHIVELOG. Habrá que tener cuidado de realizarlo cuando la carga de la BD sea pequeña. Este tipo de backup consiste en copiar todos los ficheros correspondientes a un tablespace determinado, los ficheros redo log archivados y los ficheros de control. Esto para cada tablespace de la BD.

  Para efectuar un backup en caliente debemos trabajar con la BD en modo ARCHIVELOG. El procedimiento de *backup* en caliente es bastante parecido al frio. Existen dos comandos adicionales: *begin backup* antes de comenzar y *end backup* al finalizar el *backup*. Por

ejemplo, antes y después de efectuar un *backup* del *tablespace users* se deberían ejecutar las sentencias:

SVRMGR> alter tablespace users begin backup;

SVRMGR> alter tablespace users end backup;

Así como el backup en frio permitía realizar una copia de toda la BD al tiempo, en los backups en caliente la unidad de tratamiento es el tablespace. El backup en caliente consiste en la copia de los ficheros de datos (portablespaces), el actual fichero de control y todos los ficheros redo log archivados creados durante el periodo de backup. También se necesitarán todos los ficheros redo log archivados después del backup en caliente para conseguir una recuperación total.

- Backups Lógicos con Export/Import

  Estas utilidades permiten al DBA hacer copias de determinados objetos de la BD, así como restaurarlos o moverlos de una BD a otra. Estas herramientas utilizan comandos del SQL para obtener el contenido de los objetos y escribirlos en/leerlos de ficheros

  Para realizar un *export* la BD debe estar abierta. *Export* asegura la consistencia en la tabla, aunque no entre tablas. Si se requiere

consistencia entre todas las tablas de la BD entonces no se debe realizar ninguna transacción durante el proceso de *export*. Esto se puede conseguir si se abre la BD en modo RESTRICT.

REDES: En Oracle existen archivos de configuración de la red, dependiendo de la configuración que se utilice se pueden configurar unos archivos u otros.

listener.ora
tnsnames.ora
names.ora
ldap.ora

1. listener.ora

Archivo **ubicado en el servidor** de base de datos. Es el archivo de configuración del listener de la base de datos.Este archivo tendrá que estar ubicado en $ORACLE_HOME/network/admin/listener.ora. El comando para gestionar el listener es lsnrctl. Este ejecutable lo podemos encontrar en $ORACLE_HOME/bin/lsnrctl.

- Es un proceso servidor que provee la conectividad de red con la base de datos Oracle.
- El listener está configurado para escuchar la conexión en un puerto específico en el servidor de base de datos.
- Cuando una se pide una conexión a la base de datos, el listener devuelve la información relativa a la conexión.

- La información de una conexión para una instancia de una base de datos provee el nombre de usuario, la contraseña y el SID de la base de datos.
- Si estos datos no son correctos se devolverá un mensaje de error.
    - Por defecto el puerto del listener es el 1521.
    - El listener no limita el número de conexiones a la base de datos.

2. tnsnames.ora

Archivo ubicado en los clientes, contiene los nombres de servicio de red, asignados a descriptores a través de los cuales se nos permite acceder.

- También llamado método LOCAL
- Indica que la resolución se hace a través de otro archivo de configuración llamado tnsnames.ora, residente en la misma ubicación.
- Puede haber varios ficheros Tnsnames.ora, uno en el servidor y los demás en clientes que se conectan al servidor.
- Contienen los nombres de servicio de red asignados a descriptores, a través de los cuales se nos permite acceder.

3. names.ora

Archivo **ubicado en el servidor de ORACLE NAMES**. Este archivo incluye la ubicación y la información de dominio y los parámetros de configuración opcionales para un servidor de **ORACLE NAMES**

5. ldap.ora

Archivo ubicado en el servidor de base de datos y en el cliente configurado para que funcionen como **gestión centralizada**. Contiene los parámetros necesarios para acceder al servidor de directorios.

SQL SERVER: Si cumple

INTEGRIDAD: Dos pasos importantes en el diseño de las tablas son la identificación de valores válidos para una columna y la determinación de cómo forzar la integridad de los datos en la columna. La integridad de datos pertenece a una de las siguientes categorías:

- **Integridad de entidad:** La integridad de entidad define una fila como entidad única para una tabla determinada. La integridad de entidad exige la integridad de las columnas de los identificadores o la clave principal de una tabla, mediante índices y restricciones UNIQUE, o restricciones PRIMARY KEY.
- **Integridad de dominio:** La integridad de dominio viene dada por la validez de las entradas para una columna determinada. Puede exigir la integridad de dominio para restringir el tipo mediante tipos de datos, el formato mediante reglas y restricciones CHECK, o el intervalo de valores posibles mediante restricciones FOREIGN

KEY, restricciones CHECK, definiciones DEFAULT, definiciones NOT NULL y reglas.

- **Integridad referencial:** La integridad referencial protege las relaciones definidas entre las tablas cuando se crean o se eliminan filas. En SQL Server la integridad referencial se basa en las relaciones entre claves externas y claves principales o entre claves externas y claves exclusivas, mediante restricciones FOREIGN KEY y CHECK. La integridad referencial garantiza que los valores de clave sean coherentes en las distintas tablas. Para conseguir esa coherencia, es preciso que no haya referencias a valores inexistentes y que, si cambia el valor de una clave, todas las referencias a ella se cambien en consecuencia en toda la base de datos.

  Cuando se exige la integridad referencial, SQL Server impide a los usuarios:

  - Agregar o cambiar filas en una tabla relacionada si no hay ninguna fila asociada en la tabla principal.
  - Cambiar valores en una tabla principal que crea filas huérfanas en una tabla relacionada.
  - Eliminar filas de una tabla principal cuando hay filas relacionadas coincidentes.

- **Integridad definida por el usuario:** La integridad definida por el usuario permite definir reglas de empresa específicas que no pertenecen a ninguna otra categoría de integridad. Todas las categorías de integridad admiten la integridad definida por el usuario. Esto incluye todas las restricciones de nivel de columna y nivel de tabla en CREATE TABLE, procedimientos almacenados y desencadenadores.

RESPALDOS:

En cuanto a los **tipos de respaldo** se refiere, SQL Server ofrece varias opciones: Completo, Diferencial, Filegroup y Bitácora de Transacciones.

El respaldo completo no necesita mucha explicación ya que involucra respaldar todas y cada una las páginas que forman parte de la base de datos y aquellas asociadas con la bitácora de transacciones que se generaron mientras el respaldo estuvo activo. La desventaja de los respaldos completos es que si la base de datos es muy grande, entonces pueden requerir bastante tiempo y espacio.

El respaldo diferencial consiste en respaldar todas las páginas que han sufrido cambios desde el último respaldo completo y para poder que funcione tienes que haber tomado un respaldo completo anteriormente.

Dado que se respaldan solamente las páginas que han cambiado desde el último respaldo completo, los respaldos diferenciales generalmente son más rápidos que los completos.

Nota: La base de datos Maestra no puede respaldarse diferencialmente.

El respaldo tipo filegroup consiste en respaldar todos los archivos que pertenecen a un filegroup en particular. Es importante señalar que aunque es posible respaldar un archivo en específico, dicha granularidad no es recomendable ya que el proceso de recuperación requiere que todos los archivos pertenecientes al filegroup siendo recuperado se encuentren en el mismo punto o estado. Este tipo de respaldos se usan en combinación con los respaldos de la bitácora de transacciones para recuperar secciones de la base de datos.

El respaldo de la Bitácora de Transacciones o Transaction Log solamente puede hacerse cuando el modelo de recuperación de la base de datos es FULL o Bulk-logged y se realiza principalmente con el fin de reducir la cantidad de datos que pudieran perderse en caso de una falla y reducir el tamaño del archivo que almacena la bitácora. Cuando realizas un respaldo de la bitácora, SQL Server respalda todas las páginas nuevas desde el último respaldo completo, diferencial, o desde el último respaldo

de la bitácora. Esto significa que cada respaldo de la Bitácora de Transacciones captura todas las transacciones asociadas con un punto en el tiempo.

REDES: Entre las tareas de configuración de red del servidor se incluyen las siguientes: habilitar protocolos, modificar el puerto o canalización usados por un protocolo, configurar el cifrado, configurar el servicio SQL Server Browser, mostrar u ocultar Motor de base de datos de SQL Server en la red y registrar el nombre de la entidad de seguridad del servidor. La mayoría de las veces, no es necesario cambiar la configuración de red del servidor. Solo debe volver a configurar los protocolos de red del servidor si la red tiene requisitos especiales.

La configuración de red de SQL Server se realiza mediante el Administrador de configuración de SQL Server. Para versiones anteriores de SQL Server, utilice la Herramienta de red de servidor que se incluye con dichos productos.

INFORMIX: Si cumple

INTEGRIDAD: Los CONSTRAINTS con respecto a la Integridad de los datos pueden prevenir que estos lleguen a ser incorrectos pero no pueden garantizarlo con exactitud. Hay a pesar de eso suficiente espacio para el error humano. Los CONSTRAINTS pueden prevenir que se introduzca un

dato fuera de los valores permitidos (por ejemplo, para el género de una persona, M o F), pero no pueden prevenir que una persona accidentalmente ingrese F para el caso de masculino, o viceversa.

Con respecto a las reglas del negocio, la Integridad de los CONSTRAINTS ayuda a guardar los datos en Línea con los valores como lo relatan el mundo real. Considerando la seguridad se puede prevenir acciones para usuarios específicos durante la ejecución de las funciones INSERT, UPDATE, DELETE y SELECT, los CONSTRAINTS observan los datos durante el INSERT, UPDATE O DELETE y no mira el usuario.

Los tres tipos de CONSTRAINTS de la Integridad que pueden ser dados obligatoriamente por todos los servidores de bases de datos de Informix son:

CONSTRAINTS Semánticos: Estos tratan de cómo una columna maneja datos específicos ingresados y el valor que se guarda en esa columna.

CONSTRAINTS de la Entidad: Son los que dan fuerza a filas dentro de una tabla manteniendo las llaves propias de la Llave Primaria.

CONSTRAINTS de Integridad Referencial: Son aquellos que tratan de cómo las filas dentro de una tabla corresponden con otra fila dentro de otra tabla.

Debe usar una combinación de estos tres tipos de Integridad al servidor y aplicaciones del cliente con el fin de asegurarse la Integridad de los datos.

RESPALDOS:

Existen dos formas básicas para realizar una copia de seguridad y recuperar una base de datos Informix:

- Copias de seguridad física sin un gestor de almacenamiento, utilizando ontape "es la utilidad de copia de seguridad más antigua de Informix, pero todavía va fuerte. No hace interfaz con los administradores de almacenamiento, por lo que es la forma más fácil y mejor manera de realizar copias de seguridad físicas sin un gestor de almacenamiento."
- Copias de seguridad física con un gestor de almacenamiento, utilizando onbar "es lo último en la tecnología de copia de seguridad de Informix y sólo se utiliza para interactuar con los administradores de almacenamiento como el Informix Storage Manager (ISM). (onbar se cubre en "Copias de seguridad física con un gestor de almacenamiento: onbar . ") Si está ejecutando Informix 7.3 o superior, onbar ofrece una mayor funcionalidad y flexibilidad."

REDES:

Informix hace las conexión de redes mediante Básicamente el estándar de conexión ODBC requiere de un administrador ODBC (ODBC Manager) y de un manejador ODBC (ODBC Driver), así mismo, en el caso de Informix, se

requiere de un manejador (o driver) nativo que se conecte directamente a la base de datos, el nombre que recibe este componente es “Informix-Net”, o “I-Net” para abreviar.

Para nuestro ejemplo, el administrador ODBC accederá a lo que se conoce como un nombre de fuente de datos, o DSN (Data Source Name) por sus siglas en inglés. Este DSN es un archivo de texto que hace referencia al nombre del servidor de base datos, base de datos, usuario, password, así como otros parámetros relevantes a nuestra instancia. Pero, sobre todo, en este DSN haremos referencia al manejador ODBC de Informix, que no es otra cosa que una biblioteca a nivel de sistema operativo. Esta biblioteca se conectará a la base de datos a través del manejador nativo que requiere de una configuración muy básica que le permita asociar el nombre de la instancia de Informix a la que deseamos conectarnos, a una IP-Address, un puerto de comunicaciones y un protocolo, esto lo haremos a través de un archivo propio de informix conocido como “sqlhosts”.

Monitoreando Informix con Nagios

(**Nagios** es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la

monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.)

ACCESS: Si cumple

INTEGRIDAD:

La integridad referencial es un sistema de reglas que utiliza Microsoft Access para garantizar que las relaciones entre los registros de tablas relacionadas son válidas y que no se eliminan ni modifican accidentalmente datos relacionados.

Puede establecer la integridad referencial cuando se cumplen todas las condiciones siguientes:

El campo coincidente de la tabla principal es una clave principal o tiene un índice único.

Los campos relacionados tienen el mismo tipo de datos. Existen dos excepciones: un campo Auto numérico puede estar relacionado con un campo Numérico con la propiedad Tamaño del campo establecida a Entero largo, y un campo Auto numérico con la propiedad Tamaño del campo establecida a

Id. de réplica puede estar relacionado con un campo Numérico con la propiedad Tamaño del campo establecida a Id. de réplica.

Ambas tablas pertenecen a la misma base de datos de Microsoft Access.

Cuando se exige la integridad referencial, deben observarse las reglas siguientes:

No puede introducir un valor en el campo de clave externa de la tabla relacionada que no exista en la clave principal de la tabla principal.

No puede eliminar un registro de una tabla principal si existen registros coincidentes en una tabla relacionada.

No puede cambiar un valor de clave principal en la tabla principal si ese registro tiene registros relacionados.

Si desea que Microsoft Access exija esas reglas para una relación, seleccione la casilla de verificación Exigir integridad referencial al crear la relación. Si se exige la integridad referencial e infringe una de las reglas con las tablas relacionadas, Microsoft Access muestra un mensaje y no permite el cambio.

Puede anular las restricciones sobre la eliminación o la modificación de registros relacionados y aun así conservar la integridad referencial mediante la activación de las casillas de verificación Actualizar en cascada los campos relacionados y Eliminar en cascada los registros relacionados. Cuando la casilla de verificación Actualizar en cascada los campos relacionados está activada, el cambio de un valor de clave principal en la tabla principal

actualiza automáticamente el valor coincidente en todos los registros relacionados.

Cuando la casilla de verificación Eliminar en cascada los registros relacionados está activada, la eliminación de un registro en la tabla principal elimina todos los registros relacionados en la tabla relacionada.

RESPALDOS:

Para respaldar una base de datos Access que está actualmente abierta debemos ir a la ficha Inicio e ir a la sección *Guardar & Publicar* para seleccionar la opción *Guardar base de datos como* y posteriormente, dentro de la sección Avanzadas, elegir la opción *Realizar copia de seguridad de la base de datos*.

Al pulsar el botón *Guardar como* se mostrará un cuadro de diálogo sugiriendo un nombre para el respaldo que contendrá la fecha actual.

Finalmente pulsa el botón Guardar para respaldar la base da datos. Access creará una copia de seguridad en la ubicación elegida de manera que esté disponible. Para restaurar una base de datos que está dañada será suficiente con sobrescribir el archivo actual con el último respaldo guardado.

REDES:

Access tiene conexión de redes mediante Básicamente el estándar de conexión ODBC.

Para un mejor funcionamiento en la red se puede utilizar Internet Access Monitor.

Internet Access Monitor es una herramienta integral de supervisión del uso de Internet y creación de informes para las redes corporativas. El programa aprovecha el hecho de que la mayoría de las corporaciones accede a Internet a través de servidores proxy, tales como MS ISA Server, MS Forefront TMG, WinGate, WinRoute, MS Proxy, WinProxy, EServ, Squid, Proxy Plus y otros. Cada vez que un usuario accede a un sitio web, descarga archivos o imágenes, su actividad se registra. Internet Access Monitor procesa estos archivos log para ofrecer a los administradores la posibilidad de generar informes usando opciones diferentes. El programa puede generar informes para usuarios individuales, mostrar la lista de los sitios web que él o ella visitó, junto con el análisis detallado de su actividad en Internet (descargas, lectura de textos, visualización de imágenes, películas, escucha de música, trabajo). Además, el programa puede crear informes integrales con el análisis completo del consumo del ancho de banda, creación de gráficos fáciles de entender que sugieren las áreas en las que el consumo derrochador del ancho de banda puede ser eliminado.

Los beneficios de Internet Access Monitor:

- permite la supervisión centralizada del acceso a Internet de sus

empleados;

- ayuda a prevenir intentos de utilizar el ancho de banda de Internet corporativo para propósitos personales;
- reduce sus gastos de Internet;
- es muy fácil de usar y permite supervisar a los usuarios dentro de varios minutos después de la instalación del programa;
- trabaja con todos los servidores proxy modernos;
- permite generar una gran cantidad de informes y diagramas que representan la eficacia de la utilización del servidor proxy de su compañía.
- dispone de un programador de tareas para automatizar la creación y la entrega de informes al personal autorizado.

7. Control del acceso

En esta cláusula podemos ver todo lo referente a la seguridad que tenemos que tener en conexión de accesos en las redes como: claves, identificación del equipo de red, la identificación y autenticación del usuario, etc.

Tenemos que tener los siguientes objetivos:

- Controlar los accesos a la información.
- Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

- Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.
- Impedir el acceso no autorizado a los servicios en red.
- Impedir el acceso no autorizado al sistema operativo de los sistemas.
- Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.
- Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

AUTENTICACIÓN DEL USUARIO: es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.

ORACLE, SQL SERVER, INFORMIX:

Para el ingreso a la base de datos solicita usuario y clave, también para realizar alguna acción deben tener se asignan roles y/o funciones.

Utilizando las siguientes sentencias:

- CREATE USER nuevo_usuario IDENTIFIED BY contraseña
- CREATE ROLE nuevo_rol
- GRANT select,insert,update,delete ON tabla TO nuevo_rol;
- GRANT nuevo_rol TO nuevo_usuario;

ACCESS: No cumple con el control de acceso puede cualquier persona acceder a la base de datos y puede realizar actualizaciones, inserción y eliminación de datos.

8. Adquisición, desarrollo y mantenimiento de los sistemas de información

En esta cláusula nos dice que objetivos debemos tener:

- Garantizar que la seguridad es parte integral de los sistemas de información.
- Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.
- Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.
- Garantizar la seguridad de los sistemas de ficheros.
- Mantener la seguridad del software del sistema de aplicaciones y la información.
- Reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.

ORACLE: Si cumple con actualizaciones y/o parches para solventar vulnerabilidades

SQL SERVER: Si cumple con actualizaciones y/o parches para solventar vulnerabilidades

INFORMIX: Si cumple con actualizaciones y/o parches para solventar vulnerabilidades

ACCESS: Si cumple con actualizaciones y/o parches para solventar vulnerabilidades

9. Gestión de un incidente en la seguridad de la información

En esta cláusula se refleja cómo garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

10. Gestión de la continuidad del negocio

En este punto se detalla como y que se debe hacer para mantener la continuidad del

negocio lo cual en su mayoría es identificar los eventos, con los cuales se desarrolla e implementa los planes de continuidad incluyendo la seguridad de la información, concluyendo con prueba, mantenimiento y re-evolución del plan de contingencia definido en la organización.

Así mismo reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

11. Cumplimiento

Como su nombre lo indica es de que la gerencia o directivos de la organización verifiquen el cumplimiento de cada uno de los requerimientos, controles, políticas y/o normas de seguridad, así mismo de realizar controles de auditoria y actualizaciones de planes de contingencia si fuere el caso.

Objetivos principales:

- Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.
- Garantizar la conformidad de los sistemas con las políticas y estándares de

seguridad de la Organización.

- Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

ORACLE: No aplica

SQL SERVER: No aplica

INFORMIX: No aplica

ACCESS: No aplica

Vulnerabilidades de bases de datos:

ORACLE:

- Configuraciones predeterminadas inseguros

  La instalación por defecto de Oracle Application Server incluye una serie de opciones de configuración inseguras, tales como contraseñas predeterminadas muy claras y el acceso irrestricto a las aplicaciones y la información sensible.

  VU # 307835 - Oracle9i Application Server procedimientos OWA_UTIL exponer información sensible

  Solución

  Bloquear o restringir el acceso sin autenticar el acceso del público a los procedimientos PL / SQL y aplicaciones se puede restringir mediante laexclusion_list parámetro en el archivo gateway PL / SQL de configuración, / Apache / modplsql / cfg / wdbsvr.app.

  VU # 611776 - Oracle9i Application Server PL / SQL Gateway interfaz de administración web usa la autenticación nula por defecto

  Solución

  Restringir el acceso a las páginas PL / SQL Gateway Web de administración se puede restringir mediante la especificación de nombres de usuarios autorizados y conectar cadenas o un descriptor de

base de datos Access administrativa (DAD) en el archivo gateway PL / SQL de configuración, / Apache / modplsql / cfg / wdbsvr. aplicación .

- El incumplimiento de los controles de acceso

  Oracle Application Server no es uniforme imponer restricciones de acceso. Diferentes componentes no tienen debidamente comprobada la autorización antes de conceder el acceso a los recursos protegidos.

  VU # 193523 - Oracle9i Application Server permite el acceso no autenticado a aplicaciones PL / SQL a través de descriptores de acceso alternativas de base de datos

  Solución

  Bloquear o restringir el acceso sin autenticar el acceso del público a aplicaciones PL / SQL y procedimientos se puede restringir mediante laexclusion_list parámetro en el archivo gateway PL / SQL de configuración, / Apache / modplsql / cfg / wdbsvr.app.

  VU # 977251 - Oracle 9iAS XSQL Servlet ignora los permisos de archivos permite a los usuarios ver archivos arbitrarios de configuración sensibles

VU # 547459 - Oracle 9iAS crea archivos temporales cuando se procesan las peticiones JSP que son de lectura global

Solución

Las siguientes soluciones fueron sugeridas por David Litchfield y no han sido probados por el CERT / CC.

Edite el archivo httpd.conf se encuentra en el directorio $ ORACLE_HOME $ / apache / apache / conf. Para evitar el acceso al archivo globals.jsa añadir la siguiente entrada: <Files ~ "^\globals.jsa"> Orden allow, deny Deny de todo </ Files> . Para evitar el acceso a las páginas de java añadir la siguiente entrada:<Location /_pages> Orden negar, permitir Denegar de todos </ Location> Tenga en cuenta que si las páginas JSP se almacenan en un directorio de alias (por ejemplo, no un subdirectorio de "htdocs") entonces es neccessary para añadir una entrada de <Location /dirname/_pages> Orden negar, permitir Denegar de todos </ Location> cuando "dirname" es el nombre del directorio de alias.

- Si no se validan los datos

  En un caso, el módulo PL / SQL no controla correctamente una solicitud HTTP con formato incorrecto.

  VU # 805915 - Oracle9i Application Server Apache PL / SQL módulo no controla correctamente encabezado de autorización HTTP

  Solución

  Aplicar el parche apropiado referencia en Oracle Security Alert # 28 .

- El acceso no autorizado a la información confidencial

  Un número de vulnerabilidades revelan la información de configuración o exponer datos almacenados en bases de datos subyacentes. Además, las aplicaciones inseguras podrían permitir a un intruso ejecutar consultas SQL.

Para solucionar estas vulnerabilidades se debe aplicar la cláusula:

- 3 “GESTIÓN DE ACTIVOS” la cual la organización debe definir cuales son sus activos los cuales es donde esta la información.
- 6 “GESTIÓN DE COMUNICACIONES Y OPERACIONES” definir las responsabilidades y procedimientos de operación.
- 7 “CONTROL DE ACCESO” aplicando los controles de Gestión de acceso de usuario y responsabilidades de usuario.

- 8 “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMA DE INFORMACIÓN” se debe aplicar el Control de las vulnerabilidades técnicas, lo cual es buscar nuevas actualizaciones del sistema o software que se esta utilizando.

SQL SERVER:

- Vulnerabilidad en reusó de memoria paginada - CVE-2008-0085

  Existe una vulnerabilidad de divulgación de información en la manera en que SQL Server administra el reusó de páginas de memoria. Un atacante con acceso de operación a la base datos que explote exitosamente la vulnerabilidad podría tener acceso a los datos de los usuarios.

- Desbordamiento en conversión - CVE-2008-0086

  Existe una vulnerabilidad en la función de conversión en SQL Server que podría permitir a un atacante no autenticado elevar privilegios. Un atacante que explote exitosamente la vulnerabilidad podría ejecutar código y tomar control total del sistema afectado.

- Vulnerabilidad de Corrupción de memoria en SQL Server - CVE-2008-0107

Existe una vulnerabilidad en SQL Server que podría permitir a un atacante autenticado elevar privilegios. En consecuencia podría ejecutar código y tomar control total del sistema.

- Vulnerabilidad de desbordamiento de buffer en SQL Server - CVE-2008-0106

  Existe una vulnerabilidad en SQL Server que podría permitir a un atacante autenticado elevar privilegios. Un atacante que explote exitosamente la vulnerabilidad podría ejecutar código y tomar control total del sistema.

Para solucionar estas vulnerabilidades se debe aplicar la cláusula:

- 6 “GESTIÓN DE COMUNICACIONES Y OPERACIONES” definir las responsabilidades y procedimientos de operación.
- 7 “CONTROL DE ACCESO” aplicando los controles de Gestión de acceso de usuario y responsabilidades de usuario.
- 8 “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMA DE INFORMACIÓN” se debe aplicar el Control de las vulnerabilidades técnicas, lo cual es buscar nuevas actualizaciones del sistema o software que se esta utilizando.

Vulnerabilidad	Recomendación	
	VERSION	*PARCHE*
Vulnerabilidad en reusó de memoria paginada - CVE-2008-0085	SQL Server 7.0 Service Pack 4	SQL70-KB948113-v7.00.1152-x86-ESN.exe
	SQL Server 2000 Service Pack 4	SQL2000-KB948111-v8.00.2273-x86x64-ESN.exe
	SQL Server 2000 Itanium-based Edition Service Pack 4	SQL2000-KB948111-v8.00.2273-x86x64-ESN.exe
Desbordamiento en conversión - CVE-2008-0086	SQL Server 2005 Service Pack 2	SQLServer2005-KB948108-IA64-ENU.exe SQLServer2005-KB948108-x64-ENU.exe SQLServer2005-KB948108-x86-ENU.exe
	SQL Server 2005 x64 Edition Service Pack 2	SQLServer2005-KB948108-IA64-ENU.exe SQLServer2005-KB948108-x64-ENU.exe SQLServer2005-KB948108-x86-ENU.exe
Vulnerabilidad de Corrupción de memoria en SQL Server - CVE-2008-0107	SQL Server 2005 with SP2 for Itanium-based Systems	SQLServer2005-KB948108-IA64-ENU.exe SQLServer2005-KB948108-x64-ENU.exe SQLServer2005-KB948108-x86-ENU.exe
	Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) Service Pack 4	SQL2000-KB948111-v8.00.2273-x86x64-ESN.exe
Vulnerabilidad de desbordamiento de buffer en SQL Server - CVE-2008-0106	Microsoft SQL Server 2005 Express Edition Service Pack 2	SQLServer2005-KB948108-IA64-ENU.exe SQLServer2005-KB948108-x64-ENU.exe SQLServer2005-KB948108-x86-ENU.exe
	Microsoft SQL Server 2005 Express Edition with Advanced Services Service Pack 2	SQLServer2005-KB948108-IA64-ENU.exe SQLServer2005-KB948108-x64-ENU.exe SQLServer2005-KB948108-x86-ENU.exe

- ✓ 9 "CONTROL DE ACCESO" aplicando los controles de Notificación de eventos y puntos débiles de seguridad de la información y el control de gestión de incidentes y mejoras de seguridad de la información.

INFORMIX:

- Vulnerabilidad en una función no especificada en "oninit.exe". Un atacante remoto podría ejecutar código arbitrario mediante una directiva "EXLAIN" especialmente manipulada.

  La vulnerabilidad se debe a un error de validación de entrada en el *oninit.exe* servicio. Un atacante autenticado remoto podría aprovechar esta vulnerabilidad para provocar un desbordamiento de búfer mediante el envío de datos maliciosos en el sistema vulnerable utilizando el puerto TCP 1526. El desbordamiento de búfer podría provocar que el servicio afectado se bloquee o permitir al atacante ejecutar código arbitrario con los privilegios del servicio.

  oninit.exe descripción es un archivo de proceso de una empresa desconocida que pertenece a un producto desconocido.

  Este archivo no está firmado digitalmente.

  Recomendaciones: Los administradores se les recomiendan aplicar las actualizaciones y las soluciones proporcionadas por IBM.

  Los administradores se les recomiendan restringir el acceso a la base de datos de usuarios de confianza.

  Los administradores se les aconsejan evitar posibles ataques externos mediante la implementación de una estrategia de cortafuegos fuerte.

Los administradores se les recomiendan monitorizar los sistemas críticos para detectar signos de actividad sospechosa.

Para solucionar estas vulnerabilidades se debe aplicar la cláusula:

- 8 “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMA DE INFORMACIÓN” se debe aplicar el Control de las vulnerabilidades técnicas, lo cual es buscar nuevas actualizaciones del sistema o software que se esta utilizando.

Vulnerabilidad	**Recomendación**
Vulnerabilidad en una función no especificada en "oninit.exe".	Actualización de software

- Han sido identificadas dos vulnerabilidades de seguridad posibles con los scripts de instalación para IBM® Informix® Dynamic Server (IDS), IBM® Informix® Client Software Development Kit (CSDK), y el IBM® Informix® Connect.

ÁMBITO

Los productos y los sistemas operativos siguientes son afectados:

Nombre de Producto	Versión(es) del Producto (s)	Proveedor de Hardware	Sistema Operativo
IBM® Informix® Dynamic Server	10.00	Todos	Unix, Linux
IBM® Informix® Client SDK	2.90	Todos	Unix, Linux
IBM® Informix® Connect	2.90	Todos	Unix, Linux

CAUSA

Las dos vulnerabilidades posibles son:

Los permisos por defecto de los scripts de instalación podrían permitir a un usuario no autorizado insertar código que podría comprometer la seguridad durante la instalación.

El proceso de instalación crea archivos temporales en el directorio /tmp. Es posible para un usuario con acceso a /tmp accesar estos archivos y por tanto comprometer la seguridad.

Los APAR reportados para estos defectos son:

Instalador de Producto	Script de instalación	ID del APAR
IBM® Informix® Dynamic Server	installserver	IC50785
IBM® Informix® Dynamic Server (Paquete)	ids_install	IC50784
IBM ® Informix ® CSDK	installclientsdk	IC50783
IBM® Informix® Connect	installconn	IC50786

SOLUCIÓN

Estos defectos están planificados para ser corregidos en:

Producto	Plataforma	Versión
IBM® Informix® Dynamic Server	Solaris Opteron, Linux zSeries	10.00.xC5R1
IBM® Informix® Dynamic Server	Todos los otros	10.00.xC6
IBM® Informix® CSDK	Todos	2.90.xC4R1
IBM® Informix® Connect	Todos	2.90.xC4R1

ACCESS:

- ✓ **Vulnerabilidad en Access ActiveX Control - CVE-2010-0814**

Una vulnerabilidad de ejecución remota de código existe en los controles de Access ActiveX debido a la forma en que los múltiples controles de ActiveX son cargados por Internet Explorer.

Un atacante que explotara exitosamente esta vulnerabilidad podría correr código arbitrario como un usuario con sesión iniciada. Si un usuario inicia sesión con privilegios de administrador, un atacante podría tomar control completo del sistema afectado. El atacante podría entonces instalar programas; visualizar, modificar, o eliminar datos; o crear nuevas cuentas de

usuario con todos los privilegios. Usuarios cuyas cuentas están configuradas para tener pocos privilegios sobre el sistema podrían ser menos impactados que usuarios que operan con privilegios de administrador.

- ✓ **Vulnerabilidad de variable no inicializada de ACCWIZ.dll - CVE-2010-1881**

  Una vulnerabilidad de ejecución remota de código existe en la forma en que el control FieldList ActiveX es utilizado por Microsoft Office e Internet Explorer.

  Un atacante que explotara exitosamente esta vulnerabilidad podría correr código arbitrario como un usuario con sesión iniciada. Si un usuario inicia sesión con privilegios de administrador, un atacante podría tomar control completo del sistema afectado. El atacante podría entonces instalar programas; visualizar, modificar, o eliminar datos; o crear nuevas cuentas de usuario con todos los privilegios. Usuarios cuyas cuentas están configuradas para tener pocos privilegios sobre el sistema podrían ser menos impactados que usuarios que operan con privilegios de administrador.

- ✓ **Vulnerabilidad CVE-2007-6026**

  Se trata de un problema de seguridad en un punto diferente pero de la misma librería del Access, que es la msjet40.dll. A través de esta falla, los

delincuentes han comenzado a expandir el troyano Keylogger.DB, que tiene como finalidad robar datos e información personal de la máquina de la víctima.

Existe una vulnerabilidad de saturación del buffer en Microsoft Jet Database Engine que podría permitir la ejecución remota de código en el sistema afectado. Un atacante podría explotar la vulnerabilidad enviando una consulta maliciosa a través de una aplicación que utilice el motor de base de datos (Microsoft Jet). La explotación exitosa de esta vulnerabilidad podría permitir al atacante tomar control total del sistema afectado. En consecuencia, el atacante podría instalar programas; ver, modificar o eliminar datos; o crear cuentas de usuario con los privilegios que desee. Los usuarios configurados con privilegios limitados son menos afectados que aquellos que operan con privilegios administrativos.

Vulnerabilidad	**Recomendación**
Vulnerabilidad en Access ActiveX Control - CVE-2010-0814	Ejecutar la siguiente actualización: office2003-KB981716-FullFile-ESN.exe

Vulnerabilidad de variable no inicializada de ACCWIZ.dll - CVE-2010-1881	Ejecutar la siguiente actualización: Access2007-kb979440-fullfile-x86-glb.exe
Vulnerabilidad CVE-2007-6026	Evitar descargar todo tipo de archivo desde Internet de origen desconocido, o incluso chequear bien los que se abren desde un correo electrónico. Y por supuesto, tener actualizado el antivirus. Aplicar una actualización de Microsoft Corp. Microsoft Windows 2000 Service Pack 4 Windows XP Service Pack 2 Windows XP Professional x64 Edition Windows Server 2003 Service Pack 1 Windows Server 2003 x64 Edition Windows Server 2003 con SP1 para sistemas basados en Itanium

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El estudio de normas de seguridad no solo va orientado a empresas medianas sino más bien a pequeñas empresas que están recién empezándose a formar, las cuales necesitan tener un buen comienzo y nada mejor que cuidando su información de una manera adecuada.

Una vez analizada la norma de seguridad de la información nos podemos dar cuenta que la información de las empresas es el activo mas valioso, por ello es necesario tomar las medidas para asegurarla.

La seguridad de la información conlleva seguridad en su confidencialidad, integridad y disponibilidad. Si se garantiza seguridad en los tres aspectos mencionados, se puede asegurar que la información esta segura.

Incendios, inundaciones, terremotos son algunas de las amenazas a las que ha estado expuesta la información tradicionalmente; sin embargo, con el desarrollo de sistemas y tecnologías, han surgido nuevas amenazas, que resultan ser un peligro para la

información, tales como el mapeo de sistemas, negación de servicio, gusanos, virus, troyanos, ataques de diccionario, hackeo, crackeo, entre otras.

Otra vulnerabilidad que se puede manifiesta repetidamente es la ausencia de una gestión adecuada para el acceso físico y lógico de los usuarios, incluyendo tarjetas de ingreso y claves seguras.

RECOMENDACIONES

Las empresas deben contar con normativa que regule las actividades operacionales para garantizar la seguridad de la información. No se presenta una gestión segura de los activos de información, ni se manifiesta preocupación suficiente en la inducción sobre seguridad de la información al personal.

También se deben tener en cuenta la implementación de una Política de seguridad permitirá controlar de mejor manera las actividades realizadas por los usuarios y garantizar la seguridad de la información asociada a la entrega de los servicios. Mediante la documentación y registro de todos los procedimientos será posible monitorear las actividades, disponer de información útil para futuros eventos y conservar la información necesaria para auditorías.

Las empresas deben contar con la implementación del SGSI, la confidencialidad, integridad y disponibilidad de la información, estarán garantizadas; este factor resultará decisivo para los clientes en la selección de un proveedor, al ser un elemento fundamental y diferenciador en el mercado. Sin la implementación del SGSI, no se contará con el respaldo de garantizar la seguridad de la información para los clientes, ocasionando que éstos opten por otra opción que les ofrezca seguridad.

Pero antes de desarrollar un SGSI en una organización, es necesario tener conocimiento de la misma. Es recomendable conocer su estructura, los productos o servicios que brinda, la infraestructura y funcionamiento de sus redes, los activos de información que posee. Una vez conocidos éstos, se debe proceder a realizar la valuación de riesgos para determinar qué acciones se deben tomar.

Se debe tomar en cuenta que diariamente se desarrollan amenazas nuevas. Ante esta situación, se recomienda analizar la seguridad de la información de una organización y sus controles de seguridad con mucha regularidad; es recomendable realizar los análisis básicos al menos una vez a la semana, y los minuciosos al menos una vez trimestralmente.

No esperar a que se produzca un ataque a la seguridad de la información, para tomar acciones correctivas para contrarrestarlo. Lo ideal es adoptar acciones preventivas antes que correctivas.

Si en una organización se desea implementar una normativa de seguridad de la información, es recomendable analizar las posibles opciones. Varias organizaciones en el Ecuador en su mayoría públicas basan su funcionamiento en la Norma ISO 9001, sobre Gestión de Calidad; en este caso, resulta muy conveniente la utilización de las Normas ISO 27000, sobre seguridad de la información, pues éstas guardan relación.

BIBLIOGRAFÍA

LIBROS

SILBERSCHATZ • KORTH • SUDARSHAN. (2002). Fundamentos de bases de datos. España.

C. J. Date. (2001) Introducción a los sistemas de bases de datos 7ma edición.

RAMEZ ELMASRI. SHAMKANT B. NAVATHE. Fundamentos de sistemas de bases de datos 5ta edición

Olga Pons Capote. (2005). Introducción a las bases de datos: el modelo relacional

Peltier, T. (2001). Information Security Risk Analysis. Auerbach. London.

DIRECCIONES WEB

Diario HOY. (20 de diciembre del 2010). **Robos por Internet dejan pérdidas por cerca de $500 mil en 2010** Extraído desde **http://www.hoy.com.ec/noticias-ecuador/los-ciberpiratas-al-acecho-448467.html**

Norma. (2011). Extraído desde **http://www.ilo.org/global/standards/lang-es/index.htm**

Seguridad (15 de septiembre del 2009). Extraído desde **http:// www.seguridad.gob.ec/ wp-content/uploads/downloads/2012/07/01 _ LEY_ DE _SEGURIDAD_PUBLICA_Y_DEL_ESTADO.pdf**

Norma de seguridad. (2010). Extraído desde **http://www.intertek-sc.com/espanol/our_services/ISO_27001/**

Introducción a la Seguridad de información. (2009). Extraído desde **http://www.gestion-calidad.com/seguridad-informacion.html**

Seguridad de la información (19 de agosto del 2010). Extraído desde **http://seguridadinformacioncolombia.blogspot.com/2010/08/alineando-cobit-41-itil-v3-e-iso-27002.html**

Normas ISO27000. (2011) Extraído desde **http://www.iso27000.es/iso27000.html**

ANEXO 1

DISTRIBUCIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002

1. POLÍTICA DE SEGURIDAD

1.1 Política de seguridad de la información

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1.2 Organización interna

Objetivo: Manejar la seguridad de la información dentro de la organización. Se debe establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. La gerencia debe aprobar la política de seguridad de la información, asignar los roles de seguridad, coordinar y revisar la implementación de la seguridad en toda la organización.

1.3 Grupos o personas externas

Objetivo: Mantener la seguridad de la información y los medios de procesamientos de información de la organización que son ingresados, procesados, comunicados a, o manejados por grupos externos. La seguridad de la información y los medios de procesamiento de la información de la organización no deben ser reducidos por la introducción de productos y servicios de grupos externos.

3. GESTIÓN DE ACTIVOS

1.4 Responsabilidad por los activos

Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales. Todos los activos deben ser inventariados y contar con un propietario nombrado. Los propietarios deben identificar todos los activos y se debe asignar la responsabilidad por el mantenimiento de los controles apropiados.

1.5 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel de protección apropiado. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información. La información tiene diversos grados de confidencialidad e importancia.

4. SEGURIDAD DE RECURSOS HUMANOS

1.6 Antes del empleo

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios. Las responsabilidades de seguridad deben ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo.

1.7 Durante el empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

1.8 Terminación o cambio de empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada. Se deben establecer las responsabilidades para asegurar que la salida de la organización del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

5. SEGURIDAD FÍSICA Y AMBIENTAL

1.9 Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

1.10 Seguridad de los equipos

Objetivo: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización. Se debe proteger el equipo de amenazas físicas y ambientales. La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no-autorizado a la información y proteger contra pérdida o daño. Esto también debe considerar la ubicación y eliminación del equipo.

6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1.11 Procedimientos y responsabilidades operacionales

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información. Se deben establecer las responsabilidades y procedimientos para la

gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados. Cuando sea apropiado, se debe implementar la segregación de funciones para reducir el riesgo de negligencia o mal uso deliberado del sistema.

1.12 Gestión de la entrega del servicio de terceros

Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

1.13 Planeación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallas en el sistema. Se requiere de planeación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido. Se deben realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

1.14 Protección contra el código malicioso y móvil

Objetivo: Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

1.15 Respaldo o Back-Up

Objetivo: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

1.16 Gestión de seguridad de la red

Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

1.17 Gestión de medios

Objetivo: Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales.

1.18 Intercambio de información

Objetivo: Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.

1.19 Servicios de comercio electrónico

Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.

1.20 Monitoreo

Objetivo: Detectar las actividades de procesamiento de información no autorizadas.

7. CONTROL DEL ACCESO

1.21 Requerimiento del negocio para el control del acceso

Objetivo: Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

1.22 Gestión de acceso del usuario

Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

1.23 Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información, evitar el robo de información de los medios de procesamiento de la información. La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

1.24 Control de acceso a la red

Objetivo: Evitar el acceso no autorizado a los servicios de la red. Se debe controlar el acceso a los servicios de redes internas y externas.

1.25 Control del acceso al sistema operativo

Objetivo: Evitar el acceso no autorizado a los sistemas operativos.

1.26 Control de acceso a la aplicación y la información

Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

1.27 Computación y tele-trabajo móvil

Objetivo: Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles.

8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1.28 Requerimientos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.

1.29 Procesamiento correcto en las aplicaciones

Objetivo: Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

1.30 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.

1.31 Seguridad de los archivos del sistema

Objetivo: Garantizar la seguridad de los archivos del sistema.

1.32 Seguridad en los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.

1.33 Gestión de la Vulnerabilidad Técnica

Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

9. GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN

1.34 Reporte de los eventos y debilidades de la seguridad de la información

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

1.35 Gestión de los incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1.36 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

Objetivo: Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

11. CUMPLIMIENTO

1.37 Cumplimiento de los requerimientos legales

Objetivo: Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

1.38 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

1.39 Consideraciones de auditoría de los sistemas de información

Objetivo: Maximizar la efectividad y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

ANEXO 2

APLICACIÓN DE LA NORMA ISO/IEC 27002

Antecedentes

Encontrándonos en el desarrollo de la tesis de tema: "CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LAS BASES DE DATOS Y SU EFECTO EN EL RIESGO DE LA INFORMACIÓN DE LAS EMPRESAS DE GUAYAQUIL. PROPUESTA PARA REDUCIR EL RIESGO DE LAS BASES DE DATOS QUE NO CUMPLEN LAS NORMATIVAS", la empresa GELINI S.A., nos da las facilidades para implementar la norma ISO 27002.

Confidencialidad:

Todos los datos expuestos en esta implementación respecto a la compañía Constructora GELINI serán considerados solo para la utilización en la presente tesis.

Hipótesis:

- El cumplimiento de normas de seguridad de la información logra aumentar los estándares de calidad con lo cual se aumenta continuamente la satisfacción de la empresa y sus clientes, logrando el crecimiento de la empresa.
- Los riesgos de robo y/o pérdida de información disminuyen en un gran porcentaje cuando se aplican normas de seguridad.

Importancia

La Evaluación de la seguridad de información resulta útil para:

- Validar y redefinir las actividades de la empresa (seguridad de información)
- Tener la información con el sistema de gestión de seguridad de información (integridad, disponibilidad, confiabilidad)

Ventajas

- Mejorar la seguridad, mediante la retroalimentación
- Identificar vulnerabilidades a tiempo
- Disminución de riesgos
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, entre otras).

- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

Metodología de ejecución de auditoría:

1. Cláusulas a auditar
2. Manual de proceso de cláusulas
3. Indicador de calificación
4. Porcentaje de incidencia de los procesos
5. Evaluación final
6. Evaluación de riesgo
7. Medidas correctivas – oportunidades de mejoras
8. Conclusiones y recomendaciones

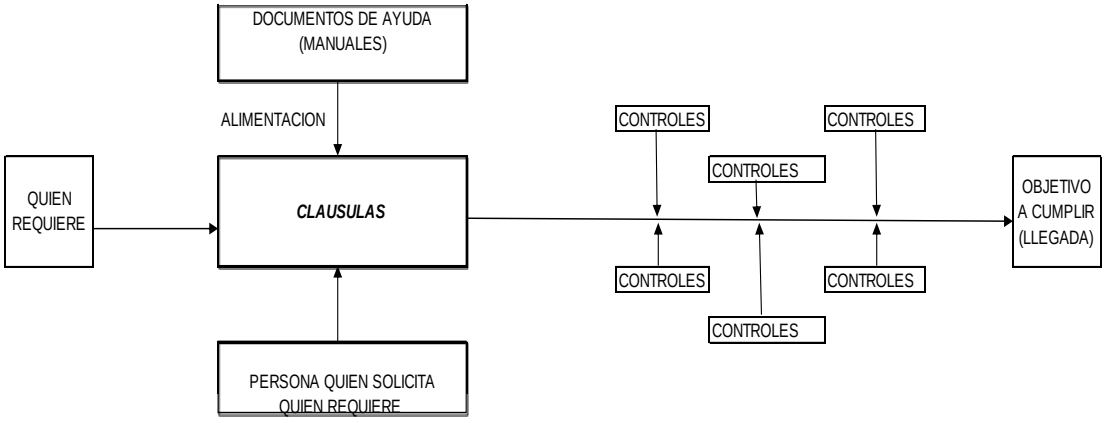
Cláusulas a auditar:

Para la implementación de la norma ISO/IEC 27002 nos vamos a basar en las 11 cláusulas detalladas a continuación:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Manual de proceso de cláusulas

Se detalla a continuación los procesos de las once cláusulas donde se trabajó en los procesos con la siguiente estructura:



Estadística:

CUADRO GENERAL DE ESTADISTICA DE INCUMPLIMINETOS POR EMPRESAS ENCUESTADAS

	PREGUNTAS										
	1	2	3	4	5	6	7	8	9	10	
EMPRESAS	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	
1											0
2				1		1				1	3
3								1		1	2
4								1		1	2
5						1		1		1	3
6				1						1	2
7										1	1
8				1	1	1				1	4
9											0
10				1	1	1			1	1	5
11		1		1	1	1			1	1	6
12		1		1	1				1	1	5
13		1		1	1	1			1	1	6
14		1				1		1	1	1	5
15		1		1	1					1	4
16		1		1	1	1				1	5
17		1				1				1	3
18		1		1	1					1	4
19		1		1	1	1				1	5
20		1		1	1	1		1		1	6
21											0
22				1	1	1		1	1	1	6
23				1	1	1		1	1	1	6
24		1		1	1	1			1	1	6
25		1		1	1				1	1	5
26				1	1				1	1	4
27					1	1			1	1	4
28				1	1	1			1	1	5
29				1		1		1	1	1	5
30				1		1			1	1	4
31				1	1			1	1		4
32		1		1	1	1			1	1	6
33				1	1	1		1	1	1	6
34				1	1	1			1	1	5
35				1	1			1	1	1	5
36				1	1				1	1	4
37				1	1	1		1	1	1	6
38				1	1	1			1	1	5
39		1	1	1	1	1				1	6
40	1	1	1	1	1		1	1		1	8
41		1	1	1	1					1	5
42	1	1	1	1	1	1	1	1		1	9
43				1	1	1				1	4
44		1	1			1		1		1	5
45				1		1				1	3
46				1		1				1	3
47		1	1	1	1	1		1	1	1	8
48		1	1	1	1	1		1	1	1	8
49				1	1	1			1	1	5
50				1					1	1	3
51				1					1	1	3
52				1	1	1			1	1	5
53				1	1	1			1	1	5
54			1	1	1	1				1	5
55			1	1				1		1	4
56			1	1						1	3
57				1	1	1				1	4
58				1	1	1		1		1	5
59				1	1	1				1	4
60				1	1			1	1	1	5
TOTAL DE INCUMPLIMIENTOS	2	20	10	49	40	38	2	20	30	56	267
TOTAL DE INCIDENCIAS % (PESO)	0,75	7,49	3,75	18,35	14,98	14,23	0,75	7,49	11,24	20,97	100,00%
PORCENTAJE DE INCUMPLIMIENTO RESPECTO A LAS EMPRESAS	3,33	33,33	16,67	81,67	66,67	63,33	3,33	33,33	50,00	93,33	
		CONSULTORAS									
		CONSTRUCTORAS									

Porcentaje de incidencia de los procesos (estadística)

Basándonos en el cuadro de porcentajes de incidencias respecto al total de incumplimiento se determina la calificación de las cláusulas a implementar:

CUADRO DE INCIDENCIAS DEL INCUMPLIMIENTO & CLAUSULAS

CLAUSULAS	PUNTUACION MAXIMA	PREGUNTAS	% INCIDENCIA
1. Política de Seguridad de la Información.	4	1 CONOCIMIENTO DE NORMAS DE SEGURIDAD	8,24
11. Cumplimiento.	5	2 CUMPLIMIENTO DE NORMAS DE SEGURIDAD	
2. Organización de la Seguridad de la Información.	5	5 EXISTENCIA DE POLITICAS DE SEGURIDAD	14,98
3. Gestión de Activos de Información.	3	7 ACTIVOS IMPORTANTES	0,75
4. Seguridad de los Recursos Humanos.	6	6 ASIGNACION DE FUNCIONES Y /O ROLES	14,23
5. Seguridad Física y Ambiental.	6	9 CONTROLES DE SEGURIDAD	14,98
10. Gestión de Continuidad del Negocio.	4	3 CONOCIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
6. Gestión de las Comunicaciones y Operaciones.	11	8 RESPALDO DE INFORMACION	46,82
7. Control de Accesos.	8	4 BASES DE DATOS UTILIZADAS	
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	7	10 RIESGOS	
9. Gestión de Incidentes en la Seguridad de la Información.	5		
TOTAL DE CALIFICACION	64	**TOTAL**	100,00

Dado este cuadro se determina que:

- ✓ La calificación máxima de la cláusula 1 Política de Seguridad de la Información y cláusula 11 Cumplimiento su puntaje máximo será de 9 puntos teniendo un total de 8.24 % de incidencia, por lo expuesto si no cumple con la

puntuación máxima será calificado en parte proporcional sobre su total de incidencias.

- ✓ La calificación máxima de la cláusula 2 Organización de la Seguridad de la Información su puntaje máximo será de 5 puntos teniendo un total de 14.98 % de incidencia, por lo expuesto si no cumple con la puntuación máxima será calificado en parte proporcional sobre su total de incidencias.

- ✓ La calificación máxima de la cláusula 3 Gestión de Activos de Información su puntaje máximo será de 3 puntos teniendo un total de 0.75 % de incidencia, por lo expuesto si no cumple con la puntuación máxima será calificado en parte proporcional sobre su total de incidencias.

- ✓ La calificación máxima de la cláusula 4 Seguridad de los Recursos Humanos su puntaje máximo será de 6 puntos teniendo un total de 14.23 % de incidencia, por lo expuesto si no cumple con la puntuación máxima será calificado en parte proporcional sobre su total de incidencias.

- ✓ La calificación máxima de la cláusula 5 Seguridad Física y Ambiental y cláusula 10 Gestión de Continuidad del Negocio su puntaje máximo será de 10 puntos teniendo un total de 14.98 % de incidencia, por lo expuesto si no

cumple con la puntuación máxima será calificado en parte proporcional sobre su total de incidencias.

- ✓ La calificación máxima de la cláusula 6 Gestión de las Comunicaciones y Operaciones, cláusula 7 Control de Accesos, cláusula 8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, y cláusula 9 Gestión de Incidentes en la Seguridad de la Información su puntaje máximo será de 31 puntos teniendo un total de 46.82 % de incidencia, por lo expuesto si no cumple con la puntuación máxima será calificado en parte proporcional sobre su total de incidencias.

Indicador de calificación:

La escala de calificación general para la seguridad de información será de:

RANGO DE PONDERACION	DESCRIPCION	RECOMENDACIONES
90-100	CUMPLE	* OK
70-89	CONFORMIDAD	* APLICAR CONTROLES ESPECIFICOS - OPORTUNIDADES DE MEJORA
60-69	NO CONFORMIDAD	* APLICAR POLITICA DE SEGURIDAD DE INFORMACION
0-59	NO CUMPLE	* APLICAR POLITICA DE SEGURIDAD DE INFORMACION

Evaluación final del riesgo (parámetros de calificación)

La empresa GELINI, fue evaluada en el cumplimiento de la norma ISO 27002, obteniendo una calificación de 81.16% estando en el rango de calificación de **conformidad**, detallado en el siguiente cuadro:

	CALIFICACION			
CLAUSULASA AUDITADAS	MAXIMA	COEFICIENTE	INCIDENCIA	PUNTAJE
1 POLÍTICAS DE SEGURIDAD	4	4	8,24	3,662
11 CUMPLIMIENTO	5	4		3,660
2 ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN	5	5	14,98	14,980
3 GESTIÓN DE ACTIVO	3	2	0,75	0,500
4 SEGURIDAD DE RECURSOS HUMANOS	6	3	14,23	7,120
5 SEGURIDAD FÍSICA Y AMBIENTAL	6	6	14,98	8,990
10 GESTIÓN DE CONTINUIDAD DEL NEGOCIO	4	3		4,490
6 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	11	9	46,82	13,590
7 CONTROL DE ACCESO	8	6		9,060
8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	7	5		7,550
9 GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN	5	5		7,550
TOTAL	64	52	100,00	81,16

Por lo cual se puede determinar que la empresa incurre en los siguientes riesgos:

RIESGO	CLAUSULA	CONTROL
Pérdida y / o robo de información, fraude y mal uso de medios	3 GESTIÓN DE ACTIVO	Responsabilidad de activos
		Uso Aceptable de activos
	4 SEGURIDAD DE RECURSOS HUMANOS	Terminación o cambio de empleo
Fallas y/o desastres en los sistemas de información o procesos comerciales	6 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	Procedimientos y responsabilidad operacionales
		Gestión de seguridad de la red
	10 GESTIÓN DE CONTINUIDAD DEL NEGOCIO	Pruebas, mantenimientos y re-evaluación del plan de contingencia del negocio
Negligencia o mal uso deliberado del sistema (información)	4 SEGURIDAD DE RECURSOS HUMANOS	Terminación o cambio de empleo
	6 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	Procedimientos y responsabilidad operacionales
Divulgación no autorizada, modificación, eliminación o destrucción de activos (información)	7 CONTROL DE ACCESO	Gestión de acceso del usuario
		Control de acceso al sistema operativo
	8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	Controles criptógrafos
Alteraciones en el funcionamiento de equipo de computo	8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	Procedimientos correctos en las aplicaciones
		Seguridad de archivos del sistema
		Gestión de la vulnerabilidad técnica
	10 GESTIÓN DE CONTINUIDAD DEL NEGOCIO	Pruebas, mantenimientos y re-evaluación del plan de contingencia del negocio

Medidas correctivas

La empresa GELINI, debe aplicar controles específicos – oportunidades de mejora en los controles no cumplidos detallados a continuación:

- ✓ Uso de activos
- ✓ Responsabilidad de terminación (empleo y/o contratos)
- ✓ Retiro de derecho de acceso
- ✓ Segregación de responsabilidades
- ✓ Seguridad en redes
- ✓ Gestión de acceso (base de datos)
- ✓ Control de acceso al sistema operativo
- ✓ Controles criptográficos
- ✓ Procesos correctos en aplicaciones (al momento de requerimiento de otra aplicación o de actualización de la misma)
- ✓ Pruebas del plan de contingencia
- ✓ Consideración de auditorías en los sistemas de información

Conclusiones y recomendaciones

En base a la implementación de la norma en la compañía GELINI se determina que el cumplimiento de normas de seguridad de la información si logra aumentar los estándares de calidad, con lo cual, se aumenta continuamente la satisfacción de la empresa y sus clientes, logrando el crecimiento de la empresa.

Así mismo se puede detectar a tiempo las vulnerabilidades y/o riesgo en la empresa, en especial el riesgo de robo y/o pérdida de información disminuyen en un gran porcentaje cuando se aplican normas de seguridad.

Se recomendó a la empresa aplicar las medidas correctivas en los controles antes descritos, deben tomar en cuenta los siguientes puntos para mejorar los controles:

- Identificar, documentar e implementar reglas para el uso correcto de medios de procesamiento de información, se puede implementar un acta de recepción por cada medio de procesamiento de información, la cual contenga: nombre de la persona encargada, lugar donde puede ser utilizada, fecha y hora de entrega, y firmas de responsabilidad
- Se debe incluir en los contratos de trabajo ya definidos por el presidente, las responsabilidades de cuando este termina o cambia de empleo, así mismo los derechos de acceso que pueda tener a la información de la empresa; una vez que los contratos se dieran por terminados se debe de retirar cualquier derecho de acceso a la información que mantenga vigente.
- La empresa debe de tener en consideración la revisión de las funciones o responsabilidades del departamento administrativo y contable, aplicando segregación de deberes ya que estos departamentos están cumpliendo las funciones de un técnico en sistema, lo cual se recomienda asignar a una persona capacitada para el manejo del sistemas contable, redes,

mantenimiento de equipo de cómputo, entre otros; para así evitar alteraciones en el funcionamiento de equipo de cómputo, negligencia o mal uso deliberado del sistema (información).

- Se debe identificar e incluir las características de seguridad, niveles de servicios y requerimientos de gestión de todos los servicios de redes, ya sean que estos servicios sean provistos externamente.
- Se determinó que la base de datos que utiliza la empresa no posee control de acceso se recomienda consultar a su proveedor la migración de sus datos a una base de datos más segura, y/o verificar costo – beneficio, el cambio de sistema con una base de datos más segura.
- Se debe evitar el acceso no autorizado, se debe colocar contraseña al sistema operativo, al acceso a la red, cuentas de usuarios de cada ordenador. Además se deben cerrar las secciones inactivas después de un periodo de inactividad definido
- Se deben implementar una política de uso de controles criptográficos, para así la información que se envía por red y correo, sea protegida su confidencialidad, autenticidad o integridad.
- Se debe establecer procedimientos de control para la instalación de software en cualquier ordenador de la empresa con previa autorización del jefe inmediato del área.

- Para reducir el riesgo de Fallas y/o desastres en los sistemas de información o procesos comerciales, debe evaluarse y/o probarse el plan de contingencia en los períodos que sean designados por el presidente.

Caso de estudios:

IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27002 "SEGURIDAD DE LA INFORMACIÓN", A LA COMPAÑÍA GELINI S.A.

Reseña Histórica

La compañía fue constituida el 22 de junio del 2000, con la finalidad de brindar servicios de construcción con empresas tantos públicas como privadas.

Teniendo como clientes principales al: Gobierno Autónomo Descentralizado Provincial de Santa Elena, Gobierno Autónomo Descentralizado Provincial del Guayas, Universidad Estatal de Milagro, Universidad Estatal de Guayaquil, entre otras.

La empresa está representada por su Presidente ingeniero civil (describirlo) el cual es responsable de toda la parte administrativa y legal de la empresa.

La empresa al momento de la auditoría mantiene vigente entre otros:

- ✓ Manual de gestión de calidad (SGS)
- ✓ Sistema contable Palmera (base de datos FoxPro)
- ✓ Reglamento interno de trabajo aprobado por el Ministerio de Relaciones Laborables

- ✓ Licencias: Windows 7, Microsoft office, AutoCAD
- ✓ Contrato de trabajos legalizados en el ministerio de relaciones laborables

Organigrama de Empresa:

ORGANIGRAMA ESTRUCTURAL DE GELINI S.A.