CARRERA DE COMPUTACIÓN

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA

TEMA:

AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ

AUTORES:
JUAN JOSÉ FRANK MONTESDEOCA
MERCEDES CECIBEL ROMERO PINO

TUTOR:
ING. GUSTAVO GABRIEL MOLINA GARZÓN, MS

CALCETA, JULIO 2016

DERECHOS DE AUTORÍA

Juan José Frank Montesdeoca y Mercedes Cecibel Romero Pino, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

.....	….....
JUAN J. FRANK MONTESDEOCA	**MERCEDES C. ROMERO PINO**

CERTIFICACIÓN DE TUTOR

Gustavo Gabriel Molina Garzón certifica haber tutelado la tesis **AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ**, que ha sido desarrollada por Juan José Frank Montesdeoca y Mercedes Cecibel Romero Pino, previa la obtención del título de Ingeniero en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

…..….....
ING. GUSTAVO G. MOLINA GARZÓN, MS.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ**, que ha sido propuesta, desarrollada y sustentada por Juan José Frank Montesdeoca y Mercedes Cecibel Romero Pino, previa la obtención del título de Ingeniero en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

.....	…….....
ING. RAMÓN J. MOREIRA PICO, MGS	LCDO. JOSÉ G. INTRIAGO CEDEÑO, MGS
MIEMBRO	**MIEMBRO**

.....

ING. LUIS C. CEDEÑO VALAREZO, MGS

PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de una educación superior de calidad y en la cual hemos forjado nuestros conocimientos profesionales día a día.

A todos y cada uno de los catedráticos que fueron fuente principal de conocimientos y apoyo académico hacia nosotros especialmente al Ing. Gustavo Molina quien fue nuestro guía en el transcurso y culminación de nuestro trabajo.

LOS AUTORES

DEDICATORIA

Este trabajo va dedicado principalmente a Dios por regalarme la oportunidad de vivir para ver este sueño hecho realidad, por ser mi guía y apoyo en cada momento vivido.

A mis padres, pilar fundamental en mi vida, les dedico todo mi esfuerzo, en reconocimiento a todo el sacrificio puesto para que esto sea posible, se merecen esto y mucho más, a mis hermanos por su apoyo infinito porque siempre estarán ahí para cuando los necesite, a mis sobrinos, a quienes amo con mi vida, quienes con su inocencia y amor puro pueden arrancarme una sonrisa hasta en el momento más duro; a mi familia en general.

A mis amigos, con quienes he compartido los mejores momentos y las mejores experiencias de mi vida, por ser ese apoyo, por tener las palabras precisas para animarme y empujarme hacia adelante, por enseñarme el verdadero significado de la amistad.

A todos ustedes… GRACIAS.

JUAN J. FRANK MONTESDEOCA

DEDICATORIA

Este trabajo es dedicado a Dios que con su bendición me ha permitido cumplir éste objetivo.

A mis padres, abuelos y hermanos dueños de mi inspiración, de quienes con ellos aprendí que el principio de la vida es predicar con el ejemplo, a ellos quienes han sido el apoyo absoluto y pilar esencial en mi vida, los que con amor y entusiasmo están moldeando mi formación espiritual e intelectual para ser una profesional de bien, guiándome a cambiar defectos por cualidades y debilidades por fortalezas porque a través de sus enseñanzas me nutren de ímpetu cuando más lo necesito.

A mis profesores que con su sabiduría que compartieron me permitió desempeñar mis responsabilidades, a mis amigos y amigas que gracias al compartir a diario aprendimos de nuestros errores y saberes.

MERCEDES C. ROMERO PINO

CONTENIDO

CONTENIDO DE FIGURAS

CONTENIDO DE GRÁFICOS

CONTENIDO CUADROS

RESUMEN

La importancia de la auditoría de base de datos radica en la necesidad de mitigar riegos en la pérdida de datos, estas eventualidades son de fuerte amenaza para una institución, puesto que los datos que contienen los sistemas de información están expuestos a cualquier eventualidad; la auditoria aplicada a las instituciones de educación superior públicas de Manabí, permitió valorar la protección de sus datos, seguridad y la eficacia de sus procesos, todo ello se realizó mediante un examen metódico y puntual que permitió conocer su estado, sacando a relucir las anomalías presentadas. Como guía de la auditoría se utilizó la metodología OCTAVE, la misma que permitió realizar un análisis y posterior valoración de los riesgos que recaen sobre sus bases de datos, de la misma manera se realizó un estudio de normas y estándares vigentes, tanto nacionales como internacionales, que dieron la pauta para saber cómo debería de estar su seguridad, calidad, administración y la protección de sus datos, para la comprobación de dichos resultados se utilizó el coeficiente de concordancia de Kendall, que consiste en medir el grado correlación de cada una de las respuestas obtenidas, el cual dio como resultado un 0,13 de concordancia, concluyendo que las entidades auditadas cuentan con un bajo cumplimiento de la norma INEN-ISO / IEC 27000.

PALABRAS CLAVE

Base de Datos, auditoría, riesgos, Instituciones de Educación Superior, Kendall, ISO 27000

ABSTRACT

The importance of the audit database is the need to mitigate risks in data loss, such eventualities are strong threat to an institution, since the data contained in the information systems are exposed to any eventuality; the audit applied to public institutions of higher education of Manabi, allowed assessing data protection, safety and effectiveness of its processes, all this was done using a methodical and timely examination allowed to know their status, bringing out irregularities It is presenting their inappropriate administration. As a guide to audit the OCTAVE methodology was used, the same that allowed a national and international analysis and subsequent assessment of the risks that fall on their databases, in the same way a study of norms and standards in force was made, , which gave the pattern for how should be safety, quality, management and protection of their data, for verification of these results the coefficient matching Kendall, which measure the degree correlation was used for each of the applied questions, which resulted in a concordance 0.13, concluding that the audited entities have a low compliance INEN ISO / IEC 27000 standard.

KEY WORDS

Database, audit, risk, Higher Education Institutions, Kendall, ISO 27000

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Las instituciones que realizan gran parte de sus actividades por medio de sistemas informáticos, se deben alinear a políticas y medidas de protección adecuadas, que sirvan como guía para precautelar la seguridad de sus operaciones y preservar la seguridad de sus datos.

La información que genera una institución es su activo más importante y fuente principal para que gerentes y administrativos tomen decisiones basadas en ella; la mayoría de empresas se deben al procesamiento diario de un sin número de datos, por lo que resulta apropiado asegurarlos de manera eficiente, contando con las medidas de seguridad que garanticen la confiabilidad de sus operaciones.

Es por ello que las instituciones optan por la aplicación de auditorías que les permitan conocer el cumplimiento de normas y estándares vigentes; el campo de la auditoría resulta muy amplio y ha ido adaptándose a las nuevas tecnologías con el pasar de los años, resultado de ello ha surgido la auditoría informática, la misma que constituye un pilar fundamental en la organización, porque tanto los procesos, sistemas y estructuras físicas deben estar sometidas a controles periódicos.

La auditoría de bases de datos es un área reciente donde se ha inmiscuido la auditoría informática, debido a la importancia que recae sobre ellas y los datos que procesan; por ello y considerando que las instituciones de educación superior tienen a su disposición grandes bloques de información sobre sus actividades académicas, lo que la hace vulnerable a amenazas tanto físicas como lógicas, por lo que un manejo inadecuado podría ocasionar pérdidas económicas y credibilidad a la institución, resultando conveniente su identificación y minimización.

Con una auditoría a las bases de datos de gestión académica a la Escuela Superior Politécnica Agropecuaria de Manabí, la Universidad Técnica de

Manabí, la Universidad Eloy Alfaro de Manabí y la Universidad Estatal del Sur de Manabí, se podría determinar si existen algún tipo de proceso que afecten sus datos y operaciones, tomando medidas pertinentes que ayuden a una correcta administración garantizando con ello el cumplimiento de la Norma Técnica Ecuatoriana NTE INEN – ISO / IEC 27000.

Por lo antes escrito los autores presentan el siguiente problema de investigación:

¿Cómo determinar el nivel de cumplimiento de normas y estándares en la seguridad de las bases de datos de gestión académica en los sistemas de información de las Instituciones de Educación Superior (IES) públicas de Manabí?

1.2. JUSTIFICACIÓN

Actualmente las instituciones y empresas se ven en la obligación de almacenar la información de sus procesos organizacionales en bases de datos que garanticen su disponibilidad y seguridad, esto con la ayuda de políticas y normas que regulen su cumplimiento, ya que un descuido en su aplicabilidad ocasionaría anomalías como la divulgación de sus datos. Por tanto, la confiabilidad de los recursos que almacenan la información tiene cada vez mayor relevancia debido a la gran cantidad de procesos que manejan y la ayuda que éstos brindan.

Con esta investigación se pretende evaluar los niveles de seguridad de los datos que manejan los sistemas de información con los que cuentan las IES públicas de Manabí y con ello dar cumplimiento a la Ley Orgánica de Educación Superior (LOES, 2010) en su capítulo 2, Art. 8 literal h textualmente expresa, que uno de los fines de la educación superior es: “Contribuir con el desarrollo local y nacional de manera permanente, a través del trabajo comunitario o extensión universitaria”; de esta manera se busca aportar con temas relacionados a la auditoria informática.

Por lo antes escrito y rigiéndose al estatuto de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, que establece en el manual de sistema de investigación institucional, referente al reglamento de tesis de grado en su Art. 2 que todo tema de tesis estará relacionado con las líneas de investigación de la carrera del postulante, enmarcadas en las áreas y prioridades de investigación establecidas por la ESPAM-MFL, se propone desarrollar una auditoría informática a las bases de datos de gestión académica que se manejan en las IES públicas de Manabí.

Con esto, se dará a conocer el cumplimiento que las instituciones dan a las normas y estándares nacionales e internacionales para la seguridad de su información, evaluando e identificando posibles riesgos para posteriormente recomendar acciones de mejoras en el manejo y seguridad de los datos, aportando con ello a la erradicación de posibles vulnerabilidades existentes.

Por ello, al realizar la auditoria informática se pretende identificar cada una de las falencias generadas por el incumplimiento de la Norma Técnica Ecuatoriana NTE INEN – ISO / IEC 27000, y no solo garantizar la integridad y seguridad de las bases de datos y su información, sino que también el de las personas involucradas en su manipulación, concluyendo además con la mitigación de futuras eventualidades presentadas.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Auditar las bases de datos de gestión académica de las IES públicas de Manabí estableciendo concordancia en el nivel de cumplimiento de las normas y estándares de seguridad.

1.3.2. OBJETIVOS ESPECÍFICOS

- ✓ Identificar las bases de datos de los sistemas de gestión académica de las instituciones a auditar.
- ✓ Examinar la estructura y seguridad de los datos en los procesos de los sistemas de información.
- ✓ Analizar los riesgos que conllevan la falta de cumplimiento de normas y estándares en las bases de datos
- ✓ Elaborar informe de control de los sistemas de información considerando los hallazgos encontrados.

1.4. IDEA A DEFENDER

La aplicación de una auditoría de base de datos de gestión académica a las instituciones de educación superior públicas de Manabí, ayudará a comprobar si se cumplen las normas y estándares de seguridad de la información mitigando riesgos existentes en sus bases de datos.

CAPÍTULO II. MARCO TEÓRICO

2.1. LA UNIVERSIDAD PÚBLICA

Senplades (2010) asegura que uno de los ejes que atraviesa el cambio de mirada respecto a la universidad consiste en redefinirla como un bien público social, que hace referencia a interpretarla como un espacio de encuentro común; en el Ecuador las instituciones de educación superior se constituyeron como un espacio de reproducción de clase y de distinción social. En este nuevo marco, se forma un ambiente donde se da un encuentro entre diferentes grupos sociales y étnicos, así como también estratos económicos, territoriales o regionales y credos disímiles.

2.1.1. ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

Manabí es una provincia rica en variados recursos. Mas, los habitantes del cantón Bolívar han dirigido su mirada a la tierra, pródiga desde siempre y, en ese contexto, se han identificado con la agricultura y la ganadería. Ello exigía, en Calceta, la presencia de un centro de estudios superiores en las áreas agrícola y pecuaria, de manera que la población estudiantil, con dificultad para trasladarse a universidades fuera de la zona, pudiera alcanzar un título académico, a fin de servir más tarde, no solo al cantón, sino a toda la región. La ESPAM inicia sus labores con las carreras de Agroindustria, Medio Ambiente, Agrícola y Pecuaria. Posteriormente, mediante un estudio de mercado, se crea la carrera de Informática. Ante la demanda de nuevas carreras, los directivos de la ESPAM, no han escatimado esfuerzos para incrementar otras, de tipo empresarial. Es así como desde el año 2003 funcionan dos nuevos programas: Administración Pública y Administración de Empresas, los que se cumplen en horarios nocturnos, al igual que la Carrera de Informática. A partir del año 2007 y, producto de un estudio, los estudiantes tienen una nueva opción: Ingeniería en Turismo. Con ello se busca potenciar a la población manabita, ávida de lograr una profesión acorde con sus aspiraciones.

2.1.2. UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

La Universidad Laica “Eloy Alfaro” de Manabí tiene su sede en Manta, una de las cinco principales ciudades del Ecuador, la cual entrega un incuantificable aporte para que se convierta en una ciudad de pujante desarrollo. Es de carácter humanista, con una clara concepción laica en materia educativa que procura la más exigente libertad de enseñanza y cátedra, entendiendo al estudiante como el gran actor de su proceso de formación y al docente como el gran facilitador del futuro profesional. En este contexto concibe su oferta académica con la mas amplia diversidad, a efectos de responder a las diferentes aspiraciones de los jóvenes que desean seguir una carrera universitaria, entendiendo bien que los procesos educativos son procesos dinámicos por lo que anualmente reajusta su oferta educativa adecuándola a los requerimientos de la juventud y a la acelerada evolución del mundo contemporáneo.

2.1.3. UNIVERSIDAD TÉCNICA DE MANABÍ

El grupo de Universitarios Manabitas residentes en Quito, pidió oficialmente al Núcleo de Manabí de la Casa de la Cultura Ecuatoriana, la contribución con un número para su programa, con motivo de un aniversario más de su Asociación en la Universidad Central, a realizarse en Portoviejo. El principal número de este Programa, sería la conferencia del señor Doctor Alfredo Pérez Guerrero, Rector de la Universidad Central. En efecto, llegado a Portoviejo el señor Rector de la Universidad Central, se promovió la sesión de Mesa Redonda acordada, la misma que se instaló a las 6 de la tarde del día 15 de Abril del referido año, en los salones de la Casa de la Cultura Ecuatoriana Núcleo Manabí.

Constituida en su primera sesión el 22 de Abril de 1952 la Junta Pro-Universidad de Manabí, eligió a sus dignatarios y funcionarios, la cual asumió la tarea que le encomendó la Asamblea del 15 de Abril de 1952, con profunda emoción y gran sentido de responsabilidad. Sus Personeros, todos sin excepción, no desmayaron en su labor y sobre todo su fe y optimismo por el éxito de la causa que perseguían.

2.1.4. UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ

La Universidad Estatal del Sur de Manabí, es una Institución de Educación Superior Pública, tiene su domicilio en la ciudad de Jipijapa, provincia de Manabí, constituida por el Estado como persona jurídica sin fines de lucro, por lo que sin lesionar su autonomía constitucionalmente establecida, debe articular sus actividades con el Sistema de Educación Superior y el Plan Nacional de Desarrollo.

La Ley de Creación de la Universidad Estatal del Sur de Manabí, reconoce a la misma como parte del Sistema de Educación Superior del Ecuador; en virtud de lo cual goza de autonomía académica, administrativa y financiera, ejerce además sus actividades como institución de educación superior de grado y post grado, materializada en el carácter de institución de docencia universitaria, rendición obligatoria de cuentas y sometida a los principios de cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y del conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global.

2.2. BASE DE DATOS

Pinto (2011) señala que son recursos que recopilan todo tipo de información, para atender las necesidades de un amplio grupo de usuarios; para Romero (2009) las bases de datos son una colección compartida de datos lógicamente relacionados, junto con una descripción de ellos, que están diseñados para satisfacer las necesidades de información de una organización. Su tipología es variada y se caracterizan por una alta estructuración y estandarización de la información. Ambos sostienen que son un conjunto de información almacenada en un soporte legible por un ordenador y organizada internamente por registros y campos.

Kioskea (2014) manifiesta que una base de datos proporciona a los usuarios el acceso a datos, que pueden visualizar, ingresar o actualizar, en concordancia con los derechos de acceso que se les hayan otorgado, se convierte más útil a

medida que la cantidad de datos almacenados crece. Considera también que una base de datos puede ser local, es decir que puede utilizarla sólo un usuario y en un equipo, o puede ser distribuida, lo que implica que la información se almacena en equipos remotos y se puede acceder a ella a través de una red.

De acuerdo con Gómez, *et al (*2012) las acciones de un sistema aparte de ejecutar operaciones en la base de datos, pueden desencadenar un conjunto de eventos que constituyen información básica para la auditoría. Los eventos se dividen por tipos para disminuir el crecimiento de la información, facilitar su análisis y mantener la escalabilidad de la solución. Los eventos más comunes e identificados, se resumen a continuación:

- ✓ **Operación:** evento que registra los atributos generales relacionados con la estructura del sistema donde se ejecutó la acción y a qué actividad y proceso de negocio responde. Incluye, además, información sobre quién la ejecutó, en qué estructura de la jerarquía y desde que dirección IP.
- ✓ **Error:** es el que se desencadena producto de un error en la ejecución de una acción del sistema, pueden generarse por una falla en la codificación o en las tecnologías que soportan el sistema.
- ✓ **Excepciones:** los que se producen como consecuencia de la violación de reglas impuestas por el negocio o por las restricciones tecnologías del entorno.
- ✓ **Rendimiento:** es el que se activa si se quiere registrar información relacionada con el consumo de memoria, tiempo de respuesta y demás parámetros relacionados con la acción ejecutada.
- ✓ **Notificación:** se ejecuta como resultado de reglas definidas que traen consigo el envío de una alerta o aviso, se activan si se ejecuta una acción que contenga alguna de ellas y pueden enviarse por correo, teléfono, sistema, entre otras vías.
- ✓ **Validación:** se desencadena en el momento que se activa la validación de una acción ejecutada en el sistema, se establecen con el fin de regular la ejecución de ciertas acciones a través de condiciones.
- ✓ **Acceso:** el que se activa en el momento que se ejecuta o se trata de ejecutar una acción no autorizada en el sistema.

El registro de los eventos descritos anteriormente debe proveer la información necesaria para realizar análisis sobre el funcionamiento de los sistemas de información y sobre los procesos que el informatiza.

2.2.1. CLASIFICACIÓN DE BASE DE DATOS

Se pueden clasificar de varias maneras, de acuerdo al contexto que se esté manejando, la utilidad de las mismas o las necesidades que satisfagan.

2.2.1.1. SEGÚN LA VARIABILIDAD DE LOS DATOS

Para Prado (2011), existen dos tipos de bases de datos según su variabilidad, que son, las estáticas y las dinámicas.

2.2.1.1.1. BASES DE DATOS ESTÁTICAS

Son sólo de lectura y utilizadas primordialmente para almacenar datos históricos que posteriormente utilizarán para estudiar el comportamiento de un conjunto de datos a través del tiempo, relacionar proyecciones y tomar decisiones. (Prado, 2011)

2.2.1.1.2. BASES DE DATOS DINÁMICAS

En ellas la información almacenada se modifica con el tiempo, permitiendo actualizaciones como, actualización, borrado y adicción de datos, además de las operaciones fundamentales de consulta. (Prado, 2011)

2.2.1.1. SEGÚN SU CONTENIDO

Las bases de datos según su contenido se clasifican de la siguiente manera:

2.2.1.1.1. BASES DE DATOS BIBLIOGRÁFICAS

Como lo expresa Prado (2011) estas bases de datos solo contienen subrogantes de la fuente primaria, que permite localizarla; un registro de este tipo contiene información sobre el autor, fecha de publicación, editorial, titulo,

edición, puede contener también un resumen o extracto de la publicación original, pero nunca su texto completo.

2.2.1.1.2. BASES DE DATOS DE TEXTO COMPLETO

De acuerdo a Ramírez *et al* (2010) estas bases de datos almacenan fuentes primarias, como por ejemplo todo el contenido de todas las ediciones de una colección de revistas científicas.

2.2.2. SISTEMAS DE GESTIÓN DE BASE DE DATOS

Definimos un Sistema Gestor de Bases de Datos o SGBD, también llamado DBMS (Data Base Management System) como una colección de datos relacionados entre sí, estructurados y organizados, y un conjunto de programas que acceden y gestionan esos datos. La colección de esos datos se denomina Base de Datos o BD, (DB Data Base). Antes de aparecer los SGBD (década de los setenta), la información se trataba y se gestionaba utilizando los típicos sistemas de gestión de archivos que iban soportados sobre un sistema operativo. Éstos consistían en un conjunto de programas que definían y trabajaban sus propios datos. Los datos se almacenan en archivos y los programas manejan esos archivos para obtener la información. Si la estructura de los datos de los archivos cambia, todos los programas que los manejan se deben modificar; por ejemplo, un programa trabaja con un archivo de datos de alumnos, con una estructura o registro ya definido; si se incorporan elementos o campos a la estructura del archivo, los programas que utilizan ese archivo se tienen que modificar para tratar esos nuevos elementos. (McGraw-Hill, 2010)

2.2.3. MODELOS DE BASES DE DATOS

Mendoza (2013), menciona que las bases de datos también se pueden clasificar de acuerdo a su modelo de administración. Los modelos de datos no son cosas físicas; son abstracciones que permiten la implementación de un sistema eficiente de base de datos, a continuación, se nombran algunas de ellas.

2.2.3.1. BASES DE DATOS JERÁRQUICAS

Para Hernández, *et al* (2010) este modelo de base de datos se organiza en forma similar a un árbol, donde un nodo padre de información puede tener varios hijos, el que no tiene padre es llamado hijo y el que no tiene hijos se lo conoce como hojas; este modelo resulta útil en aplicaciones que manejan gran volumen de información y datos compartidos, permitiendo crear estructuras estables y de gran rendimiento.

2.2.3.2. BASES DE DATOS DE RED

Como lo expresa Prado (2010) este es un modelo distinto del jerárquico, su diferencia fundamental es la modificación del concepto de nodo, se permite que un mismo nodo tenga varios padres; considera también que fue una gran mejora con respecto al otro modelo, ya que este modelo es más utilizado por programadores que por usuarios finales.

2.2.3.3. BASES DE DATOS TRANSACCIONALES

Hernández, *et al* (2010) considera que el único fin de estas bases de datos es enviar y recibir datos a grandes velocidades, soy muy pocas comunes y están dirigidas al entorno de análisis de calidad, datos de producción e industrial, recolectan y recuperan datos a la mayor velocidad posible.

2.2.3.4. BASES DE DATOS RELACIONALES

Prado (2011) hace alusión a que este es el modelo utilizado en la actualidad para modelar problemas reales y administrar datos dinámicamente, en este modelo la forma y el lugar en el que se almacenan los datos no tiene mayor relevancia, lo que es considerado como una ventaja ya que es más fácil de entender y usar para un usuario esporádico de base de datos.

2.2.3.5. BASES DE DATOS MULTIDIMENSIONALES

Poblete (2011) manifiesta que el uso de base de datos multidimensionales (BDM) podría ofrecer importantes oportunidades de aplicación en el ámbito educacional. Una BDM es un repositorio de datos que proporciona un entorno

integrado para consultas de soporte a las decisiones que requieren de agregaciones, y de enormes cantidades de datos históricos.

2.2.3.6. BASES DE DATOS ORIENTADAS A OBJETOS

Meneses, *et al* (2011) recalca que en los sistemas de gestión de bases de datos orientados a objetos, un objeto se concibe como una abstracción del mundo real (en su parte estática similar a una entidad), atributos propios del objeto y un conjunto de métodos que corresponden al comportamiento de un objeto, por otra parte acota que las bases de datos relacionales y las orientadas a objetos, buscan especificar de una forma especializada y exhaustiva la formulación de un esquema conceptual dentro de un dominio dado.

2.2.3.7. BASES DE DATOS DEDUCTIVAS

Prado (2011) ha indicado que es un sistema de base de datos con la diferencia que permite hacer deducciones a través de inferencia, se basa principalmente en reglas y hechos que son almacenados en la base de datos, este modelo de base de datos es también llamado lógico, a raíz de que se basa en lógica matemática comúnmente usado en los también llamados sistemas expertos.

2.2.4. INTEGRIDAD DE LOS DATOS

Azán, *et al* (2014) testifica que uno de los pasos para garantizar la integridad de los datos, es a través de la realización de auditorías informáticas periódicas a las tecnologías de cómputo mientras que Gelbstein (2011) afirma que la definición de integridad de datos depende del profesional que la opere.

2.2.4.1. POR UN ENCARGADO DE SEGURIDAD

Lo define como la imposibilidad de que alguien modifique datos sin ser descubierto. Desde la perspectiva de la seguridad de datos y redes, la integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria. Si se examina el concepto de “integridad”, se podría concluir que no solo alude a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del

desarrollo de sistemas estructurados [SDLC], revisión de códigos fuente por expertos, pruebas exhaustivas, etc.), sino también a la integridad personal (responsabilidad, confianza, fiabilidad, etc.).

2.2.4.2. PARA UN ADMINISTRADOR DE BASES DE DATOS

Depende de que los datos introducidos en una base de datos sean precisos, válidos y coherentes. Es muy probable que los administradores de bases de datos también analicen la integridad de las entidades, la integridad de los dominios y la integridad referencial.

2.2.4.3. PARA UN ARQUITECTO O MODELADOR DE DATOS

Puede estar relacionada con el mantenimiento de entidades primarias únicas y no nulas. La unicidad de las entidades que integran un conjunto de datos se define por la ausencia de duplicados en el conjunto de datos y por la presencia de una clave que permite acceder de forma exclusiva a cada una de las entidades del conjunto.

2.2.4.4. PARA EL PROPIETARIO DE LOS DATOS

Puede ser un parámetro de la calidad, ya que demuestra que las relaciones entre las entidades están regidas por reglas de negocio adecuadas, que incluyen mecanismos de validación, como la realización de pruebas para identificar registros huérfanos.

2.2.4.5. PARA UN PROVEEDOR

La exactitud y coherencia de los datos almacenados, evidenciada por la ausencia de datos alterados entre dos actualizaciones de un mismo registro de datos. La integridad de los datos se establece en la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores.

2.3. SEGURIDAD INFORMÁTICA

Hernández (2010) señala que un sistema es seguro si se puede confiar en él y se comporta de acuerdo a lo esperado. La seguridad se basa por tanto en conceptos como la confianza y el acuerdo, la seguridad es un conjunto de

soluciones técnicas, métodos, planes que tienen como objetivo que la información que trata nuestro sistema informático sea protegida. Lo más importante es establecer un plan de seguridad en el cual se definan las necesidades y objetivos en cuestiones de seguridad.

De acuerdo con Montesino, *et al* (2013) la seguridad informática es la preservación de la confiabilidad, integridad y disponibilidad de la información, y que la misma no es un estado que se alcanza en determinado instante del tiempo y permanece invariable, sino que es un proceso continuo que necesita ser gestionado.

2.3.1. AMENAZAS

Nuñez, *et al* (2014) por su parte señala que cuando se menciona el concepto de seguridad informática y sus características principales es necesario referirse a las principales amenazas que pueden afectarla. Entre los riesgos que tienen más probabilidad de ocurrencia se encuentran el acceso lógico y físico no autorizado a las tecnologías, los desastres naturales, el robo o hurto parcial o total de equipamiento informático, los incendios, las fallas de fluido eléctrico, el fallo de hardware y software y la contaminación por virus informáticos.

2.3.2. TIPOS DE AMENAZAS

Según Rojas, *et al* (2012) las amenazas son clasificadas de la siguiente manera:

- **Origen Físico**: Las amenazas identificadas para este grupo, son aquellas que puedan afectar los activos por elementos de carácter físico ya sea por un evento natural, por degradación o fallas eléctricas.
- **Actos Originados por Criminalidad**: Las amenazas identificadas para este grupo son aquellas que pueden afectar los activos por situaciones como actos vandálicos, sabotaje, infiltraciones y ataques de hacker.
- **Infraestructura:** Las amenazas identificadas para este grupo son aquellas que pueden afectar los activos por diferentes tipos de problemas.
- **Hardware:** Las amenazas identificadas para este grupo son aquellas que afectan los activos por errores, fallas o degradación.

- **Nivel de Usuario:** Las amenazas identificadas para este grupo son aquellas que los activos por mal manejo, falta de capacitación o indiscreción de los usuarios.
- **Políticas:** Las amenazas identificadas en este grupo van asociadas a la mala implementación o administración de seguridad para los activos
- **Redes:** Las amenazas identificadas en este grupo son las que pueden afectar los activos en transmisión de datos, redes inalámbricas, redes alámbricas

2.3.3. ANÁLISIS Y GESTIÓN DE RIESGO

Capote, *et al* (2014) revela que los modelos estratégicos deben comprender la gestión de las actividades y servicios con una mirada estratégica para la organización, estos procesos pueden ser: Protección y control de los medios básicos, auditorías internas, acciones correctivas y preventivas y formación y capacitación de los recursos humanos.

Actualmente se utilizan una serie de modelos para realizar un proceso lógico y sistemático que puede ser utilizado cuando se toman decisiones para mejorar la efectividad y eficiencia de las empresas. Los modelos permiten identificar y estar preparados para lo que puede suceder, se trata de tomar acciones destinadas a eludir y reducir la exposición a costos u otros efectos de aquellos eventos que ocurran, en lugar de reaccionar después de que un evento haya ocurrido e incurrir en los costos que implican recuperar una situación. (Hernández *et al* 2013)

Herrera (2013) establece que un punto importante para la posible mejora en la gestión de los procesos de una organización lo constituye la auditoría, mediante la cual se valida la información y sus procesos. Para llevar a cabo un proceso correcto de auditoría es necesario contar con información fiable para conocer si estos se ejecutan dentro de los límites establecidos, ya que resulta imprescindible una correcta gestión de la información para así alcanzar un satisfactorio desempeño y evolución en la institución. Las violaciones de las normas específicas impuestas por la ley o las políticas dentro del

establecimiento pueden indicar que se ha cometido algún fraude o negligencia y una alerta sobre el particular resulta importante para la toma de decisiones.

Gutiérrez (2012) añade que una empresa puede afrontar un riesgo de cuatro formas diferentes: aceptarlo, transferirlo, mitigarlo o evitarlo. Si un riesgo no es lo suficientemente crítico para la empresa la medida de control puede ser aceptarlo, es decir, ser consciente de que el riesgo existe y hacer un monitoreo sobre él. Si el riesgo representa una amenaza importante para la seguridad de la información se puede tomar la decisión de transferir o mitigar el riesgo.

2.3.4. MATRIZ DE RIESGO Y CONFIANZA

BBMapfre (2014) expresa que toda organización está permeada por procesos, buenos o malos, eficientes o no, que representan la estela por donde sus actividades se desarrollan y cruzan toda su cadena de valores. Los eventos resultantes de esas actividades están casi siempre involucrados en una franja de riesgos y oportunidades, el mismo que acota que la matriz de riesgo se crea en función de la frecuencia y del impacto.

Según la Contraloría General del Estado CGE el riesgo de auditoría es lo opuesto a la seguridad de la auditoria, es decir, es el riesgo en que los estados financieros o el área que se esté examinando, contengan errores o irregularidades no detectadas, una vez que la auditoría ha sido completada. El riesgo de la auditoría se reduce con la reunión de la evidencia, cuánto más competente sea la evidencia reunida, menor es el riesgo de auditoría asumido, razón por la cual el nivel de confianza se eleva.

La calificación de riesgos de auditoría, requiere la siguiente información tabulada y referenciada con los documentos de respaldo.

- **COMPONENTE**: comprende el sistema o actividad importante evaluada, determinando las verificaciones a ser verificadas.
- **RIESGOS**: calificación del riesgo inherente y de control (A= Alto, M= Moderado, y B= Bajo), por cada una de las afirmaciones, con la justificación de su calificación.

- **CONTROLES CLAVE**: identificación de los controles clave potenciales que proporcionan satisfacción de auditoría.
- **PRUEBAS DE CUMPLIMIENTO Y SUSTANTIVAS**: detalle esquemático de los procedimientos prioritarios que deben incluirse como parte de los programas de auditoría.
- **ENFOQUE DE AUDITORÍA**: aquí se detalla el programa de auditoría a seguir.

2.3.5. POLÍTICAS DE SEGURIDAD

Rodríguez (2010) señala que la política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los “dueños” y permiten adoptar una buena actitud dentro de la organización.

De acuerdo a Godás *et al* (2011) hay que considerar las siguientes políticas necesarias:

2.3.5.1. POLÍTICAS DE USO ACEPTABLE

Determina que se puede hacer con los recursos de cómputo (equipo y datos) de la organización. También determinan lo que no se puede hacer con esos recursos. Indica la responsabilidad de los usuarios en la protección de la información que manejan y en qué condiciones puede afectar o leer datos que no les pertenezca (Godás, 2011).

2.3.5.2. POLÍTICAS DE CUENTAS DE USUARIO

Determina el procedimiento que hay que seguir para adquirir privilegios de usuarios en uno o más sistemas de información y la vigencia de estos derechos.

Además, quien tiene la autoridad de asignar estos privilegios y quienes no podrían recibir esos privilegios por causas legales. Debe exhibir explícitamente los deberes y derechos de los usuarios. Se explicará cómo y cuándo se deshabilitaran las cuentas de usuarios y que se hará con la información que contenga. Debe especificar claramente los detalles de los procedimientos de identificación y autenticación (Godás, 2011).

2.3.5.3. NORMATIVAS

Permiten a las organizaciones presentar y certificar un nivel de calidad ante sus usuarios y el público en general. Aunque en un principio fueron de interés para las grandes empresas, las normas ISO 27000 están siendo consideradas también por medianas empresas en Latinoamérica y el mundo. Además, las normas sirven para tener una guía de buenas prácticas que pueden ser de utilidad, incluso si la organización no desea o puede certificar la misma. (Bortnik, 2010).

La Administración Pública de forma integral y coordinada debe aprender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos. La comisión para la seguridad informática y de las tecnologías de la información y comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la información (EGSI), elaborado en base a la norma NTE INEN - ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”.

Según la Secretaría Nacional de la Administración Pública SNAP (2013) en el registro oficial numero 88 manifiesta que es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la administración pública central, institucional y que dependen de la función ejecutiva.

2.3.5.3.1. ISO/IEC 27000

Según manifiesta Ladino, *et al* (2011) la norma ISO 27000 es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Cada uno de los puntos exigidos en la norma pertenece a una etapa de un proceso: Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar), que se aplica para estructurar todos los procesos. Sin embargo, al momento de realizar la auditoría, a algunos puntos se les da más relevancia que a otros:

- ✓ **Política de seguridad**: debe incluir los objetivos de seguridad de la información de la organización, tener en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, estar alineada con la gestión de riesgo general, establecer criterios de evaluación de riesgo y ser aprobada por la Dirección.
- ✓ **Asignación de responsabilidades de seguridad**: En toda actividad debe existir un responsable. Durante el proceso de certificación cada tarea debe estar definida para que una o unas personas de la organización la realicen.
- ✓ **Formación y capacitación para la seguridad**: debe realizarse una concienciación de todo el personal en lo relativo a la seguridad de la información.
- ✓ **Registro de incidencias de seguridad**: durante el proceso, debe realizarse un registro de los eventos casuales (incidencias), y determinar su impacto y frecuencia. Determinar controles de detección y respuesta a dichos incidentes.
- ✓ **Protección de datos personales**: hacen parte de la información de la organización y por ello deben ser protegidos.
- ✓ **Derechos de propiedad intelectual**: contar con las licencias y/o permisos para el uso de software en la organización.

2.3.5.3.2. NORMAS DE CONTROL INTERNO

2.3.5.3.2.1. DESARROLLO Y ADQUISICIÓN DE SOFTWARE APLICATIVO

La norma de control interno 410-07 define que se deben considerar los siguientes aspectos:

La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique

2.3.5.3.2.2. MANTENIMIENTO Y CONTROL DE LA INFRAESTRUCTURA TECNOLÓGICA

La norma de control interno 410-09 define que se deben considerar los siguientes aspectos:

Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.

2.3.5.3.2.3. SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

La norma de control interno 410-10 define que se deben considerar los siguientes aspectos:
La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.

Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía a condicionada, esto es estabilizada y polarizada, entre otros.

2.3.5.3.2.4. ADMINISTRACIÓN DE SOPORTE DE TECNOLOGÍA DE INFORMACIÓN

La norma de control interno 410-12 define que se deben considerar los siguientes aspectos:

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.

Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información

Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software

malicioso y virus informáticos. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

2.4. AUDITORÍA INFORMÁTICA

Tanto Pons (2011) como Martínez (2012) concuerdan con que la auditoría informática es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio. Menciona también que existe un cuerpo de conocimientos, normas, técnicas y buenas practicas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la información tratada y almacenada a través del computador y equipos afines, todo esto con el fin de emitir una opinión o juicio. Por otro lado, Gómez, *et al* (2012) señala que la auditoría informática ha aumentado su importancia como resultado de su impacto en la prevención o detección de violaciones que afecten la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos de una organización.

Para Pérez (2011) los principales objetivos que constituyen la auditoría informática son el control y el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normativa general de la empresa en este ámbito, y la revisión de la eficaz gestión de los recursos informáticos materiales y humanos.

Sobre el papel del auditor dentro de las organizaciones Pons (2011) manifestó que se puede resumir en dos grandes tareas principales; la primera el apoyo del auditor interno, que es básicamente la definición y aplicación de controles sobre los procesos de negocio de las organizaciones, y la segunda es la auditoría de la gestión de los sistemas de información, que se plantea básicamente dos objetivos:

- ✓ Los sistemas de información soportan adecuada y eficientemente los procesos de negocio de las organizaciones.

- ✓ La información tratada por los sistemas de información dispone de un nivel de seguridad adecuado a su valor y a los riesgos asociados a su uso.

2.4.1. TIPOS DE AUDITORÍA INFORMÁTICA

2.4.1.1. LA AUDITORÍA INTERNA

Hernández (2010) manifiesta que la auditoría interna es una actividad que tiene por objetivo fundamental examinar y evaluar la adecuada y eficaz aplicación de los sistemas de control interno, velando por la preservación de la integridad del patrimonio de una entidad y la eficiencia de su gestión económica, proponiendo a la dirección las acciones correctivas pertinentes.

2.4.1.2. LA AUDITORÍA EXTERNA

Para Santillana (2013) la auditoría externa empieza su labor y continúa con el análisis de la forma como se alcanzaron éstos, su interés primario está en poder expresar una opinión sobre si sus estados han sido preparados de conformidad con las normas aplicables; por consiguiente, este auditor está más orientado hacia los resultados finales de los estados y la evidencia que soporta la validez de éstos.

2.4.1.3. AUDITORÍA OFIMÁTICA

Comprende los programas o aplicaciones que en conjunto sirven de herramienta para generar, procesar, almacenar, recuperar, comunicar y presentar la información en un lugar de trabajo, así como de forma doméstica. (Martínez, 2012).

2.4.1.4. AUDITORÍA DE REDES

Pons (2011) explica que la auditoría de redes se encarga de una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información. En primer instancia una gestión responsable de la seguridad es identificar la estructura física (hardware,

topología) y lógica (software, aplicaciones) del sistema, y hacerle un análisis de vulnerabilidad para saber en qué grado de exposición se encuentra la entidad de esta manera estudiada la "radiografía" de la red, se procede a localizar sus falencias más críticas, para proponer una estrategia de saneamiento de los mismos; un plan de contención ante posibles incidentes y un seguimiento continuo del desempeño del sistema.

2.4.1.5. AUDITORÍA DE LA SEGURIDAD

En concordancia con Azán *et al.* (2014) una auditoría de seguridad informática es un concepto relevante para la seguridad de la información, el cual según el autor Ruiz, (2011): “es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, los servidores y las redes de comunicaciones”. Durante una auditoría de seguridad informática se realizan las auditorías de la seguridad lógica y auditoría de las comunicaciones.

2.4.1.6. AUDITORÍA DE BASE DE DATOS

Ramírez *et al* (2010) considera que este tipo de auditorías permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar: quién accede a los datos, cuándo se accedió a los datos, desde qué tipo de dispositivo/aplicación, desde que ubicación en la red, cuál fue el efecto del acceso a la base de datos, entre otros.

López, *et al* (2013) afirma que la importancia de la auditoría de bases de datos radica especialmente en la necesidad de mitigar los riesgos asociados a la pérdida de datos y a la fuga de la información, pero que también debemos considerar su importancia de acuerdo a los siguientes puntos:

- Toda información de la organización reside en bases de datos y deben existir controles relacionado con el acceso a la misma
- Se debe poder demostrar la integridad de la información almacenada en las bases de datos

- La información confidencial es responsabilidad de las organizaciones.

2.5. METODOLOGÍAS PARA LA AUDITORÍA INFORMÁTICA

Ramírez *et al* (2010) sustenta que todas las metodologías desarrolladas y utilizadas en la auditoría y el control informático, se pueden agrupar en dos grandes familias:

- ✓ **Cuantitativas**. Basadas en un modelo matemático numérico que ayuda a la realización del trabajo, están diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos

- ✓ **Cualitativas**. Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

2.5.1. MAGERIT

Las organizaciones, públicas o privadas, dependen de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

Magerit interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, Magerit les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos y por ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte todas las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del

problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista (Amutio, 2012)

Si bien ISO 27005 e ISO 31000 son los estándares más conocidos para la gestión de riesgos, existen otros instrumentos que estando alienados con estos estándares y que facilitan a una empresa enfocarse en implementar herramientas y metodologías que satisfagan los requerimientos básicos de la administración de riesgos en sus sistemas de información.

En este sentido fue desarrollado magerit una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

Puntualmente magerit se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas. (Gutiérrez, 2013)

2.5.2. COBIT

Sierra (2014) manifiesta que cobit es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores de Tecnología de Información (TI), usuarios y por supuesto, los auditores involucrados en el proceso es también un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad TI, que abarca controles específicos desde una perspectiva de negocios. Las siglas COBIT significan objetivos de control para tecnología de información y tecnologías relacionadas.

El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association). Es una herramienta de gobierno de Tecnología de Información (TI) que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

2.5.3. ITIL

Según plantea Osiatis (2013) ITIL (Información Tecnología Infrastructure Library) para la gestión de servicios, no sólo de los servicios de TI, sino también de todo tipo de servicios. Es un marco que describe las mejores prácticas para gestión de servicios de tecnología de la información y que tiene un enfoque basado en un conjunto de procesos que se agrupan en cinco fases del ciclo de vida de servicio (estrategia, diseño, transición, operación y mejora continua).

ITIL ofrece a las organizaciones un conjunto de estrategias para la continua monitorización de procesos, proporcionando una cultura organizacional que genera mayores beneficios en la calidad del servicio. Este enfoque puede ser aplicado a cualquier organización, independientemente de tamaño, sector o servicio. El resultado debe ser un confiable, seguro y servicio consistente con los costos previstos, es común en cualquier tipo de servicio, ya sea Informática, Marketing, Logística, Consultoría o cualquier otro tipo de servicio. Por consiguiente, el uso de la norma ITIL como marco de referencia se propone la gestión de cualquier tipo de servicio.

2.5.4. OCTAVE

Gómez, et al (2010) señala que OCTAVE es una metodología que tiene por objeto facilitar la evaluación de riesgos en una organización y se focaliza principalmente en los aspectos relacionados con el día a día de la empresa.

OCTAVE se centra en el estudio de riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas).

En su implementación contempla la conformación de un equipo mixto, compuesto de personas de las áreas de negocios y de TI. Esta configuración explica el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información; por su parte, el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener, estos dos puntos de vista son importantes para tener una visión global de los riesgos de seguridad de los servicios de TI.

El proceso de evaluación contemplado por OCTAVE se divide en tres fases:

1. Construcción de perfiles de amenazas basadas en activos
2. Identificación de vulnerabilidades en la infraestructura
3. Desarrollo de estrategias y planes de seguridad

El principal problema al que se está expuesto al hacer una evaluación de este tipo es que no se identifiquen oportunamente riesgos importantes, a los que eventualmente las organizaciones son vulnerables, por ello metodologías como OCTAVE minimizan este problema. Es importante que en el análisis se resalte lo valiosa que es la información, debido a que gran parte de los riesgos provienen de “costumbres” internas de las organizaciones.

2.5.4.1. TÉCNICAS

2.5.4.1.1. CHECK LIST

Es un cuestionario ordenado y estructurado por materias auditadas, ha de contener preguntas idénticas formuladas en términos aparentemente distintos. El cruzamiento de las respuestas permite aumentar el rigor del análisis. La motivación de su uso es clara, para auditar cualquier aspecto de una empresa se debe hacer un estudio serio y elaborado que es facilitado en gran medida por estos cuestionarios que nos van a dar una buena aproximación del estado o factibilidad de un proyecto o sección de la empresa por ello son una herramienta potente a utilizar en los procesos de auditoría informática.

Existen dos tipos fundamentales de CheckList:

- ✓ **De Rango**: Preguntas o conceptos a evaluar en un rango determinado. Por ejemplo de 0 a 10.
- ✓ **Binarias**: Preguntas o conceptos con respuesta única y excluyente, Si o No, 1 ó 0.

Las CheckList's de rango permiten mayor precisión si el criterio de la Auditoría es uniforme. Indicado para revisiones pequeñas. Depende excesivamente de la buena formación y competencia del equipo.

Las CheckList's binarias son excelentes si los cuestionarios están muy cuidados en su formulación. El trabajo previo es mucho más arduo y complejo para el auditor. No existen CheckList's standard para cualquier instalación. Las listas deben retocarse y adaptarse a cada organización. (Audisa, 2010)

2.5.4.1.2. COEFICIENTE DE CONCORDANCIA DE KENDALL

Según el criterio de Badia (2012) gran parte de la popularidad del coeficiente W de Kendall en todo tipo de investigaciones emana de su condición de ser una de las pocas herramientas simples para la medición del acuerdo entre expertos. Dicho acuerdo no sólo se aplica a investigaciones sobre sondeos de opinión experta sino, de manera sistemática, en la validación de instrumentos de medición en las Ciencias Sociales.

El coeficiente de concordancia de Kendall, al que la mayoría de los autores simboliza por la letra W, es una técnica de análisis estadístico muy utilizada.

Mide el grado de concordancia entre un grupo de elementos y un grupo de características. Si la concordancia es la máxima posible. W=1, el máximo valor que puede tener el coeficiente W es la unidad; por el contrario, si la concordancia es la mínima posible, es decir no hay concordancia W = 0. Por lo tanto, el coeficiente puede oscilar entre 0 y 1.

Badia (2012) afirma que la aplicación del coeficiente de kendall es la medición del grado de acuerdo entre un grupo de jueces (en el sentido más general de la palabra) aplicado a un conjunto de ítems (también en sentido general). De esta manera permite ver si hay unanimidad o un gran desacuerdo en la clasificación, obtendríamos sumas de valores similares y por tanto con una varianza pequeña.

El coeficiente de Kendall indica el grado de asociación de las evaluaciones ordinales hechas por evaluadores múltiples cuando se evalúa las mismas muestras. Los valores del coeficiente de Kendall tienen un rango de 0 a +1. Entre mayor sea el valor Kendall, más fuerte será la asociación. Generalmente, coeficientes Kendall de 0.9 o mayores son considerados muy buenos. Un coeficiente Kendall alto o significativo implica que los evaluadores están aplicando esencialmente el mismo estándar cuando evalúan las muestras.

2.6. GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

La eficiencia de la gestión académica y administrativa es de gran importancia para el correcto funcionamiento de una universidad, y en general de cualquier centro de educación. En particular los procesos que están contenidos en la gestión académica son de naturaleza dinámica pues deben adaptarse a las nuevas condiciones en que se desarrolla la labor formativa. En esta labor, esencia de todo el sistema, juegan determinado papel un conjunto de actores, los cuales están directamente implicados en la gestión automatizada con el objetivo de lograr la eficiencia planteada.

El uso intensivo de las redes de computadoras en todos los centros de educación superior en el país está sentando en las bases para lograr cambios

cualitativos significativos tanto en la gestión puramente académica como en el resto de los procesos sustantivos que se desarrollan en estos centros (Herrera, *et al* 2010).

De acuerdo a lo que manifiestan Hernández *et al* (2007), la gestión académica es una de las actividades fundamentales que se realizan, el interés que demuestran los estudiantes en el transcurso del curso escolar por sus evaluaciones es muy activo, los directivos docentes solicitan un estado de situación académica existente en los años de la especialidad para realizar un análisis comparativo respecto a los años anteriores, y las secretarias docentes están en constante actividad para generar esta información.

En todos los centros de educación se desarrolla una gestión académica para el manejo de la información referente a los estudiantes. Una vez matriculado el estudiante, este será ubicado en un año y un grupo determinado, en el cual recibirá un conjunto de asignaturas impartidas por un grupo de profesores.
La gestión académica de estudiantes, es el conjunto de procesos relacionados con:

- La matrícula.
- Ubicación en grupo docentes.
- Análisis de los resultados obtenido por cada una de las asignaturas recibidas.
- El promedio al finalizar el curso.
- El promedio final al terminar los estudios.

Todo esto con el fin de tener registrado el currículum de cada estudiante en su transcurso por la institución docente.

2.6.1. IMPORTANCIA DE LA GESTIÓN ACADÉMICA

- Permite registrar los datos personales de los estudiantes a través de expedientes
- El registro de las evaluaciones por asignaturas en su recorrido docente
- Asignar a los estudiantes a un grupo determinado
- El cálculo de promedios al finalizar cada curso

- Confección de un escalón a partir de recorrido docente de cada estudiante
- La gestión de asignaturas, profesores y grupos docentes (definiendo las asignaturas según el año escolar los profesores que impartirán cada asignatura y los grupos docentes que tendrán asignados cada uno).

CAPÍTULO III. DESARROLLO METODOLÓGICO

Este trabajo de investigación se realizó en las instituciones de educación superior públicas de Manabí, como son, Universidad Técnica de Manabí, Universidad Estatal del Sur de Manabí, Universidad Laica Eloy Alfaro de Manabí y Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López en las ciudades de Portoviejo, Jipijapa, Manta y Calceta respectivamente, tuvo una duración de nueve meses. Para el inicio de la auditoría de las bases de datos de gestión académica, fue necesario solicitar la autorización de inicio (Anexo 1) a las autoridades de las universidades involucradas, la misma que describía aspectos como los objetivos de auditoría, el alcance, personal involucrado y el tiempo estimado, obteniendo así el respectivo permiso.

Además, fue necesario investigar e indagar sobre las diferentes metodologías de gestión de riesgos informáticos existes, para poder seleccionar la que mejor se acople a las necesidades presentadas, luego de un exhaustivo trabajo se determinó utilizar la metodología OCTAVE (**sección 2.5.4**) que consiste en el análisis de los posibles riesgos y tratamiento de los mismos, que continuamente se presentan en los sistemas de información y sus bases de datos. Esta metodología utiliza un enfoque de tres fases (**Figura 3.1**) para examinar la organización y su tecnología, reuniendo una visión global de las necesidades de seguridad de información.

3.1. OCTAVE

Con esta metodología se conocerá cada uno de los procesos involucrados en una auditoría, asimismo la existencia de riesgos, amenazas y la necesidad de prevenirlos, para luego proceder a la planificación de medidas correctivas que ayuden a mitigar dichas eventualidades; con la ayuda de técnicas como el checklist, entrevistas, encuestas, entre otras, se logrará la obtención de resultados que permitirán tener una visión clara de las anomalías existentes. Octave a su vez se convertirá en una herramienta fundamental para el desarrollo de esta investigación, permitiendo entre otras cosas, incorporar la norma INEN-ISO / IEC 27000 referente a, tecnologías de la información -

técnicas de seguridad y sistemas de gestión de seguridad de la información, la misma que servirá como guía para la evaluación de las bases de datos en diferentes aspectos.

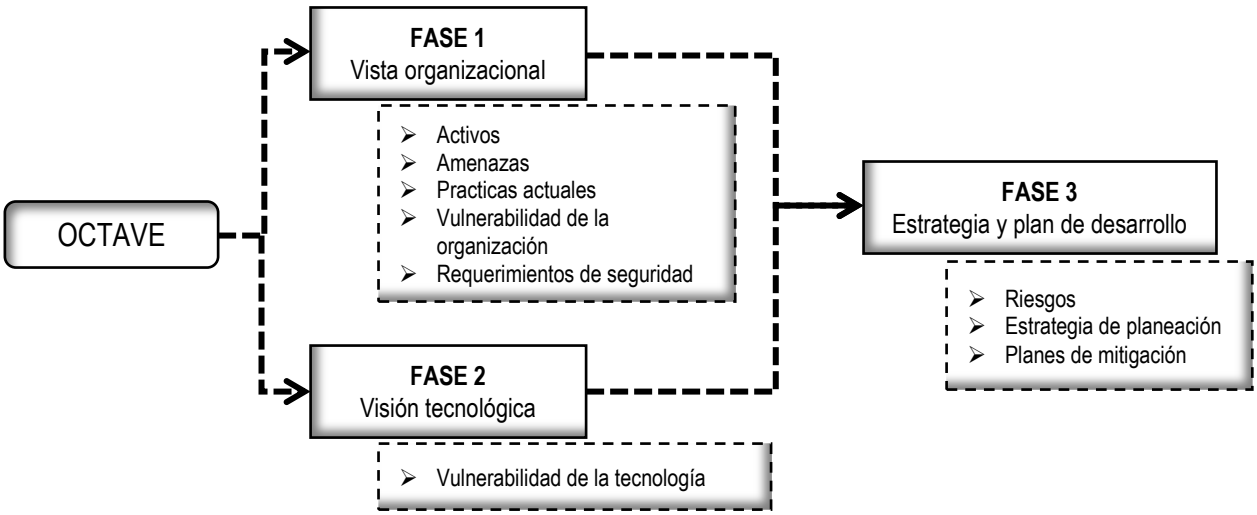


Figura 3.1. Procesos de la metodología OCTAVE

Elaboración: Los autores

3.1.1. FASE 1- VISTA ORGANIZACIONAL

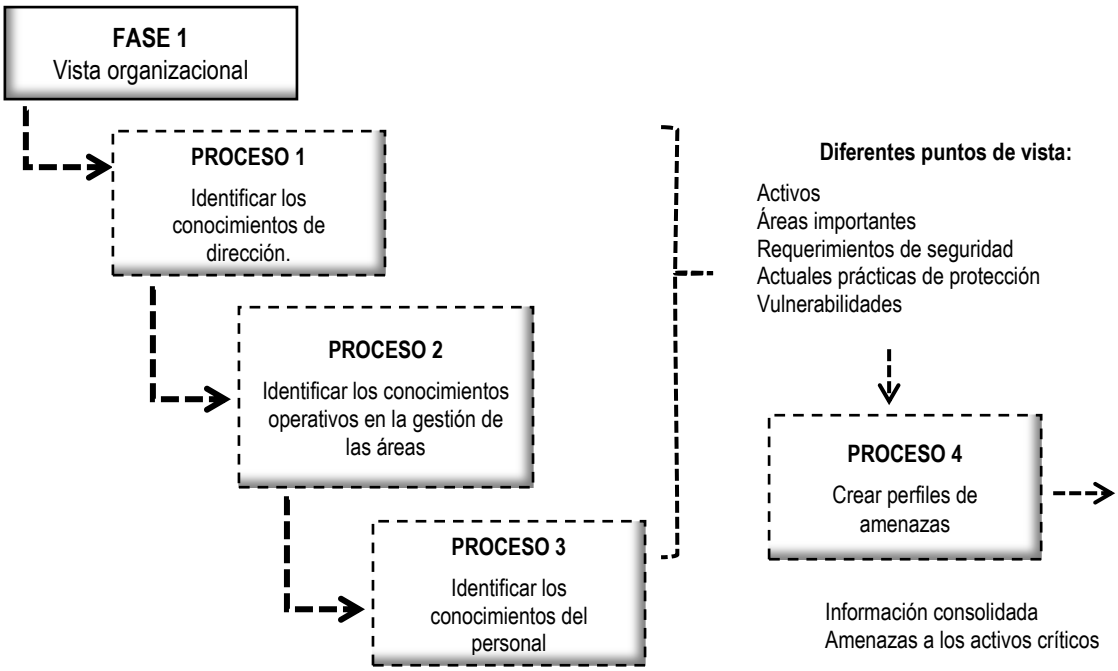


Figura 3. 2. Fase-1 Vista organizacional

Elaboración: Los autores

Como se aprecia en la Figura 3.2**,** esta fase consta de cuatro procesos que permiten obtener un vista organizacional completa; en este caso los autores luego de analizar cada etapa decidieron hacer uso del primer proceso, el mismo que consiste en identificar los conocimientos de dirección, para ello fue necesario primero analizar las instituciones que serían auditadas (**Figura 3.3**), luego de esta determinación, se continuó con la tramitación de los permisos respectivos (**anexo 1**), los mismos que dieron apertura de manera formal para la ejecución de este trabajo. Seguido a esto se realizaron las respectivas visitas y sociabilización de la auditoria, dando a conocer a los superiores el trabajo a realizar, esto dio pie para que por medio de una entrevista con los encargados de los departamentos de tecnología de la información y comunicación (TIC´s) identificar los conocimientos de dirección que ellos poseen.

	INSTITUCIONES DE EDUCACIÓN SUPERIOR (IES) PÚBLICAS DE MANABÍ
1	Universidad Técnica de Manabí
2	Universidad Estatal del Sur de Manabí
3	Universidad Laica Eloy Alfaro de Manabí
4	Escuela Superior Politécnica Agropecuaria de Manabí

Figura 3.3. IES implicadas en la auditoría
Fuente: SENESCYT

3.1.2. FASE 2- VISIÓN TECNOLÓGICA

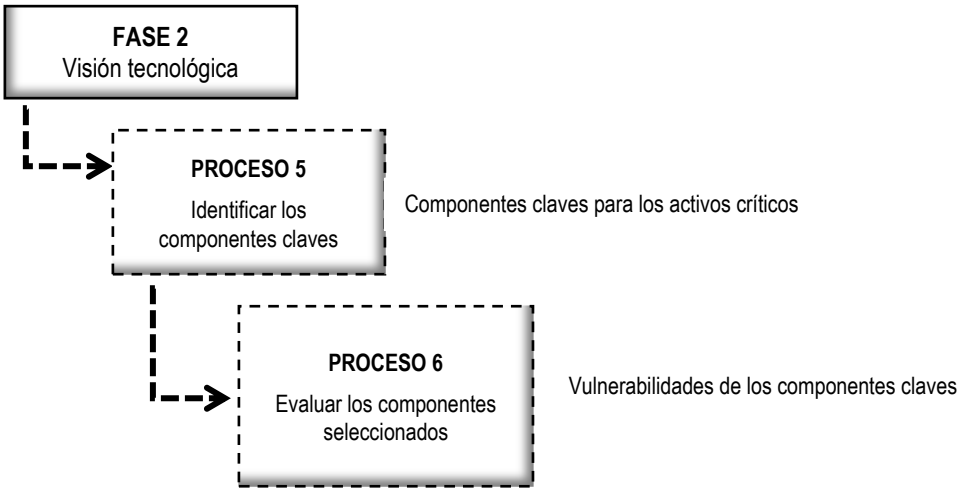


Figura 3.4. Fase-2 Visión tecnológica
Elaboración: Los autores

En esta etapa se procedió con la indagación de normas vigentes para la posterior identificación de los componentes claves a evaluar, encontrando a la Norma INEN – ISO / IEC 27000 como internacional y al acuerdo ministerial #166 como nacional, el mismo que está suscrito en el registro oficial #88 referente al esquema gubernamental de seguridad de la información (EGSI), conocido esto y teniendo en cuenta los parámetros a evaluar, se procedió a la realización del banco de preguntas y posterior aplicación de los cuestionarios (**Anexo 2 y Anexo 4**).

- **CUESTIONARIOS**

Siguiendo con lo propuesto, y luego de la realización de los cuestionarios, se continuó con la aplicación y evaluación de los componentes claves para conocer las vulnerabilidades y anomalías existentes, dichos cuestionarios recayeron sobre el responsable del departamento de TIC´S, los mismos que estaban divididos en dos partes, el primero conformado por 62 preguntas, separados en 7 apartados que permitieron evaluar aspectos como, los datos, formación del administrador, calidad, aspectos lógicos, seguridad, protección y demás áreas fundamentales, el tipo de respuestas variaba según el contexto de la pregunta, utilizando en este caso la escala de Likert para ello, el segundo banco de preguntas pretendía evaluar el cumplimiento del EGSI, conformado de 61 preguntas divididas en 8 apartados, en este caso los tipos de respuestas eran únicamente de SI y No, además de ello los encuestados deberían de dar una puntuación (0-10), donde, 0 indica que dicho proceso no se cumple, 5 que tiene un cumplimiento del 50% y 10 que se efectúa en su totalidad.

3.1.3. FASE 3- ESTRATEGIA Y PLAN DE DESARROLLO

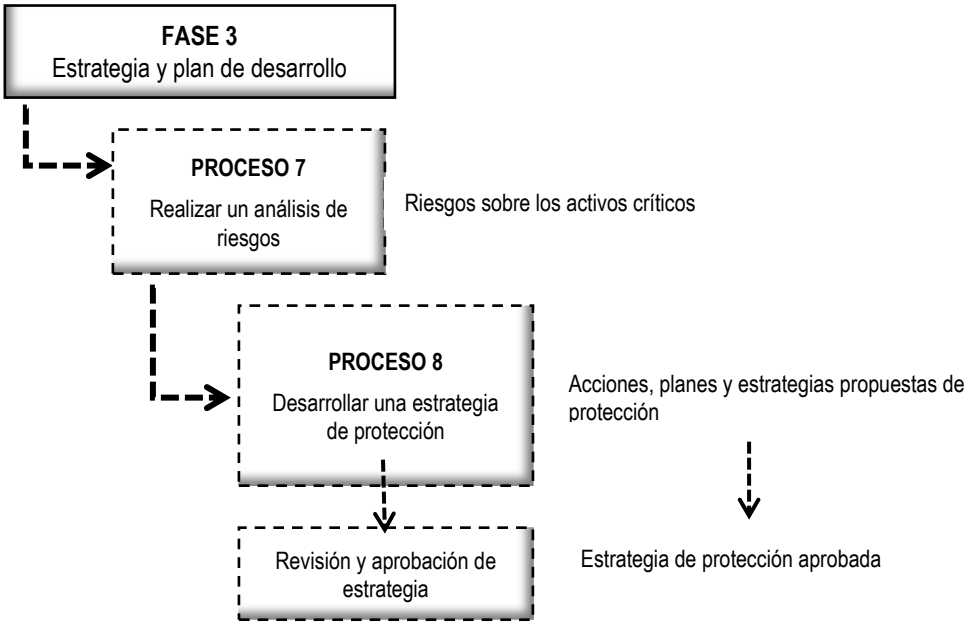


Figura 3.5 Fase-3 Estrategia y plan de desarrollo
Elaboración: Los autores

Luego de haber evaluados los componentes seleccionados como claves por medio de los cuestionarios aplicados se procedió a la realización de la matriz de determinación de riesgo-confianza (**sección 2.3.4**), la misma permitió obtener el grado de confianza y el nivel de riesgo de cada cuestionario aplicado, esto con la ayuda de la fórmula que se muestra a continuación.

$$CP = \frac{CT*100}{PT} \quad \textbf{(3.1)}$$

Dónde:

CP: Calificación porcentual

PT: Ponderación total

CT: Calificación total

Inmediatamente de obtenida la calificación porcentual (CP), se procedió a clasificarlos de la siguiente manera, si su CP se encontraba entre el 15% y 50% se enmarcaba en un nivel de confianza bajo y un riesgo alto, resaltándose de color rojo, si su CP se situaba entre el 51% y 75% indicaba una confianza y riesgo moderado con un color amarillo, por último si dicho porcentaje oscilaba el 76% y 95% mostraba una confianza alta y un riesgo bajo con un color verde, estos datos se reflejan en el capítulo de resultados (**sección 4.1.2.2.**); para la

comprobación del grado de concordancia entre las respuestas obtenidas, se continuó con la agrupación de las preguntas similares existentes y la posterior determinación de la relación gradual de su concordancia, determinando con ello el coeficiente de concordancia de Kendall (**Cuadro 4.6** y **Cuadro 4.7**).

Posteriormente se elaboró un cuadro donde se presentaran las falencias halladas en las instituciones visitadas (**Cuadro 4.8**), aquí se dio a conocer las disposiciones planteadas por la ley y el cumplimiento que las IES públicas le dan, seguidamente y como lo dicta la metodología se realizaron acciones de mejora que aporten a las instituciones a mitigar las eventualidades existentes, esto se realizó por medio de hojas de hallazgos donde se describen aspectos como, el criterio según lo dictaminado por la ley, la condición en que se encuentra la institución, causa y efecto que conlleva su incumplimiento así como también conclusiones y recomendaciones.

En ésta última fase se procedió con la elaboración del informe de auditoría, el cual incluye los resultados obtenido, en el cual realizan sugerencias a las instituciones, esperando que éstas sean aprobadas y aplicadas, lo que les servirá para tener un mejor control sobre sus bases de datos, dando cumplimiento a lo establecido por las normas nacionales e internacionales.

3.2. TÉCNICAS

3.2.1. ENTREVISTA

Con la ayuda de ésta técnica, se procedió a la visita de las instituciones involucradas, realizando entrevistas a la máxima autoridad de los establecimientos seleccionados, la mima que a su vez procedió con la aprobación para un posterior conversatorio con el personal encargado del departamento de tecnología, ello permitió la sociabilización del trabajo, exponiendo entre otras cosas el motivo de la visita y la finalidad de la misma.

3.2.2. ENCUESTA

Permitió la ejecución de las preguntas que se aplicaron al personal competente, las mismas que fueron de vital importancia para la obtención de

los resultados, ya que gracias a ella se logró conocer el estado de las bases de datos en cuanto al cumplimiento de las normas y estándares vigentes.

3.2.3. OBSERVACIÓN

La técnica de la observación se utilizó para examinar las normas y estándares internacionales vigentes y comprobar con ello si las instituciones dan cumplimiento a ellos y en qué porcentaje lo hacen.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Aquí se describen los resultados obtenidos de cada una de las fases y procesos que constituyen la metodología aplicada

4.1.1. APLICACIÓN FASE 1- VISTA ORGANIZACIONAL

Como resultado del primer objetivo planteado y luego de haber obtenido los permisos y la autorización necesaria (**Anexo 1**), se continuó con las entrevistas al personal pertinente, los encargados del departamento de tecnología y el administrador de las bases de datos, logrando obtener aparte de sus datos personales, una idea de los conocimientos que poseen sobre el puesto que representan, es decir, si conoce la importancia de los activos a su disposición, los requisitos de seguridad, prácticas de protección y vulnerabilidades a las que están expuestas las bases de datos, determinando que sus niveles sobre los conocimientos de dirección son favorables.

4.1.2. APLICACIÓN FASE 2- VISIÓN TECNOLÓGICA

Luego de determinar las normas en base a las cuales se iban a evaluar las bases de datos, se elaboraron y aplicaron los cuestionarios (**Anexo 3 y 5**) con los cuales se recolectó la información necesaria para poder determinar el cumplimiento de la norma, los mismos que dieron los resultados descritos a continuación.

4.1.2.1. COMPARATIVA DE LOS RESULTADOS OBTENIDOS DE LOS CUESTIONARIOS DE EVALUACIÓN GENERAL DE LAS BASES DE DATOS APLICADOS LAS IES PÚBLICAS DE MANABÍ

Este cuestionario consta de dos partes (**Anexo 2**), la primera, elaborado con preguntas tipo Likert y la segunda con preguntas de SI y No; en el gráfico 4.1, se puede notar que quien posee un mayor control sobre sus bases de datos en los aspectos aquí evaluados es la IES 4 con un porcentaje de 88%, así como también que la IES 2 alcanzó tan solo un 15% de puntuación, esto podría sustentarse en que dicha institución cuenta con un departamento de TIC´s

relativamente nuevo con apenas meses de creación, lo que indica que recién se están acoplando a lo dictaminado por la ley, por otro lado tanto la IES 1 como la IES 3 alcanzaron porcentajes que van desde los 56% y 60% respectivamente, cabe recalcar que dicho cuestionario constaba de 40 preguntas, la segunda parte este mismo cuestionario se conformaba por 22, en las cuales se obtuvo de manera general un total de 46 preguntas afirmativas y 20 negativas.

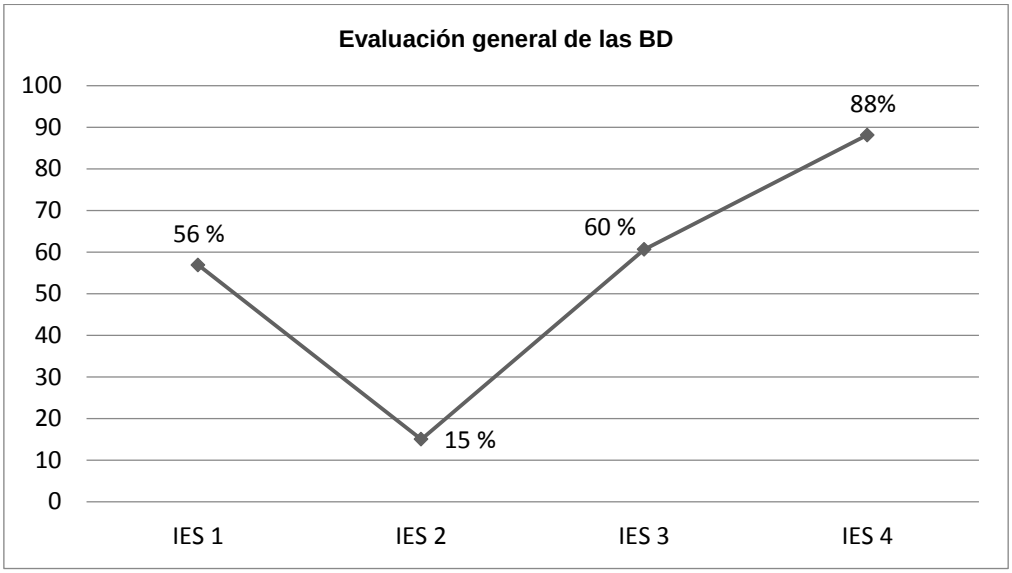


Gráfico 4. 1. Comparativa general del cuestionario de evaluación de las BD
Fuente: IES públicas de Manabí

A continuación, se presentan los resultados de cada apartado correspondiente al cuestionario de evaluación general de las bases de datos (**Anexo 2**), detallando el porcentaje alcanzado por cada una de las instituciones consideradas.

- **DATOS**

Éste apartado consta de tres preguntas, las cuales dan a conocer si la base de datos está correctamente documentada, si su redundancia está controlada y si la misma posee un valor informativo; como se muestra en la **Gráfico 4.2** y en base a las respuestas recibidas, se obtuvo como resultado que tres de las cuatro instituciones no tienen documentada sus bases de datos de manera correcta, pero que su redundancia se encuentra controlada en su mayoría, de

igual manera tienen un valor informativo bastante alto; de manera general se obtiene una ponderación total de 54,17%, representando un nivel medio en cuanto a lo evaluado.

	DATOS			
	P1	**P2**	**P3**	**T**
IES 1	*50*	*25*	*75*	**50 %**
IES 2	*25*	*0*	*50*	**25 %**
IES 3	*75*	*50*	*75*	**66,67 %**
IES 4	*75*	*75*	*75*	**75 %**
	56,25	37,5	68,75	**54,17**

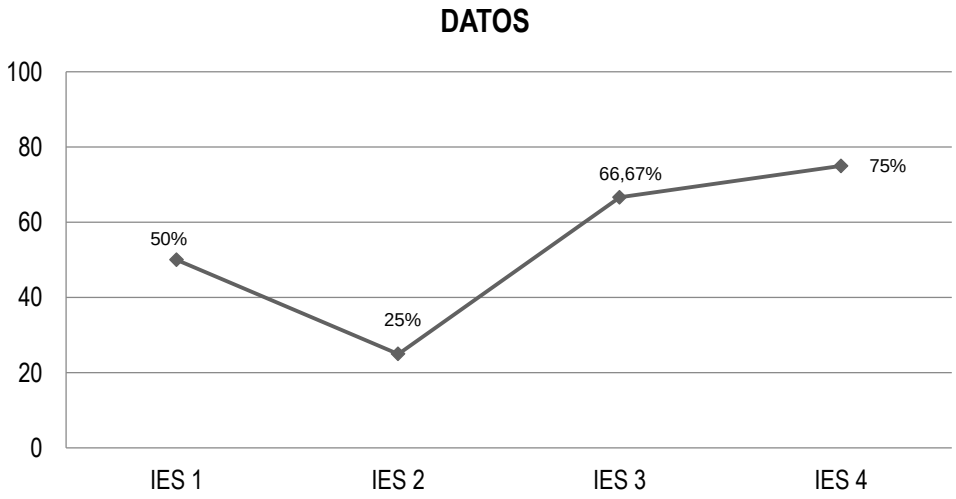


Gráfico 4.0.2. Comparativa de resultados con respecto a los datos
Fuentes: IES públicas de Manabí

- **ADMINISTRADOR DE LAS BASES DE DATOS**

Comprendido por 8 preguntas, pretende evaluar si la persona responsable del manejo y manipulación de las bases de datos cuenta con la experiencia requerida, formación y capacitación adecuada y si incluye entre otras cosas procedimientos de seguridad para adecuada gestión, como se aprecia en el **Gráfico 4.3** los porcentajes alcanzados por las instituciones, corresponden de la siguiente manera, IES 1 con un 78,13%; IES 2 un 15,63%, IES 3 un 59,38% y un 90,63% la IES 4, demostrando con ello que tres de estas cuentan con un personal altamente capacitado y formado para la manipulación de las bases de datos y que gestionan la seguridad de manera apropiada.

ADMINISTRADOR BASE DE DATOS

	P4	P5	P6	P7	P8	P9	P10	P11	T
IES 1	*100*	*100*	*100*	*100*	*100*	*75*	*50*	*0*	*78,13 %*
IES 2	*25*	*25*	*0*	*25*	*25*	*25*	*0*	*0*	*15,63 %*
IES 3	*50*	*75*	*50*	*50*	*75*	*75*	*50*	*50*	*59,38 %*
IES 4	*100*	*100*	*100*	*100*	*75*	*75*	*100*	*75*	*90,63 %*
	68,75	75	62,5	68,75	68,75	62,5	50	31,25	**60,94 %**

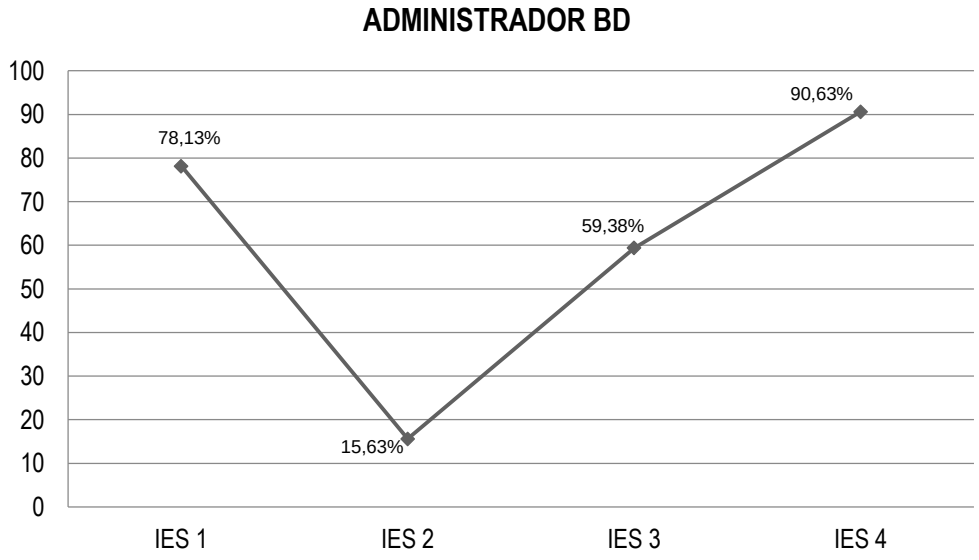


Gráfico 4.0.3. Comparativa de resultados con respecto al administrador de BD
Fuente: IES públicas de Manabí

- **CALIDAD**

Con 4 preguntas, evalúa políticas de calidad, seguridad, cumplimiento de la ley de acceso a datos y frecuencia con que se realizan auditorias, comprobando que en dos de las cuatro instituciones nunca se han realizado auditorías informáticas, por otro lado, las dos instituciones restantes a pesar de que si han sido auditadas, pero en un lapso de tiempo mayor a los 24 meses, de igual manera se muestra que existen con pocas políticas de seguridad, y a pesar de la escases de las mismas, no dan cumplimiento de éstas en su totalidad, todo ello se muestra en la **Gráfico 4.4,** donde además se aprecia una ponderación total de 53,13% en aspectos de la calidad.

CALIDAD					
	P12	P13	P14	P15	T
IES 1	*25*	*75*	*75*	*100*	**68,75 %**
IES 2	*25*	*0*	*75*	*75*	**43,75 %**
IES 3	*50*	*50*	*50*	*0*	**37,5 %**
IES 4	*75*	*100*	*75*	*0*	**62,5 %**
	43,75	56,25	68,75	43,75	***53,13 %***

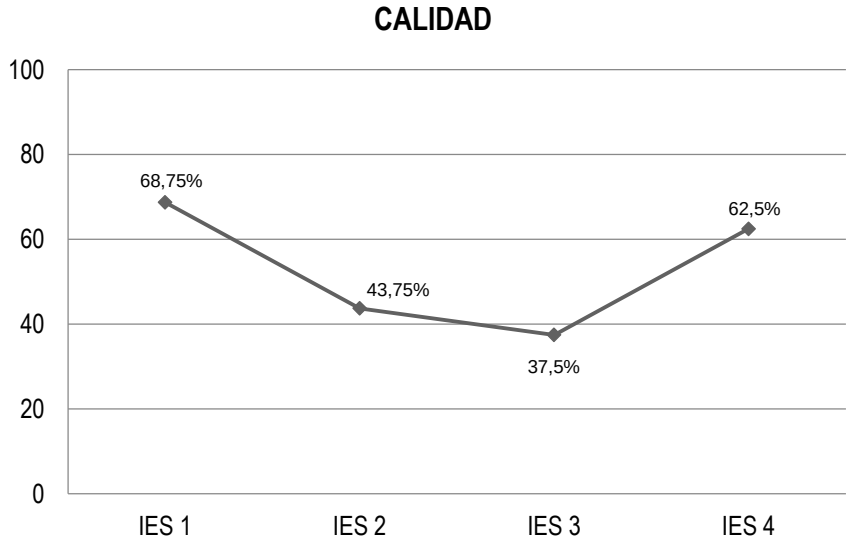


Gráfico 4.0.4. Comparativa de resultados con respecto a la calidad
Fuente: IES públicas de Manabí

- **ASPECTOS LÓGICOS**

Evaluando cinco diferentes ítems sobre, validación de datos antes de su inserción, si estos están disponibles para cualquier usuario o solo personal autorizados entre otros, si la conexión a las bases de datos se realiza de forma segura, obteniendo como resultado que las cuatro instituciones mantienen sus datos privados disponibles para usuarios autorizados, también se comprobó que dos de ellas validan el 100% de los datos ingresados y las otras solo validan un 50% de estos, de igual manera se aprecia que una de las IES no cuenta con conexión segura a sus bases de datos, como dato final se obtuvo una ponderación total de 60,94% como lo refleja la **Gráfico 4.5.**

ASPECTOS LÓGICOS						
	P16	P17	P18	P19	P20	T
IES 1	*0*	*75*	*100*	*100*	*25*	***68,75 %***
IES 2	*0*	*25*	*50*	*0*	*0*	***18,75 %***
IES 3	*50*	*75*	*50*	*75*	*50*	***62,5 %***
IES 4	*75*	*100*	*100*	*100*	*100*	***93,75 %***
	31,25	68,75	75	68,75	43,75	***60,94 %***

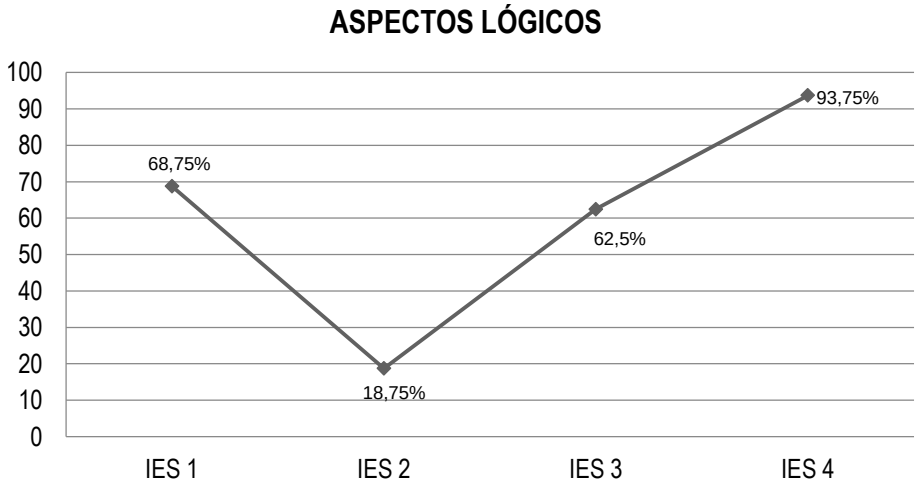


Gráfico 4.0.5. Comparativa de resultados con respecto a los aspectos lógicos
Fuente: IES públicas de Manabí

- **SEGURIDAD Y PROTECCIÓN DE LOS DATOS**

Conformada por 14 preguntas, evalúa la protección de los datos, si estos son usados con fines educativos y si existen programas contra software malicioso, entre otros, en el **Gráfico 4.6** se presenta la evidencia obtenida, tres instituciones alcanzan un porcentaje superior al 75%, lo que garantiza la seguridad de todos sus datos, de igual manera, estos datos tienen un uso estrictamente educativo, los porcentajes obtenidos fueron de 75% y 100% en tres de ellas, además en solo dos instituciones los usuarios no pueden ver, modificar o eliminar los datos que la institución posee sobre ellos con porcentajes de 25% y 75% correspondiente a la IES 3 y 4 respectivamente, se logró apreciar también un bajo cumplimiento de parte de los empleados y usuarios sobre las políticas de seguridad en tres de las instituciones auditadas alcanzando un 25%, 50% y 75% esto a pesar de que existe un responsable de hacer cumplir las mismas.

SEGURIDAD Y PROTECCIÓN DE DATOS															
	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	T
IES1	0	100	100	100	75	0	50	50	75	50	50	50	50	25	**55,36 %**
IES2	0	25	0	0	0	0	25	0	0	25	25	25	0	0	**8,93 %**
IES3	75	75	75	75	100	25	75	75	50	0	25	25	25	0	**50 %**
IES4	100	100	100	100	75	75	100	100	75	75	75	100	100	100	**91,07 %**
	43,75	75	68,75	68,75	62,5	25	62,5	56,25	50	37,5	43,75	50	43,75	31,25	**51,34 %**

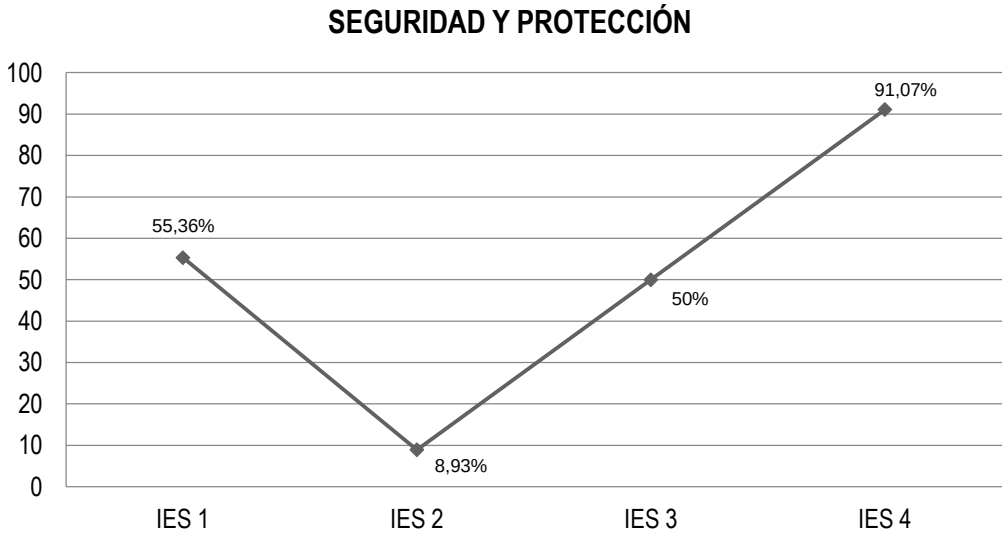


Gráfico 4.0.6. Comparativa de resultados seguridad y protección de datos
Fuente: IES públicas de Manabí

- **PROTECCIÓN CONTRA SOFTWARE MALICIOSO**

Representa al último apartado evaluado en éste primer cuestionario, conformado por 6 preguntas que pretende conocer si existe algún control para la instalación de programas y de la existencia de algún antivirus instalado en sus servidores, entre otros; alcanzando una ponderación total de 56,25% como se muestra en el **Gráfico 4.7**, comprobando también que dos IES poseen medidas para evitar la instalación de software malicioso que pueda afectar su funcionalidad, las dos restante no cumplen con estas medidas, para un mejor control, tres IES cuentan con un antivirus para la protección, el mismo que es actualizado de manera periódica, con la ayuda de este software se realiza además un escaneo de los correos que ingresan a sus servidores, alcanzando un nivel de cumplimiento del 25% en una y 100% en dos de ellas

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

	P35	P36	P37	P38	P39	P40	T
IES 1	*0*	*25*	*50*	*0*	*50*	*25*	***25 %***
IES 2	*0*	*0*	*0*	*0*	*25*	*0*	***4,17 %***
IES 3	*100*	*100*	*100*	*100*	*100*	*100*	***100 %***
IES 4	*75*	*100*	*100*	*100*	*100*	*100*	***95,83 %***
	43,75	56,25	62,5	50	68,75	56,25	***56,25 %***

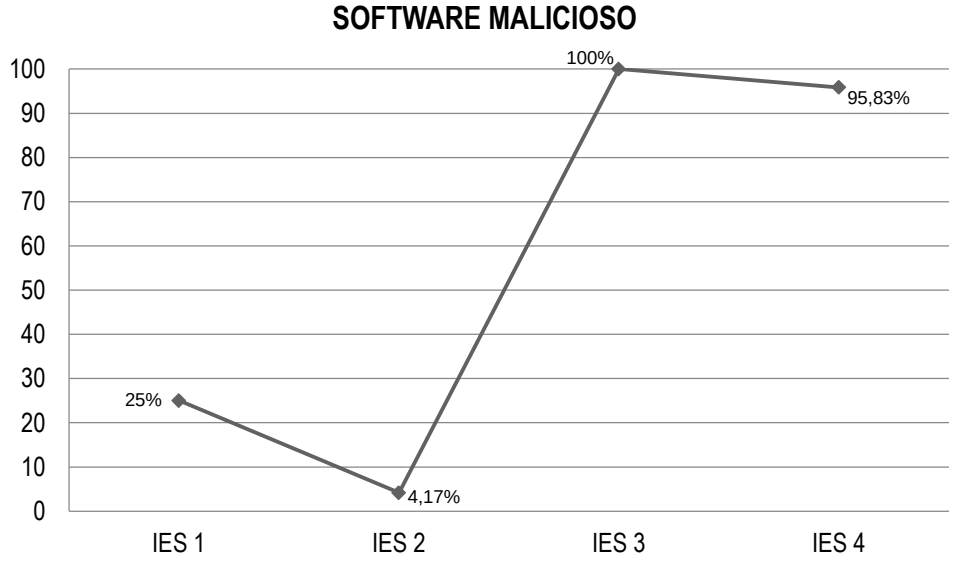


Gráfico 4.0.7. Comparativa de resultados protección contra software malicioso
Fuente: IES públicas de Manabí

Luego de haber procesado dicho cuestionario, se pudo conocer los porcentajes de cumplimiento de cada uno de los aspectos evaluados, apreciando que el apartado que presenta un menor cumplimiento corresponde a uno de los más importantes, como es el de seguridad y protección de los datos con un porcentaje de 51,34%, por otro lado se nota también que tanto los apartados relacionados con el administrador de las bases de datos y el de los aspectos lógicos representan el mayor cumplimiento, alcanzando un nivel superior al 60%, como dato adicional, se resalta que de todos los aspectos evaluados ninguno es inferior del 50%, todo lo descrito anteriormente se lo muestra en el **Gráfico 4.8.**

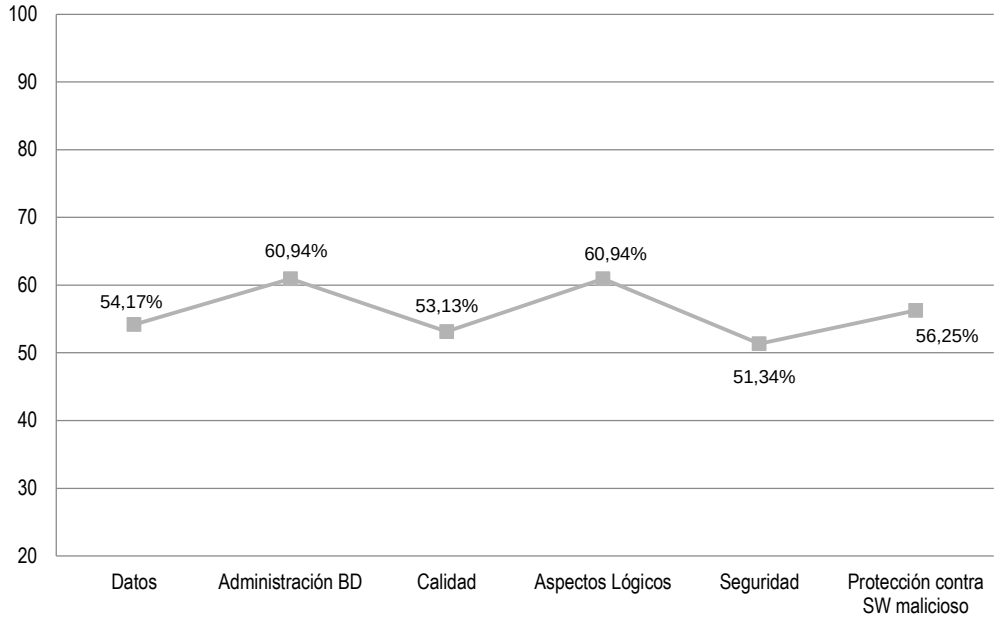


Gráfico 4.0.8. Comparativa de resultados por categoría
Fuente: IES públicas de Manabí

4.1.2.2. COMPARATIVA DE LOS RESULTADOS OBTENIDOS DE LOS CUESTIONARIOS DE EVALUACIÓN DEL CUMPLIMIENTO DE LA NORMA INEN-ISO/IEC 27000 APLICADO A LAS IES PÚBLICAS DE MANABÍ

La aplicación de este cuestionario (**Anexo 3**) sirvió para conocer el cumplimiento que las instituciones dan a la norma técnica Ecuatoriana INEN-ISO/IEC 27000, en él se evaluaron 8 aspectos diferentes, con un total de 61 preguntas, en el **Gráfico 4.9** se muestran los resultados obtenidos, los mismos que revelan un bajo cumplimiento por parte de la IES 2, se aprecia también, que de las 4 instituciones involucradas, ninguna presenta un nivel mayor al 50% en el cumplimiento de la norma, la que mejor desenseño logra alcanza un 46%.

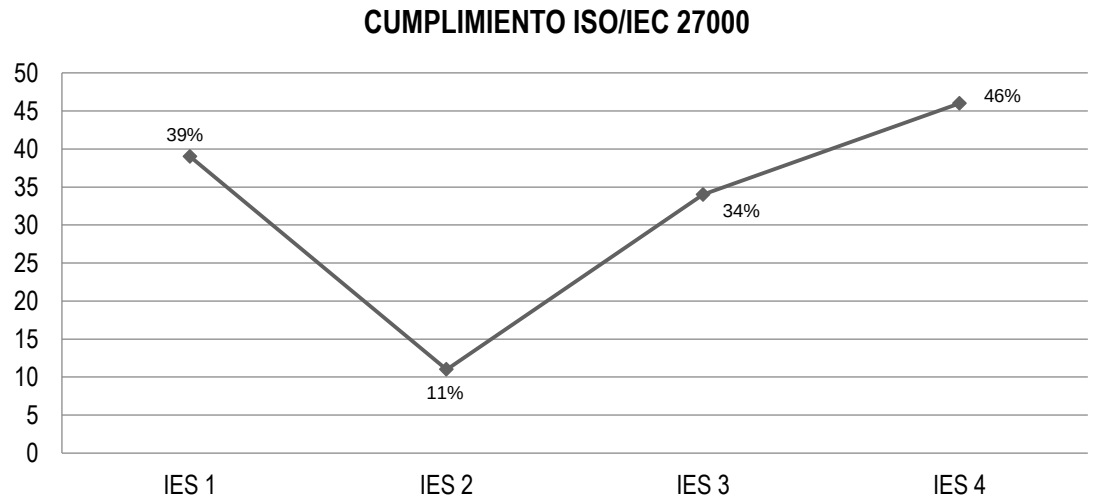


Gráfico 4.9. Comparativa de resultados del cumplimiento de la norma INEN-ISO/IEC 27000
Fuente: IES públicas de Manabí

4.1.3. APLICACIÓN FASE 3- ESTRATEGIA Y PLAN DE DESARROLLO

Seguidamente se procedió con la realización del análisis de los riesgos, con ayuda de la matriz de determinación de riesgo – confianza, en la cual se conocieron los niveles con los que cuenta cada institución, como se muestra en los siguientes cuadros con un mayor detalle (**Cuadro 4.1, 4.2, 4.3, 4.4**).

- **ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DEL R.O. No 88SI IES1**

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{352 * 100}{610}$$

$$\boldsymbol{CP} = \mathbf{57,70\%}$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESG
15 – 50	BAJO	ALTO
51 – 75	MODERDO	MODERDO
76 - 95	ALTO	BAJO

57,70%

Nivel de confianza:	**MODERADO**	57,70%
Nivel de riesgo:	**MODERADO**	42,3□%

El cuestionario de cumplimiento del R.O No 88 aplicado al departamento de las TIC´S de la IES 1, formado por 61 preguntas, arrojó una ponderación total de 610 puntos y una calificación total de 352 puntos, lo que corresponde una calificación porcentual del 57,70%, obteniendo un nivel de confianza y de riesgo moderado.

Cuadro 4.1. Matriz de Riesgo – IES 1
Elaborado por: Los autores

- **ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DEL R.O. No 88SI IES 2**

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{98 * 100}{610}$$

$$\boldsymbol{CP} = \mathbf{16,07\%}$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	MODERADO	MODERADO
76 - 95	ALTO	BAJO

16.07%

Nivel de confianza:	**BAJO**	16,07%
Nivel de riesgo:	**ALTO**	83,93%

El cuestionario de cumplimiento del R.O No 88 aplicado al departamento de las TIC´S de la IES 2, formado por 61 preguntas, arrojó una ponderación total de 610 puntos y una calificación total de 98 puntos, lo que corresponde una calificación porcentual del 16,07%, obteniendo un nivel de confianza bajo y de riesgo alto.

Cuadro 4.2. Matriz de Riesgo – IES 2
Elaborado por: Los autores

- **ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DEL R.O. No 88SI IES 3**

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{319 * 100}{610}$$

$$\boldsymbol{CP} = \mathbf{52,30\%}$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	MODERADO	MODERADO
76 - 95	ALTO	BAJO

52,30%

Nivel de confianza:	**MODERADO**	52,30%
Nivel de riesgo:	**MODERADO**	47,70%

El cuestionario de cumplimiento del R.O No 88 aplicado al departamento de las TIC´S de la IES 3, formado por 61 preguntas, arrojó una ponderación total de 610 puntos y una calificación total de 319 puntos, lo que corresponde una calificación porcentual del 52,30%, obteniendo un nivel de confianza y de riesgo moderado.

Cuadro 4.3. Matriz de Riesgo – IES 3
Elaborado por: Los autores

- **ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DEL R.O. No 88SI IES 4**

MATRIZ DE RIESGO - CONFIANZA

Determinación del riesgo confianza:

CP: Calificación Porcentual
PT: Ponderación Total
CT: Calificación Total

$$\boldsymbol{CP} = \frac{CT * 100}{PT}$$

$$\boldsymbol{CP} = \frac{469 * 100}{610}$$

$$\boldsymbol{CP = 76,89\%}$$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
15 – 50	BAJO	ALTO
51 – 75	MODERADO	MODERADO
76 - 95	ALTO	BAJO

76,89%

Nivel de confianza:	**ALTO**	76,89%
Nivel de riesgo:	**BAJO**	23,11%

El cuestionario de cumplimiento del R.O No 88 aplicado al departamento de las TIC´S de la IES 4, formado por 61 preguntas, arrojó una ponderación total de 610 puntos y una calificación total de 469 puntos, lo que corresponde una calificación porcentual del 76,89%, obteniendo un nivel de confianza alto y de riesgo bajo.

Cuadro 4.4. Matriz de Riesgo – IES 4
Elaborado por: Los autores

Con lo anterior se logró determinar el nivel de riesgo - confianza de cada institución, con lo que se determinó que la IES 1 cuenta un nivel de riesgo y confianza moderado 42,30% y 57,70% respectivamente, en el caso de la IES 2 su riesgo es alto con un 83,93% y su confianza es baja con un 16, 07% lo que indica que es la institución con el nivel más alto riesgo, esto se debe a que su departamento de tecnología cuenta con pocos meses de creación y la poca importancia que le dan a la norma, por otro lado la IES 3 se encuentra en un nivel moderado de confianza 52,30% y riesgo 47,70%, con respecto a la institución 4 es la mejor puntuada, con el nivel más alto de confianza correspondiente al 76,89% es la entidad que mayor acatamiento realiza sobre la ley, cuenta además con un nivel de riesgo de 23,11% lo que corresponde a un nivel bajo; todo lo anterior se muestra en el Cuadro 4.5.

MATRIZ DE RIESGO-CONFIANZA							
IES 1		**IES 2**		**IES 3**		**IES 4**	
RIESGO	**CONFIANZA**	**RIESGO**	**CONFIANZA**	**RIESGO**	**CONFIANZA**	**RIESGO**	**CONFIANZA**
42,30%	*57,70%*	*83,93%*	*16,07%*	*47,70%*	*52,30%*	*23,11%*	*76,89%*

Cuadro 4.5. Matriz general porcentual de nivel Riesgo – Confianza
Fuente: Cuestionario de cumplimiento de la norma INEN-ISO/IEC 27000

Luego de determinar los niveles de riesgos y confianza, se continuó con la realización de la comprobación de los niveles de concordancia de las respuestas obtenidas utilizando el coeficiente de Kendall, realizando el despeje de la fórmula y su posterior determinación como seguidamente se presenta.

Item K	Preguntas	IES 1	IES 2	IES 3	IES 4	∑aij	A	A^2
1	Existen acuerdos de confidencialidad	1	0	2	4	7	-2	4
2	Se realizan con frecuencia copias de seguridad	4	1	2	4	11	2	4
3	Existen políticas de seguridad	2	1	2	4	8	-1	1
4	Se obliga al cambio de contraseñas frecuentemente	3	2	3	2	10	1	1
						36		**10**

Cuadro 4.6. Concordancia de preguntas similares de los cuestionarios aplicados
Fuente: Cuestionario de cumplimiento de la norma INEN-ISO/IEC 27000

Fórmula del Coeficiente de Concordancia de Kendall

$$w = \frac{12\sum A^2}{n^2\, n(k^2 - 1)}$$

HALLAR EL VALOR DE A	HALLAR EL VALOR DE T
$\boldsymbol{A = \sum aij - T}$ $\boldsymbol{A = 7 - 9}$ $\boldsymbol{A = -2}$ **El mismo proceso se aplica para el resto de preguntas**	$T = \frac{\sum aij}{K}$ $T = \frac{36}{4}$ $T = 9$
REEMPLAZO DE LA FÓRMULA	
$\boldsymbol{w = \frac{12\sum A^2}{n^2\, 4(k^2 - 1)}}$ $\boldsymbol{w = \frac{12(10)}{4^2\, 4(4^2 - 1)}}$ $\boldsymbol{w = 0,13}$	

Cuadro 4.7. Reemplazo de fórmulas para el Coeficiente de Concordancia de Kendall
Fuente: Cuestionario de cumplimiento la norma INEN-ISO/IEC 27000

Una vez obtenido el resultado de la aplicación del Coeficiente de concordancia de Kendall, los autores llegan a la conclusión de que las respuestas tienen un grado de concordancia de 0,13; lo que indica que las 4 IES implicadas no llevan los mismos procesos porque existe una variación en su aplicabilidad, unas bajas y otras altas, de tal manera concuerdan en cuanto al incumplimiento a las normas y estándares de seguridad vigentes.

4.1.3.1. FALENCIAS ENCONTRADAS DURANTE EL ANÁLISIS DE LOS DATOS OBTENIDOS EN LAS IES PÚBLICAS DE MANABÍ

A continuación los autores muestran los aspectos en los que se encontraron mayor incumplimiento de la ley.

DISPOSICIÓN	CUMPLIMIENTO
La Norma de Control Interno en sus diferentes apartados establece que:	
410-07 manifiesta sobre la adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales.	La mayoría de las instituciones no hacen uso de ninguna norma y/o estándares, en algunos casos solo de políticas internas, no especificadas.
410-09 menciona que se establecerán ambientes de desarrollo/pruebas y de producción independientes	La mitad de las instituciones no cumplen con lo establecidos, solo cuentan con ambientes de desarrollo y producción.
410-10 señala la implementación y administración de seguridades a nivel de software y hardware	No se cuenta con niveles adecuados de protección.
410-12 hace referencia a la estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.	No se cuenta con la total administración de las cuentas de usuario
410-12 remarca revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.	No se realiza con regularidad, a tal punto que si algún empleado abandona la institución podría seguir accediendo con su usuario con facilidad
El registro oficial 88 establece que:	
La elaboración y aprobación de acuerdos de confidencialidad y no-divulgación de la información.	Una de las cuatro instituciones encuestada cuenta con la aprobación de estos acuerdos, el resto carecen de los mismos
Obligar el cambio de contraseñas, así como la utilización de mayúsculas y minúsculas, caracteres especiales, evitar el uso de contraseñas en blanco.	Si bien hacen recomendaciones para la complejidad de las contraseñas no se obliga al cambio constante de las mismas.
Suspender las sesiones inactivas luego de un tiempo definido de inactividad sin consideración de lugar de acceso.	Dos de las cuatro IES encuestadas aseguran no cumplir con la suspensión de la sesión, lo que se considera necesario por motivos de seguridad

Cuadro 4.8. Análisis de cumplimiento de la norma INEN-ISO/IEC 27000 y de Control Interno
Elaborado por: Los autores

Con los resultados recopilados en procesos anteriores. Los autores procedieron a la determinación de conclusiones acerca de la situación actual de las bases de datos analizadas para luego elaborar recomendaciones basadas en lo dispuesto por la norma, permitiendo con ello mejorar las falencias existentes, como se lo muestra a continuación.

AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ **HOJA DE HALLAZGOS Nº 1**
PROCEDIMIENTO: Aplicación de normas y estándares internacionales, que normen el correcto manejo de las bases de datos.
CONDICIÓN: Conforme a la evaluación realizada, se conoció que las instituciones cuentan con políticas y normas internas de cada institución, de las cuales no se tiene detalle alguno.
CRITERIO: La norma de Control Interno 410-07 manifiesta sobre la adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.
CAUSA: La mayoría de las instituciones no dan cumplimiento a ninguna política o norma ya sea nacional o internacional, la mayoría señala que cumplen con normas institucionales de las cuales no se obtuvo mayor detalle que sustente dicha afirmación.
EFECTO: La falta de cumplimiento de alguna norma o política impide que se asegure en un 100% la seguridad de los datos almacenados en las bases de datos de gestión académica de las instituciones.
CONCLUSIÓN: No existen normas que obliguen al cumplimiento de la ley y aseguren la efectividad de la seguridad de las bases de datos.
RECOMENDACIONES: Adopción de la norma técnica ecuatoriana NTE INEN- ISO/IEC 27000, para que exista un mejor control y aseguramiento de la información almacenada en sus bases de datos.

Cuadro 4.9. Hoja de hallazgo Nº1. Normas y Estándares Internacionales
Elaborado por: Los autores

AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ **HOJA DE HALLAZGOS Nº 2**
PROCEDIMIENTO: Establecer ambientes de desarrollo, pruebas y producción de manera independiente.
CONDICIÓN: En la mayoría de las instituciones en el mejor de los casos solo cuentan con el ambiente de producción, pero ninguna cuenta con el de desarrollo, pruebas y producción.
CRITERIO: La norma de Control Interno 410-09 menciona que se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.
CAUSA: Al no contar con una división de sus ambientes, los datos utilizados en el ambiente de prueba corresponderían a datos 100% reales, que pueden ser fácilmente manipulados por personal no autorizado.
EFECTO: El incumplimiento de ésta norma impide que los datos almacenados sean 100% seguros y reales, ya que al no existir una separación de los datos de acuerdo al ambiente en el que se encuentra estos podrían ser modificados y eliminados con facilidad, afectando a todos los procesos académicos involucrados.
CONCLUSIÓN: Se concluye que los datos académicos no son 100% seguros y confiables ya que se carecerían de credibilidad al ser usados en todos los ambientes tanto de desarrollo, prueba y producción.
RECOMENDACIONES: Se recomienda dar cumplimiento a la norma estableciendo los diferentes ambientes propuestos, realizar además una copia de las bases de datos para que tanto desarrollo, prueba y producción trabajen bajo los mismos datos pero sin verse afectados los datos reales.

Cuadro 4.10. Hoja de hallazgo Nº2. Ambientes de desarrollo, prueba y producción
Elaborado por: Los autores

AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ HOJA DE HALLAZGOS Nº 3
PROCEDIMIENTO: Revocar o eliminar el acceso a usuarios con los que las instituciones den por concluido su relación laboral.
CONDICIÓN: En la mayoría de los casos una vez que se da por terminada la relación laboral, no son eliminados sus usuarios y privilegios de manera inmediata.
CRITERIO: La norma de Control Interno 410-10 recomienda la revisión regular de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.
CAUSA: Al seguir teniendo acceso a los sistemas de las instituciones, el personal que ya no forma parte del establecimiento puede seguir accediendo sin mayor problema y realizar cambios de manera intencional.
EFECTO: El efecto con mayor repercusión es la vulnerabilidad presentada, ya que el ex empleado podría fácilmente eliminar o realizar cambios importantes sobre los datos almacenados, provocando la perdida de información indispensable para la institución.
CONCLUSIÓN: Existen usuarios activos del personal que no forman parte de la institución, esto se pudo constatar por uno de los cuestionarios aplicados que hace referencia a este apartado.
RECOMENDACIONES: Eliminar de manera inmediata los usuarios o cambiar su estado de activo a pasivo, para que los sistemas reconozcan éstos y revoque su acceso automáticamente, evitando la fuga de información o la pérdida de la misma.

Cuadro 4.11. Hoja de hallazgo Nº3. Acceso a usuarios
Elaborado por: Los autores

AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ HOJA DE HALLAZGOS Nº 4
PROCEDIMIENTO: Elaborar y aprobar acuerdos de confidencialidad y no divulgación de información.
CONDICIÓN: Las instituciones no cuentan con acuerdos de confidencialidad, por ende sus empleados no conocen ni han firmado acuerdo alguno.
CRITERIO: La norma técnica Ecuatoriana INEN-ISO/IEC 27000 establece elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la constitución, las leyes, las necesidades de protección de información de la institución y el EGSI
CAUSA: El no conocer sobre la norma vigente hace que las instituciones no consideren importante la elaboración de acuerdos de confidencialidad.
EFECTO: Al no existir acuerdos de confidencialidad las personas involucradas en el manejo de datos, se ven exentas de culpa al hacer públicos datos de vital importancia para la institución, datos con un nivel de sensibilidad altos, los mismos que ameritan un manejo confidencial.
CONCLUSIÓN: No existe un conocimiento por ende no se aplican acuerdos de confidencialidad en la mayoría de las instituciones de educación superior, lo que compromete sus datos y exentan a los responsables de su mala utilización.
RECOMENDACIONES: Elaboración de acuerdos de confidencialidad, que den a conocer a cada persona involucrada con el manejo de datos sensibles, que la mala utilización o divulgación de los mismos estará sujeto a sanciones y amonestaciones, que podrán ir desde económicas hasta despidos, dependiendo del caso.

Cuadro 4.12. Hoja de hallazgo Nº4. Acuerdos de confidencialidad
Elaborado por: Los autores

AUDITORÍA DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ HOJA DE HALLAZGOS Nº 5
PROCEDIMIENTO: Obligatoriedad en el cambio de contraseñas.
CONDICIÓN: No existe control con el cambio periódico de las contraseñas de acceso de los sistemas, indistintamente del que fuere.
CRITERIO: La norma técnica Ecuatoriana INEN-ISO/IEC 27000 recomienda en su apartado 7.6 la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplan una complejidad media y alta, evitar contraseñas en blanco o que vienen por defecto según el sistema, puesto que son fácilmente descifrables y por último controlar cambios periódicos de contraseñas de usuarios.
CAUSA: Al no existir un cambio continuo de contraseñas los sistemas se vuelven más vulnerables a ataques, lo que ocasionaría la pérdida de información.
EFECTO: Las instituciones son blanco fácil para personas mal intencionadas que buscan realizar ataques a sus sistemas.
CONCLUSIÓN: No existe regulación alguna que controle y obligue el cambio de contraseñas en un periodo de tiempo determinado, existiendo ocasiones donde los usuarios nunca han realizado cambio alguno.
RECOMENDACIONES: Cumplir la normativa y obligar a todas las personas involucradas al cambio inmediato de sus contraseñas, además dar a conocer de la política que obliga al cambio de las mismas en periodos de tiempo no mayor a 6 meses.

Cuadro 4.13. Hoja de hallazgo Nº5. Cambio de contraseñas
Elaborado por: Los autores

4.1.4. INFORME FINAL

Una vez dada por terminada cada una de las etapas anteriores y luego de haber obtenido cada uno de los resultados esperados, los autores continuaron con la elaboración del informe final de auditoría (ANEXO 6), en el que se incluye todos los hallazgos, conclusiones y recomendaciones, para que las instituciones pertinentes tomen en cuenta para un mejor control en la seguridad de sus bases de datos.

4.2. DISCUSIÓN

Para el desarrollo de la Auditoría de las bases de Datos de Gestión Académica de las Instituciones de Educación Superior Públicas de Manabí, se utilizó como guía varias fases y etapas de la metodología OCTAVE, que como manifiesta (Gómez, *et al* 2010), facilita la evaluación de los riesgos en una organización y se focaliza principalmente en los aspectos relacionados con el día a día de la empresa, también fue necesario realizar una evaluación a las bases de datos conforme lo establecen la Norma de Control Interno y la Norma técnica Ecuatoriana NTE INEN-ISO/IEC2700, ello con el fin de determinar el estado de las mismas.

Realizando una comparativa con trabajos relacionados con auditorías a bases de datos y luego de una indagación exhaustiva, los autores encontraron el trabajo de tesis titulado Procedimientos de Auditoría para la seguridad en las Bases de Datos, del autor Roberto Carlos Almeida Paredes (Almeida, 2014) donde señala que COBIT otorga una mejor interpretación en lo que a mejores prácticas y sistemas de información de auditoría, que ayudan a entender y administrar los riesgos relacionados con la seguridad de las bases de datos.

Por otra parte, en el artículo publicado por Gómez Ricardo, Pérez Diego, Donoso Yezid y Herrera Andrea (Gómez, *et al* 2010) señalan de la existencia de muchas metodologías para la realización de una evaluación de riesgos informáticos, pero que el principal problema al que se está expuesto al realizar este tipo de evaluaciones es la no identificación oportuna de riesgos importantes, a los que eventualmente la organización está expuesta.

Por lo antes expresado y luego de examinados ambos puntos de vista los autores concuerdan con lo expresado por Gómez, *et al* (2010), que en su artículo manifiesta que, al existir diferentes metodologías que aporten y ayuden de manera significativa con la evaluación de los riesgos informáticos presentes en las organizaciones, la metodología OCTAVE resulta una gran ayuda y guía para la identificación y evaluación de los mismos, ya que ésta focaliza los aspectos diarios de las organizaciones ayudando con ello a la identificación

oportuna de riesgos inminentes, dando beneficio a la investigación ya que se analizó directamente los procesos que conllevan a la realización y control de las bases de datos.

Cabe mencionar también que las normativas vigentes son de gran aporte para la mitigación de dichas eventualidades, las cuales representan un apoyo para cualquier metodología aplicada, adicional se propone la utilización de la matriz de riesgo-confianza que permite determinar el nivel de riesgo y confianza en el que se encuentra cada organización de acuerdo a las normas y estándares sobre los cuales fueron evaluados, así mismo de determinar el nivel de concordancia de cada pregunta aplicada por medio del Coeficiente de Concordancia de Kendall, el cual resulta de mucha ayuda al momento de determinar la correlación existente entre las respuestas de las personas encuestadas.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Una vez finalizada la auditoría a las bases de datos de gestión académica de las instituciones de educación superior públicas de Manabí y analizada la información con los datos recopilados, se proporcionan las respectivas conclusiones de la investigación en bases a los resultados obtenidos:

- El análisis de las instituciones de educación superior públicas existentes en Manabí y la identificación de sus bases de datos de gestión académica permitió delimitar la investigación, ya que éste sirvió como punto de partida para la ejecución de la auditoría (**sección 3.1.**)

- Para el desarrollo de la auditoría a las bases de datos fue trascendental contar con una metodología que se acople a las necesidades y objetivos planteados, siendo OCTAVE la elegida, la misma que a través de sus diferentes fases permitió el cumplimiento de cada uno (**sección 3.1.2.**).

- Con el estudio de las normas y estándares vigentes tanto nacionales como internacionales (**sección 2.3.5.3**), se obtuvo una guía para la elaboración de los cuestionarios que permitieron conocer el estado en el que se encontraban las bases de datos, en aspectos, lógicos, seguridad, calidad, administración y protección, los mismos que sirvieron para la identificación de los riesgos que generan el incumplimiento de los mismos (**Anexo 2 y 5**).

- La utilización de técnicas como check list y el coeficiente de concordancia de Kendall permitieron conocer de manera confiable información sobre la evaluación de las bases de datos, detallando cada uno de los hallazgos encontrados durante la ejecución de la auditoría determinando así medidas de protección (**sección 4.1.3.1.**).

5.2. RECOMENDACIONES

Concluida la auditoría a las bases de datos de gestión académica de las instituciones de educación superior públicas de Manabí, los autores recomiendan lo siguiente:

- Es importante que las instituciones de educación superior tanto pública como privada, cuenten con una unidad de auditoría interna, para que realicen auditorías periódicas con el fin de tomar medidas preventivas y correctivas que ayuden a la mitigación de vulnerabilidades.

- Es necesario que en lo posterior se indague a profundidad sobre las metodologías informáticas existentes, seleccionando la que mejor se acople a las necesidades y los objetivos planteados para con ello dar cumplimiento a cabalidad con los mismos.

- Considerando la acelerada evolución de las tecnologías es necesario que las instituciones conozcan sobre las normas y estándares vigentes, para la seguridad y protección de sus datos, utilizando estos como una guía para un manejo adecuado de los mismos, garantizando calidad y confiabilidad en sus operaciones.

- Para el posterior desarrollo de auditorías realizar un análisis profundo de todos los procesos y operaciones que contienen las bases de datos, aplicar técnicas necesarias que aporten a la evaluación y el procesamiento de los datos, aportando con información suficiente que permitan sustentar cada uno de los hallazgos encontrados.

BIBLIOGRAFÍA

Acuerdo Nº 039 CG. 2009. Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos. San Francisco de Quito, EC. 16 de feb.

Amutio, M. 2012. MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. (En línea). ES. Consultado el 21 de febrero de 2015. Formato PDF. Disponible en https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_ metodo.pdf

Audisa, 2010. Checklist, ¿Qué es?¿Para qué sirve?. (en línea). Consultado el 5 de marzo de 2015. Disponible en https://audisa.wordpress.com/2010/11/02/checklist-%C2%BFque-es%C2%BFpara-que-sirve/

Azán, Y; Bravo, L; Rosales, W; Trujillo, D; García, E; Pimentel, A. 2014. Solución basada en el Razonamiento Basado en casos para el apoyo a las auditorías informáticas a bases de datos. La Habana. Revista Cubana de Ciencias Informáticas. Vol. . n. 2.

Badia, D. 2012. Metodología de los mapas de concordancia para la estratificación de variables cuantitativas: aplicación a la asignatura de medidas electrónicas. Tesis doctoral. Universidad Ramón Llull la Salle. Barcelona, ES. p.71

Bortnik, S. 2010. La serie de normas ISO 27000. (En línea). ESET. Consultado 20 de mayo 2015. Formato HTML. Disponible en http://www.welivesecurity.com/la-es/2010/04/16/la-serie-de-normas-iso-27000/

Capote, T; Brito, Y; Yzquierdo, R; Febles, A. 2014. Estrategia para desarrollar la perspectiva Procesos internos en un laboratorio de pruebas de software. La Habana. Revista Cubana de Ciencias Informáticas. Vol.8 . n. 4.

CGE (Contraloría General del Estado). s.f. Manual de Auditoría financiera. 12 ed. Quito-EC. p 252 – 276.

BBMapfre. 2014. Metodología de evaluación de riesgos operacionales y controles. (En línea). Consultado 16 de febrero 2016. Formato HTML. Disponible en https://www.fundacionmapfre.org/documentacion/.../i18n/catalogo_imagenes/imagen.cmd?path=1079028&posicion=1

ESPAM MFL (Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López). 2016. Reseña Histórica. (En línea). EC. Consultado 19 de mayo 2016. Formato HTML.Disponible en http://espam.edu.ec/

Gelbstein, E. 2011. La integridad de los datos: el aspecto más relegado de la seguridad de la información. ISACA JOURNAL. Vol 6.

Godás, D. 2011. Esquemas de Seguridad Informática. (En línea). Consultado 20 de mayo 2015. Formato HTML. Disponible en http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/PoliticasNecesarias.php

Gómez, G; Oltra, R; Adarme, W. 2014. Gestión de calidad de servicios basado en ITIL. Medellín, COL. Revista DYNA. Nº 1. p 53

Gómez, O; Estrada, V; Bauta, R; García, I. 2012. Modelo de gestión de log para la auditoria de información de apoyo a la toma de decisiones en las organizaciones. La Habana, CU. Revista ACIMED. Nº 23. Vol. 2. p 187-200

Gómez, R; Hernán, D; Donoso, Y; Herrera, A. 2010. Metodología y gobierno de riesgo de tecnologías de información. Bogotá, CO. Revista de ingeniería. Vol. 31. p 109-118

Gutiérrez, C. 2013 ¿Qué es y por qué hacer un análisis de riesgos? (En línea). ESET. Consultado 20 de mayo 2015. Formato HTML. Disponible en http://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

_____. 2013. Metodología práctica para gestionar riesgos. (En línea). Consultado el 10 de Enero de 2015. Formato (HTML). Disponible en http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Hernández, A. 2010. Auditoria Informática y Gestión de Tecnologías de Información y Comunicación. Compendiun, VE. Vol. 13. Nº. 25. p 4.

Hernández, D; Cuza, B. 2013. Modelos causales para la Gestión de Riesgos. La Habana-Cu. Rev cuba cienc informat [online]. vol.7, N.4, pp. 58-74. ISSN 2227-1899.

Hernández, E. 2010. Seguridad y privacidad en los sistemas informáticos. (En Línea). ES. Consultado, 12 mayo 2015. Formato PDF. Disponible en http://www.disca.upv.es/enheror/pdf/ACTASeguridad.PDF

Hernández, E; López, M; Olivares, A; Román, D. 2010. Modelo de seguridad de base de datos. Tesis. Lcdo. en Ciencias de la Informática. Instituto Politécnico Nacional. México D.F., MX. p. 108.

Hernández, J; Hernández, G. 2007. Sistema de información y Gestión académica de estudiantes para los institutos Politécnicos de Informática del país. Universidad de La Habana, CU. Revista Memorias. Vol. 5. p. 12 – 18.

Herrera, F; Mesa, M; Ramos, A. 2010. La infraestructura computacional para la informatización de la gestión académica en la Universidad. Universidad

Central Marta Abreu de Las Villas, CU. Revista Tecnológica. Vol. 3. p 5–8.

Herrera, Y. 2013. Minería de procesos como herramienta para la auditoría. La Habana, CU. Revista Ciencias de la Información. Vol 44. p 25 – 32.

Kioskea. 2014. Introduccion-Base de datos. (En linea). Consultado el 3 de noviembre de 2014. Formato (HTML). Disponible en http://es.kioskea.net/contents/66-introduccion-bases-de-datos

Landino, M; Villa, P; López, A. 2011. Fundamentos de ISO 27001 y su aplicación en las empresas. Universidad Tecnológica de Pereira. COL Revista de Científica. N. 47. p 334 - 339.

López, J; Zuluaga, A. 2013. Metodología para el Control de Riesgos para la auditoría de Bases de Datos. Tesis. Ing. De Sistemas y Computación. Universidad tecnológica de Pereira. Colombia. p 18.

Martínez, A. 2012. Auditoria con Informática. Revista de arquitectura e Ingeniería. Vol. 6. Nº 2. p 3. Cuba.

McGraw-Hill Companies. 2010. Sistemas gestores de bases de datos (En linea). Consultado el 3 de noviembre de 2014. Formato (PDF). Disponible en http://www.mcgraw-hill.es/bcv/guide/ capitulo/ 8448148797.pdf

Mendoza, M. 2013. Tipos y modelos de bases de datos. (En línea). CO. Consultado 14 de mayo 2015. Formato PDF. Disponible en https://tecnologiaeinformaticacji.files.wordpress.com/2013/02/lectura-tipos-de-bases-de-datos.pdf

Meneses, C; Gálvez, J; Chavarro, J; Febles, A. 2011. Especificación de temporalidad en modelos conceptuales para bases relacionales y orientadas a objetos. Universidad Tecnológica de Pereira. COL. Revista Scientia et Technica. Vol.17 . n. 47. p 130 - 135

Montesino, R; Baluja, W; Porvén, J. 2013. Gestión automatizada e integridad de controles de seguridad informática. La Habana, CU. Revista RIELAC. Vol. 34. p 40-58

Nuñez, L; Reyes, Y; Álvarez, Y; González, M. 2014. Selección de productos antivirus. Una mirada actual desde el sector de la salud en Cuba. Ciudad de la Habana. Revista Cubana de Informática Médica. Vol. 6. n. 2.

Osiatis S.A. 2013. ¿Qué es ITIL?. (En línea). Consultado el 4 de marzo de 2015. Formato (HTML). Disponible en http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Pérez, J. 2011. Las bases de datos, su seguridad y auditoría. El caso de MySql. Tesis. Ing. Técnica en informática de gestión. Universidad Carlos III de Madrid. Leganés-Madrid, ES. p. 244.

Pinto . M. 2011. Bases de datos. (En linea). Consultado el 3 de Noviembre de 2014. Formato (HTML). Disponible en http://www.mariapinto.es/e-coms/bases_datos.htm

Poblete, G. 2011. Bases de datos multidimencionales para datos educacionales (En linea). Consultado el 15 de febrero de 2016. Formato (PDF). Disponible en http://jcc2013.inf.uct.cl/wp-content/proceedings/ECC/Bases%20de%20Datos%20multidimensionales%20para%20datos%20educacionales.pdf

Pons, F. 2011. Auditoría informática, una aproximación a la mejora del control interno. CH. Revista Nuevas Tecnologías. Nº 41. p. 97 – 100.

Prado, M. 2011. Diseño y administración de base de datos relacionales. Tesis. Ing. en Comunicación y Electrónica. Instituto Politécnico Nacional. México D.F., MX. p. 95.

Ramírez, E; Torres, I; Yañez, J; Mosqueda, Y. 2010. Auditoría a las bases de datos SQL del sistema de “seguridad de presas” CONAGUA. Tesis. Lcdo. en Ciencias de la Informática. Instituto Politécnico Nacional. México D.F., MX. p. 136.

Rodríguez, A. 2010. La seguridad informática una necesidad en la docencia universitaria. CU. Revista IPLAC. Nº 1.

Rojas, Á; Castro, D. 2012. Riesgos, Amenazas y Vulnerabilidades de los sistemas de información. Universidad Católica de Colombia. Revista de Ingeniería de Sistemas. Vol. 7. p 15.

Ruiz, A. 2011. Un sistema de auditoría de seguridad informática avanzado bajo GNU/Linux. Tesis. Ing. Informática. Universidad de Almería. ES. p 30

SNAP (Secretaría Nacional de la Administración Pública). 2013. Esquema Gubernamental de Seguridad de la Información (EGSI). EC. v 1.0.

CGE (Contraloría General del Estado). s.f. Manual de Auditoría financiera. 12 ed. Quito-EC. p 252 – 276.

Santillana, J. 2013. Auditoría Interna (En linea). Consultado el 16 de febrero de 2016. Formato (PDF). Disponible en http https://catedrafinancierags.files.wordpress.com/2012/04/auditoria-interna-juan-ramc3b3n-santillana.pdf

Senplades, 2010. Transformar la universidad para transformar a la sociedad. 1era ed. Quinto. EC. p 9 -11

Sierra, N. 2014. Definición, obejtivos y carácteristicas de COBIT. (En linea). Consultado el 31 de Enero de 2015. Formato (HTML). Disponible en https://www.academia.edu/8412401/COBIT_Esperanza_Rojas_Rojas_Auditoria_de_Sistemas

ULEAM (Universidad Laica Eloy Alfaro de Manabí). 2016. Reseña Histórica. (En línea). EC. Consultado 19 de mayo 2016. Formato HTML.Disponible en http://www.uleam.edu.ec/

UNESUM (Universidad Estatal Del Sur de Manabí). 2016. Reseña Histórica. (En línea). EC. Consultado 19 de mayo 2016. Formato HTML.Disponible en http://unesum.edu.ec/

UTM (Universidad Técnica de Manabí). 2016. Reseña Histórica. (En línea). EC. Consultado 19 de mayo 2016. Formato HTML.Disponible en http://www.utm.edu.ec/

ANEXOS

ANEXO 1
OFICIOS DE AUTORIZACIÓN

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ

COORDINACIÓN
UNIDAD TECNOLÓGICA

Oficio Nº ESPAM MFL-CUT-2015-0051-OF
Calceta, 21 de julio de 2015

Magister, Ing.
César Moreira Zambrano
ADMISNISTRADOR DATA CENTER DE LA ESPAM MFL
Presente.-

De mi consideración:

En respuesta al oficio Nº ESPAM MFL-CI-2014-011-OF de fecha 19 de enero del 2015, tengo a bien comunicarle de la manera más cordial, preste sus conocimientos y les brinde la facilidad para la elaboración de la tesis de los alumnos **FRANK MONTESDEOCA JUAN JOSÉ Y ROMERO PINO MERCEDES CECIBEL,** dicho pedido de mi parte es por cuanto el tema de ellos se refiere bastante a sus conocimientos en lo que es BASE DE DATOS.

Adjunto copia del oficio solicitado por la Ingeniera Jéssica Morales Carrillo, Directora de la Carrera de Informática.

Contando con su ayuda, quedo de Usted, eternamente agradecido.

Particular que informo para los fines correspondientes.

Atentamente,

Lic. Geovanny García Montes
COORDINADOR (E) DE LA UNIDAD TECNOLÓGICA DE LA ESPAM MFL

Recibido
21-07-2015
18:40

WWW.ESPAM.EDU.EC

REPÚBLICA DEL ECUADOR

ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

Departamento de las TICS, para los fines pertinentes.

Oficio n.°: ESPAM MFL-CI-2016- 002-OF
Calceta, 21 de enero de 2016

UNIVERSIDAD TÉCNICA DE MANABÍ
RECTORADO
26 ENE 2016
Hora: 09H49
RECIBIDO POR:

ASUNTO: Solicitud para realizar una encuesta.

Ingeniero
Vicente Véliz Briones
RECTOR DE LA UNIVERSIDAD TÉCNICA DE MANABÍ
Portoviejo.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel, que deben efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática; así mismo, todo tema de tesis de grado estará relacionado con las líneas de investigación de la carrera, enmarcados en las áreas y prioridades de investigación establecidas por la ESPAM MFL en concordancia con el Plan Nacional del Buen Vivir.

Con estos antecedentes, solicito a usted de la manera más cordial, se brinde la facilidad de aplicar una encuesta para la obtención de información en la elaboración del trabajo de investigación titulado "**AUDITORIA A LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL EN EL CANTÓN BOLÍVAR**"; por parte de los señores: **Frank Montesdeoca Juan José** y **Romero Pino Mercedes Cecibel**, egresados de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida.

Atentamente,

Ing. Jéssica Morales Carrillo
DIRECTORA CARRERA DE INFORMÁTICA ESPAM-MFL

JMC/rvm

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
"MANUEL FÉLIX LÓPEZ

REPÚBLICA DEL ECUADOR

CARRERA DE INFORMÁTICA

Oficio Nº ESPAM MFL - CI – 2015- 453-OF
Calceta, 23 de diciembre de 2015

Asunto: Solicitud para realizar una encuesta.

Doctor
Miguel Camino Solórzano
RECTOR ENCARGADO DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ
Manta.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel que tienen que efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática y, dentro de estas, las Instituciones públicas o privadas.

Con estos antecedentes, solicito a usted de la manera más cordial, se brinde la facilidad de aplicar una encuesta para la obtención de información en la elaboración del trabajo de investigación titulado "***AUDITORIA A LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL EN EL CANTÓN BOLÍVAR***"; por parte de los señores: **Frank Montesdeoca Juan José** y **Romero Pino Mercedes Cecibel**, egresados de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida

Atentamente,

Ing. Jéssica Morales Carrillo,
DIRECTORA CARRERA DE INFORMÁTICA ESPAM – MFL
JMC/rvm

RECIBIDO
18 ENE 2016
10h04
SECRETARIA RECTORADO

Por favor atender Departamento de la Tics

1 / 1

Dirección: Campus Politécnico Sitio "El Limón". **Teléfono: (05)3029021**
Email: informatica@espam.edu.ec - carrerainformaticaespam@gmail.com
CALCETA - ECUADOR

REPÚBLICA DEL ECUADOR

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

Oficio n.º: ESPAM MFL-CI-2016- 003-OF
Calceta, 20 de enero de 2016

DEPARTAMENTO DE CIENCIAS INFORMÁTICAS PARA LOS FINES PERTINENTES

ASUNTO: Solicitud para realizar una encuesta.

Doctor
Omelio Borroto Leal
RECTOR ENCARGADO DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ
Jipijapa.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel, que deben efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática; así mismo, todo tema de tesis de grado estará relacionado con las líneas de investigación de la carrera, enmarcados en las áreas y prioridades de investigación establecidas por la ESPAM MFL en concordancia con el Plan Nacional del Buen Vivir.

Con estos antecedentes, solicito a usted de la manera más cordial, se brinde la facilidad a los egresados: **Frank Montesdeoca Juan José** y **Romero Pino Mercedes Cecibel**, para aplicar una encuesta que permitirá realizar un análisis estadístico comparativo de las normativas y base de datos académicas en las universidades públicas de Manabí; se asegura que la información proporcionada en la encuesta será procesada de manera confidencial.

Esperando favorable acogida a la presente quedo de usted agradecida.

Atentamente,

RECIBIDO
22 ENE 2016
RECTORADO
10:35

Ing. Jéssica Morales Carrillo
DIRECTORA CARRERA DE INFORMÁTICA ESPAM-MFL

JMC/rvm

1 / 1

Dirección: Campus Politécnico Sitio "El Limón". **Teléfono: (05)3029021 - (05)2 686102**
Email: informatica@espam.edu.ec - carrerainformaticaespam@gmail.com
www.espam.edu.ec
CALCETA – MANABÍ - ECUADOR

ANEXO 2
FORMATO DE LOS CUESTIONARIOS DE EVALUACIÓN GENERAL DE LAS BASES DE DATOS

CARRERA DE INFORMÁTICA DE LA ESPAM MFL
TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL
AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

ÁREA:			**FECHA DE APLICACIÓN:**				
DIRIGIDO:			**FUNCIÓN:**				
#		**PREGUNTA**	**CUMPLIMIENTO**				
			0%	**25%**	**50%**	**75%**	**100%**
DATOS	1	¿La redundancia de la base de datos está controlada?					
	2	¿La base de datos está convenientemente documentada?					
	3	¿La base de datos posee valor informativo?					
ADMINISTRADOR DE LAS BASES DE DATOS	4	¿El administrador tiene formación adecuada para el desarrollo de sus funciones?					
	5	¿Tiene experiencia?					
	6	¿Existen políticas y procedimientos de seguridad para la base de datos?					
	7	¿El personal que utiliza la base de datos ha sido capacitado?					
			NUNCA	**POCAS VECES**	**ALGUNAS VECES**	**CASI SIEMPRE**	**SIEMPRE**
	8	¿El administrador interactúa y mantiene comunicación fluida con usuarios, directivos, analistas, programadores, suministradores y personal de administración?					
	9	¿Se ha involucrado en la capacitación a los usuarios?					
	10	¿Ha establecido estándares para asegurar que la base de datos mantiene la seguridad e integridad de los datos?					
	11	¿Ha realizado una descripción conceptual y lógica de la base de datos?					
CALIDAD			**0%**	**25%**	**50%**	**75%**	**100%**
	12	¿La institución tiene política de calidad?					
	13	¿Se cumple con las políticas de seguridad?					
	14	¿Conoce la ley de acceso a los datos?					
			0 – 6 MESES	**6 -12 MESES**	**12- 18 MESES**	**18 – 24 MESES**	**MÁS DE 24 MESES**
	15	¿Con que frecuencia se realizan auditorías?					
			0%	**25%**	**50%**	**75%**	**100%**
ASPECTOS LÓGICOS	16	¿Se ha formado a los empleados en la correcta utilización de los programas antivirus y firewall?					
	17	¿Los datos están disponibles para los usuarios autorizados?					
	18	¿Los datos son validados antes de ser introducidos en la Base de datos?					
	19	¿El acceso a la base de datos se realiza mediante una conexión segura?					
			NUNCA	**POCAS VECES**	**ALGUNAS VECES**	**CASI SIEMPRE**	**SIEMPRE**
	20	¿Se limita o controla de alguna manera el número de intentos fallidos de conexión?					
SEGURIDAD Y PROTECCIÓN DE LOS DATOS	21	¿Cuándo se recoge información personal, el usuario es informado de la existencia de un fichero o almacén que contiene esa información y los derechos que tiene sobre ellos?					
	22	¿La persona que tiene almacenados sus datos en un fichero o tabla de la base de datos puede consultarlos y acceder a ellos?					
	23	¿Se garantiza la seguridad de la información personal?					
	24	¿Se puede garantizar la seguridad de los datos personales almacenados en la base de datos?					
	25	¿Los datos sólo se dan a conocer si es para fines educativos?					
	26	¿La persona que cede sus datos puede verlos, rectificarlos en caso de ser erróneos o haber cambiado o puede eliminarlos si así lo desea?					
	27	¿Se han tenido en cuenta los posibles cambios tecnológicos?					

	28	¿En las políticas se ha recogido la prevención y detección de virus, así como otro software malicioso?					
	29	¿Los usuarios y empleados realmente respetan las políticas de seguridad que se recogen en los manuales?					
			MUY BAJA	**BAJA**	**MEDIA**	**ALTA**	**MUY ALTA**
	30	¿Existe seguridad de acceso al recinto, ya sea mediante guardias de seguridad, tarjetas de control, seguridad biométrica, etc.?					
			NUNCA	**POCAS VECES**	**ALGUNAS VECES**	**CASI SIEMPRE**	**SIEMPRE**
	31	¿El acceso físico a despachos, equipos, etc., se encuentra realmente bien controlado?					
	32	¿Se adoptan medidas de seguridad en el departamento de sistemas de información?					
	33	¿Existe una persona responsable de la seguridad?					
	34	¿Se controla el trabajo fuera de horario?					
PROTECCIÓN DE SOFTWARE MALICIOSO	35	¿Se controla la descarga de software no autorizado?					
	36	¿Existe antivirus instalado, en uso y actualizado en todos los puestos donde esté instalada la base de datos (servidor, clientes)?					
	37	¿Se realizan revisiones periódicas del software instalado en los sistemas?					
	38	¿Se investiga formalmente la presencia de ficheros no aprobados o de la modificación de ficheros no autorizados?					
	39	¿Se controla el acceso a los servicios en redes internas y externas?					
	40	¿Se realiza un "escaneo" previo de todo fichero adjunto en un correo electrónico a través de un programa antivirus antes de descargarlo?					

Nº	**PREGUNTAS**	**RESPUESTA**		**CUMPLIMIENTO**		**OBSERVACIONES**
		SI	**NO**	**POND**	**CAL**	
1	¿Existen políticas, normas y procedimientos para la implementación y administración de bases de datos?			**10**		
2	¿Existe una persona responsable en la administración de bases de datos?			**10**		
3	¿Existen log de registros de acceso?			**10**		
4	¿Se realizan respaldos periódicos de la información?			**10**		**¿Cada cuánto tiempo?**
5	¿Existe control de acceso en los puertos?			**10**		
6	¿La solicitud y autorización de accesos a la base de datos se hace por escrito?			**10**		
7	¿Las características de longitud, composición (que permita letras mayúsculas y minúsculas, números y caracteres especiales), encriptado, etc. son adecuadas para que estos no sean fácilmente deducidos?			**10**		
8	¿Prevén que las contraseñas no sean difundidas en forma inadvertida, ni desplegados durante el proceso de acceso a la red o impresos en alguna salida?			**10**		
9	¿Prevén que las contraseñas sean almacenadas en archivos encriptados?			**10**		

10	¿Contemplan políticas de cambio frecuente de éstos. Por ej. Usar una fecha de expiración asociada a las contraseñas o limitar su uso a un número determinado de accesos para obligar su cambio?			**10**		
11	¿Prevén la eliminación de las claves de acceso de aquellos individuos que cesan su relación de trabajo con la empresa?			**10**		
12	¿Prevén la desconexión automática cuando transcurren algunos minutos de haber realizado el último acceso al sistema (última instrucción tecleada)?			**10**		
13	¿Prevén la suspensión del código de acceso, o la deshabilitación del sistema en caso que haya varios intentos de acceso fallidos durante el mismo día?			10		
14	¿Existe suficiente espacio físico para almacenar completa y correctamente los datos?			**10**		
15	¿Existe algún reciento cerrado (habitación, despacho, local) donde se encuentran situados todos los servidores?			**10**		**¿Se controla el acceso?**
16	¿Existe alguna alarma contra intrusos interconectada con la policía?			**10**		
17	¿Existe un documento de política de seguridad de la información accesible para los empleados donde puedan realizar consultas sobre ella?			**10**		
18	¿Esta política se revisa periódicamente para asegurarse que no ha variado nada y que se recoge todo lo necesario?			**10**		
19	¿Los empleados conocen las consecuencias de las violaciones de la política de seguridad?			**10**		
20	¿Existe un tiempo forzoso de espera antes de permitir un nuevo intento de conexión?			**10**		
21	¿Existe desconexión automática de la base de datos tras un tiempo prudencial de inactividad?			**10**		
22	¿El acceso a la base de datos se realiza mediante una conexión segura?			**10**		
TOTALES						
PONDERACION TOTAL (PT)				**220**		
CALIFICACIÓN TOTAL (CT)						

ANEXO 3
CUESTIONARIOS DE EVALUACIÓN GENERAL DE LAS BASES DE DATOS

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL

AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

ASPECTOS LÓGICOS DE LAS BASES DE DATOS

ÁREA:

FECHA DE APLICACIÓN:

DIRIGIDO:

FUNCIÓN:

	#	PREGUNTA	CUMPLIMIENTO				
			0%	25%	50%	75%	100%
DATOS	1	¿La redundancia de la base de datos está controlada?			X		
	2	¿La base de datos está convenientemente documentada?		X			
	3	¿La base de datos posee valor informativo?				X	
ADMINISTRADOR DE LAS BASES DE DATOS	4	¿El administrador tiene formación adecuada para el desarrollo de sus funciones?					X
	5	¿Tiene experiencia?					X
	6	¿Existen políticas y procedimientos de seguridad para la base de datos?					X
	7	¿El personal que utiliza la base de datos ha sido capacitado?					X
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	8	¿El administrador interactúa y mantiene comunicación fluida con usuarios, directivos, analistas, programadores, suministradores y personal de administración?					X
	9	¿Se ha involucrado en la capacitación a los usuarios?				X	
	10	¿Ha establecido estándares para asegurar que la base de datos mantiene la seguridad e integridad de los datos?			X		
	11	¿Ha realizado una descripción conceptual y lógica de la base de datos?	X				
			0%	25%	50%	75%	100%
CALIDAD	12	¿La institución tiene política de calidad?		X			
	13	¿Se cumple con las políticas de seguridad?				X	
	14	¿Conoce la ley de acceso a los datos?				X	
			0 – 6 MESES	6 -12 MESES	12- 18 MESES	18 – 24 MESES	MÁS DE 24 MESES
	15	¿Con que frecuencia se realizan auditorías?					X
			0%	25%	50%	75%	100%
ASPECTOS LÓGICOS	16	¿Se ha formado a los empleados en la correcta utilización de los programas antivirus y firewall?	X				
	17	¿Los datos están disponibles para los usuarios autorizados?				X	
	18	¿Los datos son validados antes de ser introducidos en la Base de datos?					X
	19	¿El acceso a la base de datos se realiza mediante una conexión segura?					X
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	20	¿Se limita o controla de alguna manera el número de intentos fallidos de conexión?		X			

SEGURIDAD Y PROTECCIÓN DE LOS DATOS	21	¿Cuándo se recoge información personal, el usuario es informado de la existencia de un fichero o almacén que contiene esa información y los derechos que tiene sobre ellos?	X				
	22	¿La persona que tiene almacenados sus datos en un fichero o tabla de la base de datos puede consultarlos y acceder a ellos?					X
	23	¿Se garantiza la seguridad de la información personal?					X
	24	¿Se puede garantizar la seguridad de los datos personales almacenados en la base de datos?					X
	25	¿Los datos sólo se dan a conocer si es para fines educativos?				X	
	26	¿La persona que cede sus datos puede verlos, rectificarlos en caso de ser erróneos o haber cambiado o puede eliminarlos si así lo desea?	X				
	27	¿Se han tenido en cuenta los posibles cambios tecnológicos?			X		
	28	¿En las políticas se ha recogido la prevención y detección de virus, así como otro software malicioso?			X		
	29	¿Los usuarios y empleados realmente respetan las políticas de seguridad que se recogen en los manuales?				X	
			MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
	30	¿Existe seguridad de acceso al recinto, ya sea mediante guardias de seguridad, tarjetas de control, seguridad biométrica, etc.?			X		
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	31	¿El acceso físico a despachos, equipos, etc., se encuentra realmente bien controlado?			X		
	32	¿Se adoptan medidas de seguridad en el departamento de sistemas de información?			X		
	33	¿Existe una persona responsable de la seguridad?			X		
	34	¿Se controla el trabajo fuera de horario?		X			
PROTECCIÓN DE SOFTWARE MALICIOSO	35	¿Se controla la descarga de software no autorizado?	X				
	36	¿Existe antivirus instalado, en uso y actualizado en todos los puestos donde esté instalada la base de datos (servidor, clientes)?		X			
	37	¿Se realizan revisiones periódicas del software instalado en los sistemas?			X		
	38	¿Se investiga formalmente la presencia de ficheros no aprobados o de la modificación de ficheros no autorizados?	X				
	39	¿Se controla el acceso a los servicios en redes internas y externas?			X		
	40	¿Se realiza un "escaneo" previo de todo fichero adjunto en un correo electrónico a través de un programa antivirus antes de descargarlo?		X			

Nº	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existen políticas, normas y procedimientos para la implementación y administración de bases de datos?		X	10		
2	¿Existe una persona responsable en la administración de bases de datos?	X		10	9	
3	¿Existen log de registros de acceso?	X		10	8	
4	¿Se realizan respaldos periódicos de la información?	X		10	10	¿Cada cuánto tiempo? Diario
5	¿Existe control de acceso en los puertos?		X	10		
6	¿La solicitud y autorización de accesos a la base de datos se hace por escrito?		X	10		
7	¿Las características de longitud, composición (que permita letras mayúsculas y minúsculas, números y caracteres especiales), encriptado, etc. son adecuadas para que estos no sean fácilmente deducidos?	X		10	10	
8	¿Prevén que las contraseñas no sean difundidas en forma inadvertida, ni desplegados durante el proceso de acceso a la red o impresos en alguna salida?	X		10	8	
9	¿Prevén que las contraseñas sean almacenadas en archivos encriptados?	X		10	9	
10	¿Contemplan políticas de cambio frecuente de éstos. Por ej. Usar una fecha de expiración asociada a las contraseñas o limitar su uso a un número determinado de accesos para obligar su cambio?		X	10		
11	¿Prevén la eliminación de las claves de acceso de aquellos individuos que cesan su relación de trabajo con la empresa?	X		10	10	
12	¿Prevén la desconexión automática cuando transcurren algunos minutos de haber realizado el último acceso al sistema (última instrucción tecleada)?	X		10	10	
13	¿Prevén la suspensión del código de acceso, o la deshabilitación del sistema en caso que haya varios intentos de acceso fallidos durante el mismo día?	X		10	8	
14	¿Existe suficiente espacio físico para almacenar completa y correctamente los datos?	X		10	10	
15	¿Existe algún reciento cerrado (habitación, despacho, local) donde se encuentran situados todos los servidores?	X		10	10	¿Se controla el acceso? Si

16	¿Existe alguna alarma contra intrusos interconectada con la policía?		X	10		
17	¿Existe un documento de política de seguridad de la información accesible para los empleados donde puedan realizar consultas sobre ella?		X	10		
18	¿Esta política se revisa periódicamente para asegurarse que no ha variado nada y que se recoge todo lo necesario?		X	10		
19	¿Los empleados conocen las consecuencias de las violaciones de la política de seguridad?		X	10		
20	¿Existe un tiempo forzoso de espera antes de permitir un nuevo intento de conexión?		X	10		
21	¿Existe desconexión automática de la base de datos tras un tiempo prudencial de inactividad?	X		10	8	
22	¿El acceso a la base de datos se realiza mediante una conexión segura?	X		10	8	
TOTALES						
PONDERACION TOTAL (PT)				220		
CALIFICACIÓN TOTAL (CT)						

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL

AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

ASPECTOS LÓGICOS DE LAS BASES DE DATOS

ÁREA:

DIRIGIDO:

FECHA DE APLICACIÓN: 18/01/2016

FUNCIÓN: Director

	#	PREGUNTA	CUMPLIMIENTO				
			0%	25%	50%	75%	100%
DATOS	1	¿La redundancia de la base de datos está controlada?		X			
	2	¿La base de datos está convenientemente documentada?	X				
	3	¿La base de datos posee valor informativo?			X		
ADMINISTRADOR DE LAS BASES DE DATOS	4	¿El administrador tiene formación adecuada para el desarrollo de sus funciones?		X			
	5	¿Tiene experiencia?		X			
	6	¿Existen políticas y procedimientos de seguridad para la base de datos?	X				
	7	¿El personal que utiliza la base de datos ha sido capacitado?		X			
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	8	¿El administrador interactúa y mantiene comunicación fluida con usuarios, directivos, analistas, programadores, suministradores y personal de administración?		X			
	9	¿Se ha involucrado en la capacitación a los usuarios?		X			
	10	¿Ha establecido estándares para asegurar que la base de datos mantiene la seguridad e integridad de los datos?	X				
	11	¿Ha realizado una descripción conceptual y lógica de la base de datos?	X				
			0%	25%	50%	75%	100%
CALIDAD	12	¿La institución tiene política de calidad?		X			
	13	¿Se cumple con las políticas de seguridad?	X				
	14	¿Conoce la ley de acceso a los datos?				X	
			0 – 6 MESES	6 -12 MESES	12- 18 MESES	18 – 24 MESES	MÁS DE 24 MESES
	15	¿Con que frecuencia se realizan auditorías?				X	
			0%	25%	50%	75%	100%
ASPECTOS LÓGICOS	16	¿Se ha formado a los empleados en la correcta utilización de los programas antivirus y firewall?	X				
	17	¿Los datos están disponibles para los usuarios autorizados?		X			
	18	¿Los datos son validados antes de ser introducidos en la Base de datos?			X		
	19	¿El acceso a la base de datos se realiza mediante una conexión segura?	X				
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	20	¿Se limita o controla de alguna manera el número de intentos fallidos de conexión?	X				

SEGURIDAD Y PROTECCIÓN DE LOS DATOS	21	¿Cuándo se recoge información personal, el usuario es informado de la existencia de un fichero o almacén que contiene esa información y los derechos que tiene sobre ellos?	X				
	22	¿La persona que tiene almacenados sus datos en un fichero o tabla de la base de datos puede consultarlos y acceder a ellos?		X			
	23	¿Se garantiza la seguridad de la información personal?	X				
	24	¿Se puede garantizar la seguridad de los datos personales almacenados en la base de datos?	X				
	25	¿Los datos sólo se dan a conocer si es para fines educativos?	X				
	26	¿La persona que cede sus datos puede verlos, rectificarlos en caso de ser erróneos o haber cambiado o puede eliminarlos si así lo desea?	X				
	27	¿Se han tenido en cuenta los posibles cambios tecnológicos?		X			
	28	¿En las políticas se ha recogido la prevención y detección de virus, así como otro software malicioso?	X				
	29	¿Los usuarios y empleados realmente respetan las políticas de seguridad que se recogen en los manuales?	X				
			MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
	30	¿Existe seguridad de acceso al recinto, ya sea mediante guardias de seguridad, tarjetas de control, seguridad biométrica, etc.?		X			
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	31	¿El acceso físico a despachos, equipos, etc., se encuentra realmente bien controlado?		X			
	32	¿Se adoptan medidas de seguridad en el departamento de sistemas de información?		X			
	33	¿Existe una persona responsable de la seguridad?	X				
	34	¿Se controla el trabajo fuera de horario?	X				
PROTECCIÓN DE SOFTWARE MALICIOSO	35	¿Se controla la descarga de software no autorizado?	X				
	36	¿Existe antivirus instalado, en uso y actualizado en todos los puestos donde esté instalada la base de datos (servidor, clientes)?	X				
	37	¿Se realizan revisiones periódicas del software instalado en los sistemas?	X				
	38	¿Se investiga formalmente la presencia de ficheros no aprobados o de la modificación de ficheros no autorizados?	X				
	39	¿Se controla el acceso a los servicios en redes internas y externas?	X	X			
	40	¿Se realiza un "escaneo" previo de todo fichero adjunto en un correo electrónico a través de un programa antivirus antes de descargarlo?	X				

Nº	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existen políticas, normas y procedimientos para la implementación y administración de bases de datos?		X	10		
2	¿Existe una persona responsable en la administración de bases de datos?		X	10		
3	¿Existen log de registros de acceso?		X	10		
4	¿Se realizan respaldos periódicos de la información?		X	10		¿Cada cuánto tiempo?
5	¿Existe control de acceso en los puertos?	X		10		
6	¿La solicitud y autorización de accesos a la base de datos se hace por escrito?		X	10		
7	¿Las características de longitud, composición (que permita letras mayúsculas y minúsculas, números y caracteres especiales), encriptado, etc. son adecuadas para que estos no sean fácilmente deducidos?		X	10		
8	¿Prevén que las contraseñas no sean difundidas en forma inadvertida, ni desplegados durante el proceso de acceso a la red o impresos en alguna salida?		X	10		
9	¿Prevén que las contraseñas sean almacenadas en archivos encriptados?		X	10		
10	¿Contemplan políticas de cambio frecuente de éstos. Por ej. Usar una fecha de expiración asociada a las contraseñas o limitar su uso a un número determinado de accesos para obligar su cambio?		X	10		
11	¿Prevén la eliminación de las claves de acceso de aquellos individuos que cesan su relación de trabajo con la empresa?		X	10		
12	¿Prevén la desconexión automática cuando transcurren algunos minutos de haber realizado el último acceso al sistema (última instrucción tecleada)?		X	10		
13	¿Prevén la suspensión del código de acceso, o la deshabilitación del sistema en caso que haya varios intentos de acceso fallidos durante el mismo día?		X	10		
14	¿Existe suficiente espacio físico para almacenar completa y correctamente los datos?	X		10		
15	¿Existe algún reciento cerrado (habitación, despacho, local) donde se encuentran situados todos los servidores?		X	10		¿Se controla el acceso?

16	¿Existe alguna alarma contra intrusos interconectada con la policía?		X	10		
17	¿Existe un documento de política de seguridad de la información accesible para los empleados donde puedan realizar consultas sobre ella?		X	10		
18	¿Esta política se revisa periódicamente para asegurarse que no ha variado nada y que se recoge todo lo necesario?		X	10		
19	¿Los empleados conocen las consecuencias de las violaciones de la política de seguridad?		X	10		
20	¿Existe un tiempo forzoso de espera antes de permitir un nuevo intento de conexión?		X	10		
21	¿Existe desconexión automática de la base de datos tras un tiempo prudencial de inactividad?		X	10		
22	¿El acceso a la base de datos se realiza mediante una conexión segura?		X	10		
TOTALES						
PONDERACION TOTAL (PT)				220		
CALIFICACIÓN TOTAL (CT)						

GRACIAS...

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL

AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

ÁREA: **ASPECTOS LÓGICOS DE LAS BASES DE DATOS**

DIRIGIDO: **FECHA DE APLICACIÓN:**

FUNCIÓN:

	#	PREGUNTA	CUMPLIMIENTO				
			0%	25%	50%	75%	100%
DATOS	1	¿La redundancia de la base de datos está controlada?				X	
	2	¿La base de datos está convenientemente documentada?			X		
	3	¿La base de datos posee valor informativo?				X	
ADMINISTRADOR DE LAS BASES DE DATOS	4	¿El administrador tiene formación adecuada para el desarrollo de sus funciones?			X		
	5	¿Tiene experiencia?				X	
	6	¿Existen políticas y procedimientos de seguridad para la base de datos?			X		
	7	¿El personal que utiliza la base de datos ha sido capacitado?			X		
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	8	¿El administrador interactúa y mantiene comunicación fluida con usuarios, directivos, analistas, programadores, suministradores y personal de administración?				X	
	9	¿Se ha involucrado en la capacitación a los usuarios?				X	
	10	¿Ha establecido estándares para asegurar que la base de datos mantiene la seguridad e integridad de los datos?			X		
	11	¿Ha realizado una descripción conceptual y lógica de la base de datos?			X		
			0%	25%	50%	75%	100%
CALIDAD	12	¿La institución tiene política de calidad?			X		
	13	¿Se cumple con las políticas de seguridad?			X		
	14	¿Conoce la ley de acceso a los datos?			X		
			0 – 6 MESES	6 -12 MESES	12- 18 MESES	18 – 24 MESES	MÁS DE 24 MESES
	15	¿Con que frecuencia se realizan auditorías?	X				
			0%	25%	50%	75%	100%
ASPECTOS LÓGICOS	16	¿Se ha formado a los empleados en la correcta utilización de los programas antivirus y firewall?			X		
	17	¿Los datos están disponibles para los usuarios autorizados?				X	
	18	¿Los datos son validados antes de ser introducidos en la Base de datos?			X		
	19	¿El acceso a la base de datos se realiza mediante una conexión segura?				X	
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	20	¿Se limita o controla de alguna manera el número de intentos fallidos de conexión?			X		

SEGURIDAD Y PROTECCIÓN DE LOS DATOS	21	¿Cuándo se recoge información personal, el usuario es informado de la existencia de un fichero o almacén que contiene esa información y los derechos que tiene sobre ellos?				X	
	22	¿La persona que tiene almacenados sus datos en un fichero o tabla de la base de datos puede consultarlos y acceder a ellos?				X	
	23	¿Se garantiza la seguridad de la información personal?				X	
	24	¿Se puede garantizar la seguridad de los datos personales almacenados en la base de datos?				X	
	25	¿Los datos sólo se dan a conocer si es para fines educativos?					X
	26	¿La persona que cede sus datos puede verlos, rectificarlos en caso de ser erróneos o haber cambiado o puede eliminarlos si así lo desea?		X			
	27	¿Se han tenido en cuenta los posibles cambios tecnológicos?				X	
	28	¿En las políticas se ha recogido la prevención y detección de virus, así como otro software malicioso?				X	
	29	¿Los usuarios y empleados realmente respetan las políticas de seguridad que se recogen en los manuales?			X		
			MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
	30	¿Existe seguridad de acceso al recinto, ya sea mediante guardias de seguridad, tarjetas de control, seguridad biométrica, etc.?	X				
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	31	¿El acceso físico a despachos, equipos, etc., se encuentra realmente bien controlado?		X			
	32	¿Se adoptan medidas de seguridad en el departamento de sistemas de información?		X			
	33	¿Existe una persona responsable de la seguridad?		X			
	34	¿Se controla el trabajo fuera de horario?	X				
PROTECCIÓN DE SOFTWARE MALICIOSO	35	¿Se controla la descarga de software no autorizado?					
	36	¿Existe antivirus instalado, en uso y actualizado en todos los puestos donde esté instalada la base de datos (servidor, clientes)?					X
	37	¿Se realizan revisiones periódicas del software instalado en los sistemas?					X
	38	¿Se investiga formalmente la presencia de ficheros no aprobados o de la modificación de ficheros no autorizados?					X
	39	¿Se controla el acceso a los servicios en redes internas y externas?					X
	40	¿Se realiza un "escaneo" previo de todo fichero adjunto en un correo electrónico a través de un programa antivirus antes de descargarlo?					X

Nº	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existen políticas, normas y procedimientos para la implementación y administración de bases de datos?		X	10		
2	¿Existe una persona responsable en la administración de bases de datos?	X		10		
3	¿Existen log de registros de acceso?		X	10		
4	¿Se realizan respaldos periódicos de la información?	X		10		¿Cada cuánto tiempo?
5	¿Existe control de acceso en los puertos?	X		10		
6	¿La solicitud y autorización de accesos a la base de datos se hace por escrito?	X		10		
7	¿Las características de longitud, composición (que permita letras mayúsculas y minúsculas, números y caracteres especiales), encriptado, etc. son adecuadas para que estos no sean fácilmente deducidos?	X		10		
8	¿Prevén que las contraseñas no sean difundidas en forma inadvertida, ni desplegados durante el proceso de acceso a la red o impresos en alguna salida?		X	10		
9	¿Prevén que las contraseñas sean almacenadas en archivos encriptados?		X	10		
10	¿Contemplan políticas de cambio frecuente de éstos. Por ej. Usar una fecha de expiración asociada a las contraseñas o limitar su uso a un número determinado de accesos para obligar su cambio?	X		10		
11	¿Prevén la eliminación de las claves de acceso de aquellos individuos que cesan su relación de trabajo con la empresa?		X	10		
12	¿Prevén la desconexión automática cuando transcurren algunos minutos de haber realizado el último acceso al sistema (última instrucción tecleada)?		X	10		
13	¿Prevén la suspensión del código de acceso, o la deshabilitación del sistema en caso que haya varios intentos de acceso fallidos durante el mismo día?		X	10		
14	¿Existe suficiente espacio físico para almacenar completa y correctamente los datos?		X	10		
15	¿Existe algún reciento cerrado (habitación, despacho, local) donde se encuentran situados todos los servidores?	X		10		¿Se controla el acceso?

16	¿Existe alguna alarma contra intrusos interconectada con la policía?		X	10		
17	¿Existe un documento de política de seguridad de la información accesible para los empleados donde puedan realizar consultas sobre ella?		X	10		
18	¿Esta política se revisa periódicamente para asegurarse que no ha variado nada y que se recoge todo lo necesario?		X	10		
19	¿Los empleados conocen las consecuencias de las violaciones de la política de seguridad?	X		10		
20	¿Existe un tiempo forzoso de espera antes de permitir un nuevo intento de conexión?		X	10		
21	¿Existe desconexión automática de la base de datos tras un tiempo prudencial de inactividad?		X	10		
22	¿El acceso a la base de datos se realiza mediante una conexión segura?	X		10		
TOTALES						
PONDERACION TOTAL (PT)				**220**		
CALIFICACIÓN TOTAL (CT)						

GRACIAS...

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL

AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

ASPECTOS LÓGICOS DE LAS BASES DE DATOS

ÁREA: **FECHA DE APLICACIÓN:**

DIRIGIDO: **FUNCIÓN:**

	#	PREGUNTA	CUMPLIMIENTO				
			0%	25%	50%	75%	100%
DATOS	1	¿La redundancia de la base de datos está controlada?			X		
	2	¿La base de datos está convenientemente documentada?		X			
	3	¿La base de datos posee valor informativo?				X	
ADMINISTRADOR DE LAS BASES DE DATOS	4	¿El administrador tiene formación adecuada para el desarrollo de sus funciones?					X
	5	¿Tiene experiencia?					X
	6	¿Existen políticas y procedimientos de seguridad para la base de datos?					X
	7	¿El personal que utiliza la base de datos ha sido capacitado?					X
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	8	¿El administrador interactúa y mantiene comunicación fluida con usuarios, directivos, analistas, programadores, suministradores y personal de administración?					X
	9	¿Se ha involucrado en la capacitación a los usuarios?				X	
	10	¿Ha establecido estándares para asegurar que la base de datos mantiene la seguridad e integridad de los datos?			X		
	11	¿Ha realizado una descripción conceptual y lógica de la base de datos?	X				
			0%	25%	50%	75%	100%
CALIDAD	12	¿La institución tiene política de calidad?		X			
	13	¿Se cumple con las políticas de seguridad?				X	
	14	¿Conoce la ley de acceso a los datos?				X	
			0 – 6 MESES	6 -12 MESES	12- 18 MESES	18 – 24 MESES	MÁS DE 24 MESES
	15	¿Con que frecuencia se realizan auditorías?					X
			0%	25%	50%	75%	100%
ASPECTOS LÓGICOS	16	¿Se ha formado a los empleados en la correcta utilización de los programas antivirus y firewall?	X				
	17	¿Los datos están disponibles para los usuarios autorizados?				X	
	18	¿Los datos son validados antes de ser introducidos en la Base de datos?					X
	19	¿El acceso a la base de datos se realiza mediante una conexión segura?					X
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	20	¿Se limita o controla de alguna manera el número de intentos fallidos de conexión?		X			

SEGURIDAD Y PROTECCIÓN DE LOS DATOS	21	¿Cuándo se recoge información personal, el usuario es informado de la existencia de un fichero o almacén que contiene esa información y los derechos que tiene sobre ellos?	X				
	22	¿La persona que tiene almacenados sus datos en un fichero o tabla de la base de datos puede consultarlos y acceder a ellos?					X
	23	¿Se garantiza la seguridad de la información personal?					X
	24	¿Se puede garantizar la seguridad de los datos personales almacenados en la base de datos?					X
	25	¿Los datos sólo se dan a conocer si es para fines educativos?				X	
	26	¿La persona que cede sus datos puede verlos, rectificarlos en caso de ser erróneos o haber cambiado o puede eliminarlos si así lo desea?	X				
	27	¿Se han tenido en cuenta los posibles cambios tecnológicos?			X		
	28	¿En las políticas se ha recogido la prevención y detección de virus, así como otro software malicioso?			X		
	29	¿Los usuarios y empleados realmente respetan las políticas de seguridad que se recogen en los manuales?				X	
			MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
	30	¿Existe seguridad de acceso al recinto, ya sea mediante guardias de seguridad, tarjetas de control, seguridad biométrica, etc.?			X		
			NUNCA	POCAS VECES	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
	31	¿El acceso físico a despachos, equipos, etc., se encuentra realmente bien controlado?			X		
	32	¿Se adoptan medidas de seguridad en el departamento de sistemas de información?			X		
	33	¿Existe una persona responsable de la seguridad?			X		
	34	¿Se controla el trabajo fuera de horario?		X			
PROTECCIÓN DE SOFTWARE MALICIOSO	35	¿Se controla la descarga de software no autorizado?	X				
	36	¿Existe antivirus instalado, en uso y actualizado en todos los puestos donde esté instalada la base de datos (servidor, clientes)?		X			
	37	¿Se realizan revisiones periódicas del software instalado en los sistemas?			X		
	38	¿Se investiga formalmente la presencia de ficheros no aprobados o de la modificación de ficheros no autorizados?	X				
	39	¿Se controla el acceso a los servicios en redes internas y externas?			X		
	40	¿Se realiza un "escaneo" previo de todo fichero adjunto en un correo electrónico a través de un programa antivirus antes de descargarlo?		X			

Nº	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
		SI	NO	POND	CAL	
1	¿Existen políticas, normas y procedimientos para la implementación y administración de bases de datos?		X	10		
2	¿Existe una persona responsable en la administración de bases de datos?	X		10	9	
3	¿Existen log de registros de acceso?	X		10	8	
4	¿Se realizan respaldos periódicos de la información?	X		10	10	¿Cada cuánto tiempo? Diario
5	¿Existe control de acceso en los puertos?		X	10		
6	¿La solicitud y autorización de accesos a la base de datos se hace por escrito?		X	10		
7	¿Las características de longitud, composición (que permita letras mayúsculas y minúsculas, números y caracteres especiales), encriptado, etc. son adecuadas para que estos no sean fácilmente deducidos?	X		10	10	
8	¿Prevén que las contraseñas no sean difundidas en forma inadvertida, ni desplegados durante el proceso de acceso a la red o impresos en alguna salida?	X		10	8	
9	¿Prevén que las contraseñas sean almacenadas en archivos encriptados?	X		10	9	
10	¿Contemplan políticas de cambio frecuente de éstos. Por ej. Usar una fecha de expiración asociada a las contraseñas o limitar su uso a un número determinado de accesos para obligar su cambio?		X	10		
11	¿Prevén la eliminación de las claves de acceso de aquellos individuos que cesan su relación de trabajo con la empresa?	X		10	10	
12	¿Prevén la desconexión automática cuando transcurren algunos minutos de haber realizado el último acceso al sistema (última instrucción tecleada)?	X		10	10	
13	¿Prevén la suspensión del código de acceso, o la deshabilitación del sistema en caso que haya varios intentos de acceso fallidos durante el mismo día?	X		10	8	
14	¿Existe suficiente espacio físico para almacenar completa y correctamente los datos?	X		10	10	
15	¿Existe algún reciento cerrado (habitación, despacho, local) donde se encuentran situados todos los servidores?	X		10	10	¿Se controla el acceso? Si

16	¿Existe alguna alarma contra intrusos interconectada con la policía?		X	10		
17	¿Existe un documento de política de seguridad de la información accesible para los empleados donde puedan realizar consultas sobre ella?		X	10		
18	¿Esta política se revisa periódicamente para asegurarse que no ha variado nada y que se recoge todo lo necesario?		X	10		
19	¿Los empleados conocen las consecuencias de las violaciones de la política de seguridad?		X	10		
20	¿Existe un tiempo forzoso de espera antes de permitir un nuevo intento de conexión?		X	10		
21	¿Existe desconexión automática de la base de datos tras un tiempo prudencial de inactividad?	X		10	8	
22	¿El acceso a la base de datos se realiza mediante una conexión segura?	X		10	8	
TOTALES						
PONDERACION TOTAL (PT)				220		
CALIFICACIÓN TOTAL (CT)						

ANEXO 4
FORMATO DEL CUESTIONARIO BASADO EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

CARRERA DE INFORMÁTICA DE LA ESPAM MFL
TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL
AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

DEPARTAMENTO	**FECHA:**
DIRIGIDO:	**CARGO:**

Cuestionario basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) del acuerdo ministerial Nº 166 del 19 de septiembre de 2013, de la Secretaría Nacional de la Administración Pública

Nº		PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
			SI	**NO**	**POND**	**CAL**	
Confidencialidad	1	¿Existen acuerdos de confidencialidad y de no-divulgación de la información conforme lo establece la ley?			**10**		¿Ha sido aprobado?
	2	¿El personal de la institución conoce y ha firmado estos acuerdos de confidencialidad?			**10**		
	3	¿Existe un contrato de confidencialidad con las terceras partes (estudiantes, pasantes u otros)?			**10**		
Clasificación de la información	4	¿Existe una clasificación de la información como pública o confidencial?			**10**		
	5	¿Existe un catálogo de clasificación de la información, respecto a, su valor, requisitos legales, sensibilidad e importancia?			**10**		
	6	¿Existe un aislamiento de datos sensibles para las diferentes instancias o ambientes (desarrollo, pruebas y capacitación)?			**10**		
Privilegios de acceso	7	¿Existe gestión de privilegios mediante GRANT y REVOKE para todos los usuarios de la base de datos?			**10**		
	8	¿Se suspende el acceso a los usuarios en caso de vacaciones, comisiones, licencias, es decir permisos temporales?			**10**		
	9	¿Se proporciona acceso temporal a usuarios externos o terceros de acuerdo al tiempo de su permanencia según las actividades para las que fueron contratados?			**10**		¿Firmar un acuerdo de confidencialidad?
	10	Se eliminan los usuarios con sus respectivos privilegios luego de que se termine el contrato laboral			**10**		
Seguridad	11	¿Las solicitudes y autorización de acceso a la base de datos se hacen por escrito?			**10**		
	12	¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?			**10**		
	13	¿Está restringido el acceso al entorno de desarrollo?			**10**		
	14	¿Se llevan a cabo copias de seguridad del repositorio?			**10**		
	15	¿Las copias de seguridad se efectúan diariamente?			**10**		
	16	¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?			**10**		
	17	¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?			**10**		
	18	¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?			**10**		¿Se realiza de manera escrita?
	19	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?			**10**		
	20	¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?			**10**		

	21	¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?			**10**		
	22	¿Existe un control de las entradas y las salidas de la base de datos (A nivel datos)?			**10**		
	23	¿Se notifican las acciones realizadas a nivel de mantenimiento de hardware?			**10**		
	24	¿Se han formulado políticas respecto a seguridad, privacidad y protección ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?			**10**		
	25	¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?			**10**		
	26	¿Se solicita formalmente la realización de copias de las bases de datos para realizar alguna prueba			**10**		
	27	¿Se eliminan esas copias luego de haber concluido con las pruebas pertinentes?			**10**		
	28	¿Se destruyen los dispositivos que contienen información sensible utilizando técnicas que aseguren la no recuperación de la misma?			**10**		
	29	¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?			**10**		
	30	¿Existe un control de acceso para evitar el acceso de personal no autorizado?			**10**		
Software malicioso	31	¿Existe un listado de software autorizado, con el fin de evitar la proliferación de virus?			**10**		
	32	¿Se examinan el código fuente de cada programa, para evitar así que exista la fuga de información?			**10**		
	33	¿Existen medidas para evitar las descargar que puedan contener alguna inyección maliciosa?			**10**		
	34	¿Se instala o actualiza periódicamente el software contra códigos maliciosos?			**10**		
Uso del sistema	35	¿Se registran el acceso autorizados y no autorizados a los sistemas?			**10**		
	36	¿Se monitorean las operaciones privilegiadas?			**10**		
	37	¿Se revisan los cambios en la configuración y controles a la seguridad del sistema?			**10**		
	38	¿Se utiliza algún control que asegure la validez de los datos ingresados?			**10**		
	39	En caso de existir una pérdida de datos, ¿quién es el responsable?			**10**		
	40	¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación de un sistema?			**10**		
	41	¿Se tiene un sistema de registro de acciones propio, con fines de auditoría?			**10**		
	42	¿Los datos utilizados en el entorno de desarrollo, son reales?			**10**		
	43	¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?			**10**		
	44	¿Posee el diccionario de datos un diseño físico y lógico?			**10**		
	45	¿Los manuales o guías de ayuda a los usuarios son completos o entendibles?			**10**		

	46	¿Se han realizado suficientes pruebas con datos antes de la instalación de la base de datos para evitar problemas posteriores?			**10**		
	47	¿El sistema de ayuda a los usuarios es completo y entendible por ellos?			**10**		
Sesión de usuarios y uso de contraseñas	48	¿Existe alguna regla para las contraseñas como longitud, composición (que permita letras entre mayúsculas y minúsculas, números y caracteres especiales)?			**10**		
	49	¿Se renuevan las claves de los usuarios de la Base de Datos?			**10**		
	50	¿Se obliga el cambio de la contraseña de forma automática?			**10**		
	51	¿Se evitan las contraseñas en blanco o que vienen por defecto en el sistema?			**10**		
	52	¿Se fuerza el cambio de contraseña luego de iniciar sesión por primera vez?			**10**		
	53	¿Se Cierra la sesión luego de un tiempo de inactividad?			**10**		
	54	¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?			**10**		
	55	¿Se registran la fecha hora y detalles de los eventos clave, como registro de inicio y cierre de sesión?			**10**		
	56	¿Se registran los intentos aceptados y rechazados de acceso al sistema?			**10**		
	57	¿Se revisan periódicamente los derechos de acceso de los usuarios?			**10**		
	58	¿Se realizan depuraciones de los accesos de usuarios en un tiempo determina, en caso de existir cambios estructurales en la institución?			**10**		
Especificaciones de las bases de datos	59	¿Hay suficiente espacio físico para almacenar completa y correctamente los datos?			**10**		
	60	¿El tamaño de las bases de datos es la correcta para el almacenamiento de datos e índices?			**10**		
	61	¿El motor de Base de Datos soporta herramientas de auditoria?			**10**		
TOTALES							
PONDERACION TOTAL (PT)					**610**		
CALIFICACIÓN TOTAL (CT)							

ANEXO 5
CUESTIONARIO BASADO EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

TRABAJO I **DE INFORMÁTICA DE LA ESPAM MFL**
N DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL
AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

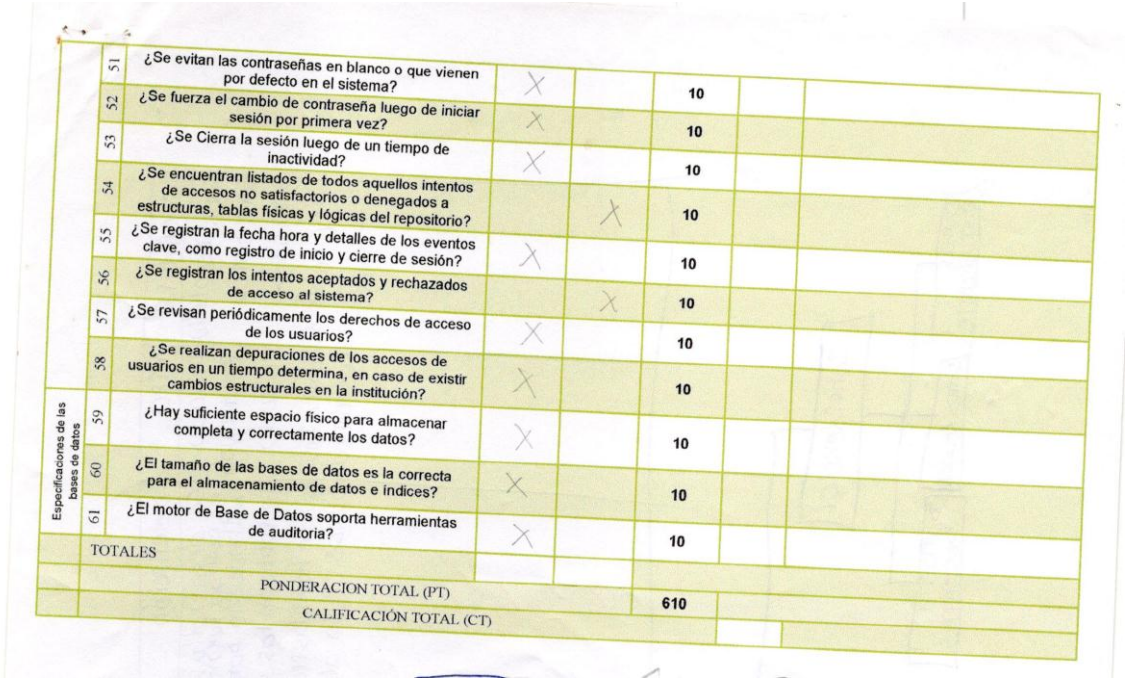
DEPARTAMENTO: Unidad de Producción de Software **FECHA:**

DIRIGIDO: Ing. Harold Buenaventura **CARGO:**

Cuestionario basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) del acuerdo ministerial Nº 166 del 19 de septiembre de 2013, de la Secretaría Nacional de la Administración Pública

	Nº	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
			SI	NO	POND	CAL	
Confidencialidad	1	¿Existen acuerdos de confidencialidad y de no-divulgación de la información conforme lo establece la ley?		X	10		¿Ha sido aprobado?
	2	¿El personal de la institución conoce y ha firmado estos acuerdos de confidencialidad?		X	10		
	3	¿Existe un contrato de confidencialidad con las terceras partes (estudiantes, pasantes u otros)?		X	10		Solo con pasantes
Clasificación de la información	4	¿Existe una clasificación de la información como pública o confidencial?	X		10		plantilla
	5	¿Existe un catálogo de clasificación de la información, respecto a, su valor, requisitos legales, sensibilidad e importancia?		X	10		
	6	¿Existe un aislamiento de datos sensibles para las diferentes instancias o ambientes (desarrollo, pruebas y capacitación)?	X		10		Caracteristicas (tablas).
Privilegios de acceso	7	¿Existe gestión de privilegios mediante GRANT y REVOKE para todos los usuarios de la base de datos?	X		10		
	8	¿Se suspende el acceso a los usuarios en caso de vacaciones, comisiones, licencias, es decir permisos temporales?		X	10		
	9	¿Se proporciona acceso temporal a usuarios externos o terceros de acuerdo al tiempo de su permanencia según las actividades para las que fueron contratados?	X		10		¿Firmar un acuerdo de confidencialidad?
	10	Se eliminan los usuarios con sus respectivos privilegios luego de que se termine el contrato laboral	X		10		
Seguridad	11	¿Las solicitudes y autorización de acceso a la base de datos se hacen por escrito?	X		10		secretaria Gral.
	12	¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?	X		10		
	13	¿Está restringido el acceso al entorno de desarrollo?	X		10		
	14	¿Se llevan a cabo copias de seguridad del repositorio?	X		10		
	15	¿Las copias de seguridad se efectúan diariamente?	X				
	16	¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	X		10		
	17	¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	X		10		
	18	¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	X		10		¿Se realiza de manera escrita?
	19	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?	X		10		
	20	¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?		X	10		
	21	¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?			10		Se hace
	22	¿Existe un control de las entradas y las salidas de la base de datos (A nivel datos)?			10		
	23	¿Se notifican las acciones realizadas a nivel de mantenimiento de hardware?			10		

	24	¿Se han formulado políticas respecto a seguridad, privacidad y protección ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?		X	10		
	25	¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?		X	10		
	26	¿Se solicita formalmente la realización de copias de las bases de datos para realizar alguna prueba	X		10		
	27	¿Se eliminan esas copias luego de haber concluido con las pruebas pertinentes?		X	10		
	28	¿Se destruyen los dispositivos que contienen información sensible utilizando técnicas que aseguren la no recuperación de la misma?		X	10		
	29	¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?		X	10		
	30	¿Existe un control de acceso para evitar el acceso de personal no autorizado?			10		
Software malicioso	31	¿Existe un listado de software autorizado, con el fin de evitar la proliferación de virus?		X	10		NO TIENE LIC
	32	¿Se examinan el código fuente de cada programa, para evitar así que exista la fuga de información?	X		10		
	33	¿Existen medidas para evitar las descargar que puedan contener alguna inyección maliciosa?	X		10		
	34	¿Se instala o actualiza periódicamente el software contra códigos maliciosos?		X	10		
Uso del sistema	35	¿Se registran el acceso autorizados y no autorizados a los sistemas?		X	10		
	36	¿Se monitorean las operaciones privilegiadas?	X		10		
	37	¿Se revisan los cambios en la configuración y controles a la seguridad del sistema?	X		10		
	38	¿Se utiliza algún control que asegure la validez de los datos ingresados?	X		10		
	39	En caso de existir una pérdida de datos, ¿quién es el responsable?	X		10		El JEFE
	40	¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación de un sistema?		X	10		
	41	¿Se tiene un sistema de registro de acciones propio, con fines de auditoría?		X	10		
	42	¿Los datos utilizados en el entorno de desarrollo, son reales?	X		10		
	43	¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?	X		10		
	44	¿Posee el diccionario de datos un diseño físico y lógico?		X	10		Lógico
	45	¿Los manuales o guías de ayuda a los usuarios son completos o entendibles?	X		10		
	46	¿Se han realizado suficientes pruebas con datos antes de la instalación de la base de datos para evitar problemas posteriores?	X		10		
	47	¿El sistema de ayuda a los usuarios es completo y entendible por ellos?	X		10		
Sesión de usuarios y uso de contraseñas	48	¿Existe alguna regla para las contraseñas como longitud, composición (que permita letras entre mayúsculas y minúsculas, números y caracteres especiales)?	X		10		
	49	¿Se renuevan las claves de los usuarios de la Base de Datos?	X		10		Cada semestre
	50	¿Se obliga el cambio de la contraseña de forma automática?		X	10		



	51	¿Se evitan las contraseñas en blanco o que vienen por defecto en el sistema?	X		10		
	52	¿Se fuerza el cambio de contraseña luego de iniciar sesión por primera vez?	X		10		
	53	¿Se Cierra la sesión luego de un tiempo de inactividad?	X		10		
	54	¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?		X	10		
	55	¿Se registran la fecha hora y detalles de los eventos clave, como registro de inicio y cierre de sesión?	X		10		
	56	¿Se registran los intentos aceptados y rechazados de acceso al sistema?		X	10		
	57	¿Se revisan periódicamente los derechos de acceso de los usuarios?	X		10		
	58	¿Se realizan depuraciones de los accesos de usuarios en un tiempo determina, en caso de existir cambios estructurales en la institución?	X		10		
Especificaciones de las bases de datos	59	¿Hay suficiente espacio físico para almacenar completa y correctamente los datos?	X		10		
	60	¿El tamaño de las bases de datos es la correcta para el almacenamiento de datos e índices?	X		10		
	61	¿El motor de Base de Datos soporta herramientas de auditoria?	X		10		
	TOTALES						
	PONDERACION TOTAL (PT)				610		
	CALIFICACIÓN TOTAL (CT)						

CARRERA DE INFORMÁTICA DE LA ESPAM MFL

TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL

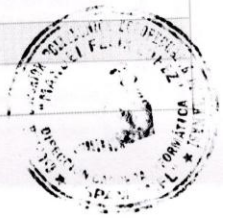
AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

DEPARTAMENTO | **FECHA:**

DIRIGIDO: | **CARGO:**

Cuestionario basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) del acuerdo ministerial Nº 166 del 19 de septiembre de 2013, de la Secretaría Nacional de la Administración Pública

	Nº	PREGUNTAS	RESPUESTA SI	RESPUESTA NO	CUMPLIMIENTO POND	CUMPLIMIENTO CAL	OBSERVACIONES
Confidencialidad	1	¿Existen acuerdos de confidencialidad y de no-divulgación de la información conforme lo establece la ley?		X	10		¿Ha sido aprobado?
	2	¿El personal de la institución conoce y ha firmado estos acuerdos de confidencialidad?		X	10		
	3	¿Existe un contrato de confidencialidad con las terceras partes (estudiantes, pasantes u otros)?		X	10		
Clasificación de la información	4	¿Existe una clasificación de la información como pública o confidencial?		X	10		
	5	¿Existe un catálogo de clasificación de la información, respecto a, su valor, requisitos legales, sensibilidad e importancia?		X	10		
	6	¿Existe un aislamiento de datos sensibles para las diferentes instancias o ambientes (desarrollo, pruebas y capacitación)?		X	10		
Privilegios de acceso	7	¿Existe gestión de privilegios mediante GRANT y REVOKE para todos los usuarios de la base de datos?	X		10		
	8	¿Se suspende el acceso a los usuarios en caso de vacaciones, comisiones, licencias, es decir permisos temporales?		X	10		
	9	¿Se proporciona acceso temporal a usuarios externos o terceros de acuerdo al tiempo de su permanencia según las actividades para las que fueron contratados?	X		10		¿Firmar un acuerdo de confidencialidad?
	10	Se eliminan los usuarios con sus respectivos privilegios luego de que se termine el contrato laboral		X	10		
Seguridad	11	¿Las solicitudes y autorización de acceso a la base de datos se hacen por escrito?		X	10		
	12	¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?		X	10		
	13	¿Está restringido el acceso al entorno de desarrollo?		X	10		
	14	¿Se llevan a cabo copias de seguridad del repositorio?	X		10		
	15	¿Las copias de seguridad se efectúan diariamente?		X	10		
	16	¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?		X	10		
	17	¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?		X	10		
	18	¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	X		10		¿Se realiza de manera escrita?
	19	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?	X		10		
	20	¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?		X	10		
	21	¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?	X		10		
	22	¿Existe un control de las entradas y las salidas de la base de datos (A nivel datos)?		X	10		
	23	¿Se notifican las acciones realizadas a nivel de mantenimiento de hardware?		X	10		



	24	¿Se han formulado políticas respecto a seguridad, privacidad y protección ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?		X	10		
	25	¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?		X	10		
	26	¿Se solicita formalmente la realización de copias de las bases de datos para realizar alguna prueba		X	10		
	27	¿Se eliminan esas copias luego de haber concluido con las pruebas pertinentes?		X	10		
	28	¿Se destruyen los dispositivos que contienen información sensible utilizando técnicas que aseguren la no recuperación de la misma?		X	10		
	29	¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?		X	10		
	30	¿Existe un control de acceso para evitar el acceso de personal no autorizado?		X	10		
Software malicioso	31	¿Existe un listado de software autorizado, con el fin de evitar la proliferación de virus?		X	10		
	32	¿Se examinan el código fuente de cada programa, para evitar así que exista la fuga de información?		X	10		
	33	¿Existen medidas para evitar las descargar que puedan contener alguna inyección maliciosa?		X	10		
	34	¿Se instala o actualiza periódicamente el software contra códigos maliciosos?		X	10		
Uso del sistema	35	¿Se registran el acceso autorizados y no autorizados a los sistemas?		X	10		
	36	¿Se monitorean las operaciones privilegiadas?		X	10		
	37	¿Se revisan los cambios en la configuración y controles a la seguridad del sistema?		X	10		
	38	¿Se utiliza algún control que asegure la validez de los datos ingresados?	X		10		
	39	En caso de existir una pérdida de datos, ¿quién es el responsable?			10		no hay responsables definidos / el desarrollador es el cond
	40	¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación de un sistema?		X	10		
	41	¿Se tiene un sistema de registro de acciones propio, con fines de auditoria?		X	10		
	42	¿Los datos utilizados en el entorno de desarrollo, son reales?	X		10		
	43	¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?		X	10		
	44	¿Posee el diccionario de datos un diseño fisico y lógico?		X	10		
	45	¿Los manuales o guías de ayuda a los usuarios son completos o entendibles?		X	10		
	46	¿Se han realizado suficientes pruebas con datos antes de la instalación de la base de datos para evitar problemas posteriores?		X	10		
	47	¿El sistema de ayuda a los usuarios es completo y entendible por ellos?		X	10		
Sesión de usuarios y uso de contraseñas	48	¿Existe alguna regla para las contraseñas como longitud, composición (que permita letras entre mayúsculas y minúsculas, números y caracteres especiales)?		X	10		
	49	¿Se renuevan las claves de los usuarios de la Base de Datos?		X	10		
	50	¿Se obliga el cambio de la contraseña de forma automática?	X		10		

	51	¿Se evitan las contraseñas en blanco o que vienen por defecto en el sistema?		X	10		
	52	¿Se fuerza el cambio de contraseña luego de iniciar sesión por primera vez?	X		10		
	53	¿Se Cierra la sesión luego de un tiempo de inactividad?		X	10		
	54	¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?		X	10		
	55	¿Se registran la fecha hora y detalles de los eventos clave, como registro de inicio y cierre de sesión?		X	10		
	56	¿Se registran los intentos aceptados y rechazados de acceso al sistema?		X	10		
	57	¿Se revisan periódicamente los derechos de acceso de los usuarios?		X	10		
	58	¿Se realizan depuraciones de los accesos de usuarios en un tiempo determina, en caso de existir cambios estructurales en la institución?		X	10		
Especificaciones de las bases de datos	59	¿Hay suficiente espacio físico para almacenar completa y correctamente los datos?	X		10		
	60	¿El tamaño de las bases de datos es la correcta para el almacenamiento de datos e índices?		X	10		
	61	¿El motor de Base de Datos soporta herramientas de auditoria?	X		10		
TOTALES							
PONDERACION TOTAL (PT)					610		
CALIFICACIÓN TOTAL (CT)							

GRACIAS...

DATOS DE CONTACTO

NOMBRES: Juan José Frank Montesdeoca, Mercedes Cecibel Romero Pino

CORREO ELECTRÓNICO: juanjfrank@hotmail.com -- mechyropi@gmail.com

INSTRUCCIÓN: Egresados de Ingeniería en Informática – ESPAM MFL.

DATOS DE LA INSTITUCIÓN

NOMBRES: 1

CORREO ELECTRÓNICO:

TÍTULO:

CARGO QUE OCUPA: JEFE TIC

TIEMPO ES SU CARGO: 15 DÍAS

CARRERA DE INFORMÁTICA DE LA ESPAM MFL
TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL
AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

DEPARTAMENTO **FECHA:**

DIRIGIDO: **CARGO:**

Cuestionario basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) del acuerdo ministerial Nº 166 del 19 de septiembre de 2013, de la Secretaría Nacional de la Administración Pública

	Nº	PREGUNTAS	RESPUESTA		CUMPLIMIENTO		OBSERVACIONES
			SI	NO	POND	CAL	
Confidencialidad	1	¿Existen acuerdos de confidencialidad y de no-divulgación de la información conforme lo establece la ley?		X	10		¿Ha sido aprobado?
	2	¿El personal de la institución conoce y ha firmado estos acuerdos de confidencialidad?		X	10		
	3	¿Existe un contrato de confidencialidad con las terceras partes (estudiantes, pasantes u otros)?		X	10		
Clasificación de la información	4	¿Existe una clasificación de la información como pública o confidencial?	X		10		
	5	¿Existe un catálogo de clasificación de la información, respecto a, su valor, requisitos legales, sensibilidad e importancia?	X		10		
	6	¿Existe un aislamiento de datos sensibles para las diferentes instancias o ambientes (desarrollo, pruebas y capacitación)?		X	10		
Privilegios de acceso	7	¿Existe gestión de privilegios mediante GRANT y REVOKE para todos los usuarios de la base de datos?		X	10		
	8	¿Se suspende el acceso a los usuarios en caso de vacaciones, comisiones, licencias, es decir permisos temporales?	X		10		
	9	¿Se proporciona acceso temporal a usuarios externos o terceros de acuerdo al tiempo de su permanencia según las actividades para las que fueron contratados?	X		10		¿Firmar un acuerdo de confidencialidad?
	10	Se eliminan los usuarios con sus respectivos privilegios luego de que se termine el contrato laboral	X		10		
Seguridad	11	¿Las solicitudes y autorización de acceso a la base de datos se hacen por escrito?	X		10		
	12	¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?		X	10		
	13	¿Está restringido el acceso al entorno de desarrollo?	X		10		
	14	¿Se llevan a cabo copias de seguridad del repositorio?	X		10		
	15	¿Las copias de seguridad se efectúan diariamente?		X	10		
	16	¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	X		10		
	17	¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?		X	10		
	18	¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	X		10		¿Se realiza de manera escrita?
	19	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?	X		10		
	20	¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		10		
	21	¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?	X		10		
	22	¿Existe un control de las entradas y las salidas de la base de datos (A nivel datos)?		X	10		
	23	¿Se notifican las acciones realizadas a nivel de mantenimiento de hardware?	X		10		

	24	¿Se han formulado políticas respecto a seguridad, privacidad y protección ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?		X	10		
	25	¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?		X	10		
	26	¿Se solicita formalmente la realización de copias de las bases de datos para realizar alguna prueba	X		10		
	27	¿Se eliminan esas copias luego de haber concluido con las pruebas pertinentes?	X		10		
	28	¿Se destruyen los dispositivos que contienen información sensible utilizando técnicas que aseguren la no recuperación de la misma?		X	10		
	29	¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?	X		10		
	30	¿Existe un control de acceso para evitar el acceso de personal no autorizado?		X	10		
Software malicioso	31	¿Existe un listado de software autorizado, con el fin de evitar la proliferación de virus?		X	10		
	32	¿Se examinan el código fuente de cada programa, para evitar así que exista la fuga de información?		X	10		
	33	¿Existen medidas para evitar las descargar que puedan contener alguna inyección maliciosa?	X		10		
	34	¿Se instala o actualiza periódicamente el software contra códigos maliciosos?	X		10		
Uso del sistema	35	¿Se registran el acceso autorizados y no autorizados a los sistemas?	X		10		
	36	¿Se monitorean las operaciones privilegiadas?	X		10		
	37	¿Se revisan los cambios en la configuración y controles a la seguridad del sistema?		X	10		
	38	¿Se utiliza algún control que asegure la validez de los datos ingresados?	X		10		
	39	En caso de existir una pérdida de datos, ¿quién es el responsable?	X		10		
	40	¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación de un sistema?	X		10		
	41	¿Se tiene un sistema de registro de acciones propio, con fines de auditoría?		X	10		
	42	¿Los datos utilizados en el entorno de desarrollo, son reales?		X	10		
	43	¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?		X	10		
	44	¿Posee el diccionario de datos un diseño físico y lógico?		X	10		
	45	¿Los manuales o guías de ayuda a los usuarios son completos o entendibles?		X	10		
	46	¿Se han realizado suficientes pruebas con datos antes de la instalación de la base de datos para evitar problemas posteriores?		X	10		
	47	¿El sistema de ayuda a los usuarios es completo y entendible por ellos?	X		10		
Sesión de usuarios y uso de contraseñas	48	¿Existe alguna regla para las contraseñas como longitud, composición (que permita letras entre mayúsculas y minúsculas, números y caracteres especiales)?		X	10		
	49	¿Se renuevan las claves de los usuarios de la Base de Datos?	X		10		
	50	¿Se obliga el cambio de la contraseña de forma automática?	X		10		

	51	¿Se evitan las contraseñas en blanco o que vienen por defecto en el sistema?	X		10		
	52	¿Se fuerza el cambio de contraseña luego de iniciar sesión por primera vez?	X		10		
	53	¿Se Cierra la sesión luego de un tiempo de inactividad?	X		10		
	54	¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?		X	10		
	55	¿Se registran la fecha hora y detalles de los eventos clave, como registro de inicio y cierre de sesión?		X	10		
	56	¿Se registran los intentos aceptados y rechazados de acceso al sistema?		X	10		
	57	¿Se revisan periódicamente los derechos de acceso de los usuarios?		X	10		
	58	¿Se realizan depuraciones de los accesos de usuarios en un tiempo determina, en caso de existir cambios estructurales en la institución?	X		10		
Especificaciones de las bases de datos	59	¿Hay suficiente espacio físico para almacenar completa y correctamente los datos?	X		10		
	60	¿El tamaño de las bases de datos es la correcta para el almacenamiento de datos e índices?	X		10		
	61	¿El motor de Base de Datos soporta herramientas de auditoria?	X		10		
TOTALES							
PONDERACION TOTAL (PT)					610		
CALIFICACIÓN TOTAL (CT)							

GRACIAS...

DATOS DE CONTACTO

NOMBRES: Juan José Frank Montesdeoca, Mercedes Cecibel Romero Pino

CORREO ELECTRÓNICO: juanjfrank@hotmail.com -- mechyropi@gmail.com

INSTRUCCIÓN: Egresados de Ingeniería en Informática – ESPAM MFL.

DATOS DE LA INSTITUCIÓN

NOMBRES:

CORREO ELECTRÓNICO:

TÍTULO: Magister en Sistemas de Información Gerencial

CARGO QUE OCUPA: Jefe del Dpt. de Sistemas Informáticos

TIEMPO ES SU CARGO: 2 meses.

CARRERA DE INFORMÁTICA DE LA ESPAM MFL
TRABAJO DE TESIS SOBRE LA EVALUACIÓN DE LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LA ESPAM MFL
AUTORES: FRANK MONTESDEOCA JUAN JOSÉ, ROMERO PINO MERCEDES CECIBEL

DEPARTAMENTO TIC'S **FECHA:** 26/ENE/2016

DIRIGIDO: [illegible] **CARGO:** DIRECTOR TIC's

Cuestionario basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) del acuerdo ministerial Nº 166 del 19 de septiembre de 2013, de la Secretaria Nacional de la Administración Pública

	Nº	PREGUNTAS	RESPUESTA SI	RESPUESTA NO	CUMPLIMIENTO POND	CUMPLIMIENTO CAL	OBSERVACIONES
Confidencialidad	1	¿Existen acuerdos de confidencialidad y de no-divulgación de la información conforme lo establece la ley?	X		10	10	¿Ha sido aprobado? Si
	2	¿El personal de la institución conoce y ha firmado estos acuerdos de confidencialidad?	X		10	8	
	3	¿Existe un contrato de confidencialidad con las terceras partes (estudiantes, pasantes u otros)?	X		10	9	
Clasificación de la información	4	¿Existe una clasificación de la información como pública o confidencial?	X		10	10	
	5	¿Existe un catálogo de clasificación de la información, respecto a, su valor, requisitos legales, sensibilidad e importancia?	X		10	9	
	6	¿Existe un aislamiento de datos sensibles para las diferentes instancias o ambientes (desarrollo, pruebas y capacitación)?	X		10	10	DESARROLLO / PRODUCCION
Privilegios de acceso	7	¿Existe gestión de privilegios mediante GRANT y REVOKE para todos los usuarios de la base de datos?	X		10	8	
	8	¿Se suspende el acceso a los usuarios en caso de vacaciones, comisiones, licencias, es decir permisos temporales?		X	10	10	CIERTOS CASOS.
	9	¿Se proporciona acceso temporal a usuarios externos o terceros de acuerdo al tiempo de su permanencia según las actividades para las que fueron contratados?	X		10	10	¿Firmar un acuerdo de confidencialidad? SI NO TIENEN SANCIONES.
	10	Se eliminan los usuarios con sus respectivos privilegios luego de que se termine el contrato laboral		X	10	10	CAMBIA DE ESTADO INACTIVO
Seguridad	11	¿Las solicitudes y autorización de acceso a la base de datos se hacen por escrito?	X		10	9	SOLO PERSONAL AUTORIZADO
	12	¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?	X		10	10	
	13	¿Está restringido el acceso al entorno de desarrollo?	X		10	9	POR TAREAS.
	14	¿Se llevan a cabo copias de seguridad del repositorio?	X		10	10	
	15	¿Las copias de seguridad se efectúan diariamente?	X		10	10	Y EN SERVER EXTERNOS
	16	¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	X		10	10	PERIODICAMENTE
	17	¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	X		10	9	
	18	¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	X		10	10	¿Se realiza de manera escrita? Si
	19	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?	X		10	10	
	20	¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		10	10	
	21	¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?	X		10	10	
	22	¿Existe un control de las entradas y las salidas de la base de datos (A nivel datos)?	X		10	9	AUDITORIAS
	23	¿Se notifican las acciones realizadas a nivel de mantenimiento de hardware?	X		10	9	

	24	¿Se han formulado políticas respecto a seguridad, privacidad y protección ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?	X		10	9	
	25	¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?	X		10	9	
	26	¿Se solicita formalmente la realización de copias de las bases de datos para realizar alguna prueba	X		10	10	
	27	¿Se eliminan esas copias luego de haber concluido con las pruebas pertinentes?		X	10	10	HISTÓRICOS
	28	¿Se destruyen los dispositivos que contienen información sensible utilizando técnicas que aseguren la no recuperación de la misma?		X	10	9	SEGURIDAD.
	29	¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?	X		10	9	.
	30	¿Existe un control de acceso para evitar el acceso de personal no autorizado?	X		10	9	
Software malicioso	31	¿Existe un listado de software autorizado, con el fin de evitar la proliferación de virus?	X		10	9	
	32	¿Se examinan el código fuente de cada programa, para evitar así que exista la fuga de información?	X		10	9	
	33	¿Existen medidas para evitar las descargar que puedan contener alguna inyección maliciosa?	X		10	9	
	34	¿Se instala o actualiza periódicamente el software contra códigos maliciosos?	X		10	9	
Uso del sistema	35	¿Se registran el acceso autorizados y no autorizados a los sistemas?	X		10	9	
	36	¿Se monitorean las operaciones privilegiadas?	X		10	9	
	37	¿Se revisan los cambios en la configuración y controles a la seguridad del sistema?	X		10	9	
	38	¿Se utiliza algún control que asegure la validez de los datos ingresados?	X		10	9	
	39	En caso de existir una pérdida de datos, ¿quién es el responsable?	X		10	9	ADMINISTRADOR BD.
	40	¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación de un sistema?	X		10	8	
	41	¿Se tiene un sistema de registro de acciones propio, con fines de auditoría?	X		10	10	
	42	¿Los datos utilizados en el entorno de desarrollo, son reales?	X		10	10	MENOS USUARIOS/CLAVES
	43	¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?	X		10	10	
	44	¿Posee el diccionario de datos un diseño físico y lógico?	X		10	8	
	45	¿Los manuales o guías de ayuda a los usuarios son completos o entendibles?	X		10	10	
	46	¿Se han realizado suficientes pruebas con datos antes de la instalación de la base de datos para evitar problemas posteriores?	X		10	9	
	47	¿El sistema de ayuda a los usuarios es completo y entendible por ellos?	X		10	9	
Sesión de usuarios y uso de contraseñas	48	¿Existe alguna regla para las contraseñas como longitud, composición (que permita letras entre mayúsculas y minúsculas, números y caracteres especiales)?	X		10	10	TIENEN TIEMPO DE VALIDEZ
	49	¿Se renuevan las claves de los usuarios de la Base de Datos?	X		10	10	PERIODICAMENTE
	50	¿Se obliga el cambio de la contraseña de forma automática?	X		10	10	

	51	¿Se evitan las contraseñas en blanco o que vienen por defecto en el sistema?			10		
	52	¿Se fuerza el cambio de contraseña luego de iniciar sesión por primera vez?			10		
	53	¿Se Cierra la sesión luego de un tiempo de inactividad?			10		
	54	¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?			10		
	55	¿Se registran la fecha hora y detalles de los eventos clave, como registro de inicio y cierre de sesión?			10		
	56	¿Se registran los intentos aceptados y rechazados de acceso al sistema?			10		
	57	¿Se revisan periódicamente los derechos de acceso de los usuarios?			10		
	58	¿Se realizan depuraciones de los accesos de usuarios en un tiempo determina, en caso de existir cambios estructurales en la institución?			10		
Especificaciones de las bases de datos	59	¿Hay suficiente espacio físico para almacenar completa y correctamente los datos?			10		
	60	¿El tamaño de las bases de datos es la correcta para el almacenamiento de datos e índices?			10		
	61	¿El motor de Base de Datos soporta herramientas de auditoria?			10		
TOTALES							
PONDERACION TOTAL (PT)					610		
CALIFICACIÓN TOTAL (CT)							

GRACIAS...

DATOS DE CONTACTO

NOMBRES: Juan José Frank Montesdeoca, Mercedes Cecibel Romero Pino

CORREO ELECTRÓNICO: juanjfrank@hotmail.com -- mechyropi@gmail.com

INSTRUCCIÓN: Egresados de Ingeniería en Informática – ESPAM MFL.

DATOS DE LA INSTITUCIÓN

NOMBRES:

CORREO ELECTRÓNICO:

TÍTULO:

CARGO QUE OCUPA:

TIEMPO ES SU CARGO:

ANEXO 6
INFORME FINAL

INFORME FINAL

AUDITORÍA A LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ

CONTENIDO

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

AUDITORÍA A LAS BASES DE DATOS DE GESTIÓN ACADÉMICA DE LAS IES PÚBLICAS DE MANABÍ

FECHA DE INFORME: 18 / 02 / 2016

MOTIVO DE LA AUDITORÍA

La auditoría a las bases de datos de gestión académica a las instituciones de educación públicas de Manabí, se ejecutó como propuesta de tesis, la misma que los autores plantearon, la misma que contó con la autorización de las autoridades de las diferentes instituciones involucradas, y previa autorización del tribunal de tesis.

OBJETIVO

- ✓ Identificar las bases de datos de los sistemas de gestión académica de las instituciones a auditar.
- ✓ Examinar la estructura y seguridad de los datos en los procesos de los sistemas de información.
- ✓ Analizar los riesgos que conllevan la falta de cumplimiento de normas y estándares en las bases de datos
- ✓ Elaborar informe de control de los sistemas de información considerando los hallazgos encontrados.

ALCANCE DEL EXAMEN

El proceso de Auditoría a las bases de datos de gestión académica se realizará en las instituciones de educación superior públicas de Manabí, en el área de tecnología de la información y comunicación TIC´s

FECHA DE INICIO DE LA AUDITORÍA: 5 / 01 /2016

FECHA DE FINALIZACIÓN DE LA AUDITORÍA: 16 / 02 / 2016

HERRAMIENTAS UTILIZADAS

- Metodología OCTAVE
- Coeficiente de concordancia de Kendall

PROCEDIMIENTOS A APLICAR

Se utilizará la adaptación de la ISO / IEC 27000 correspondiente a la gestión de seguridad de la información que la secretaría nacional de la administración pública denominó Norma Técnica Ecuatoriana NTE INEN – ISO / IEC 27000 / 27002 y 27005 que tratan sobre la seguridad de la información; así como también las Normas de control Interno emitidas por la Contraloría General del Estado.

CAPÍTULO II

RESULTADO DE LA EVALUACIÓN A LAS BASES DE DATOS

La evaluación de las bases de datos efectuada a las instituciones de educación superior públicas de Manabí, dio como resultados varias debilidades, los resultados se muestran a continuación.

El cuestionario en que se evaluaron aspectos generales sobre las bases de datos permitió conocer el estado en el que se encontraban las bases de datos como se muestra en el **gráfico 1** que la institución que tiene un mayor dominio sobre ellas es IES 4 con un porcentaje de 88%, la IES 2 alcanzó tan solo un 15% de puntuación, esto podría sustentarse en que dicha institución cuenta con un departamento de TIC´s relativamente nuevo con apenas meses de creación, lo que indica que recién se están acoplando a lo dictaminado por la ley, por otro lado tanto la IES 1 como la IES 3 alcanzaron porcentajes que van desde los 56% y 60% respectivamente, cabe recalcar que dicho cuestionario constaba de 40 preguntas.

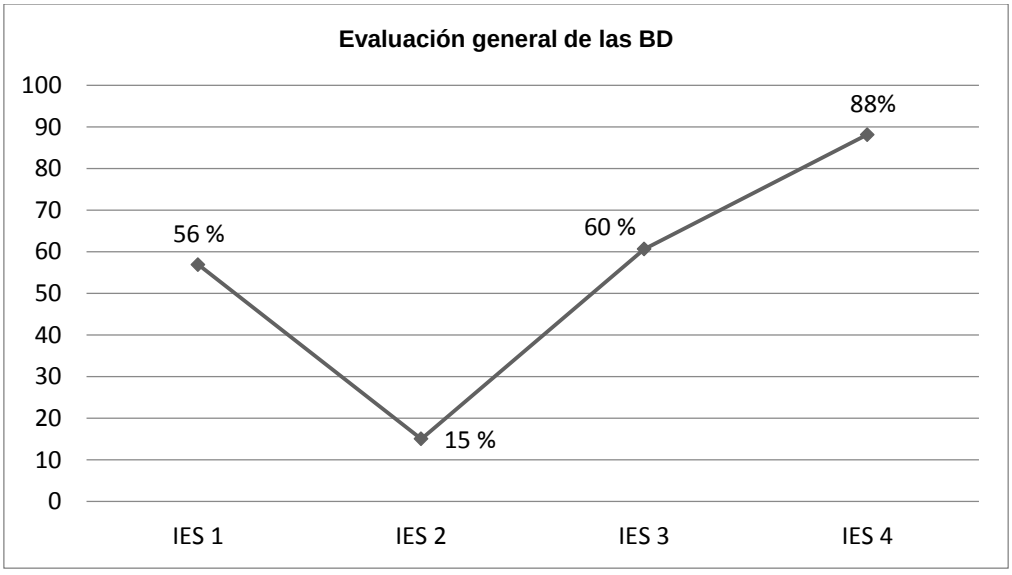


Gráfico 1. Comparativa general del cuestionario de evaluación de las BD

El segundo cuestionario aplicado dio a conocer el cumplimiento que las instituciones dan a la norma técnica Ecuatoriana INEN-ISO/IEC 27000, en el **Gráfico 2** se muestran los resultados obtenidos, los mismos que revelan un

bajo cumplimiento por parte de la IES 2, se aprecia también, que ninguna de las instituciones presenta un nivel mayor al 50% en el cumplimiento de la norma, la que mejor desenseño logra alcanza un 46%.

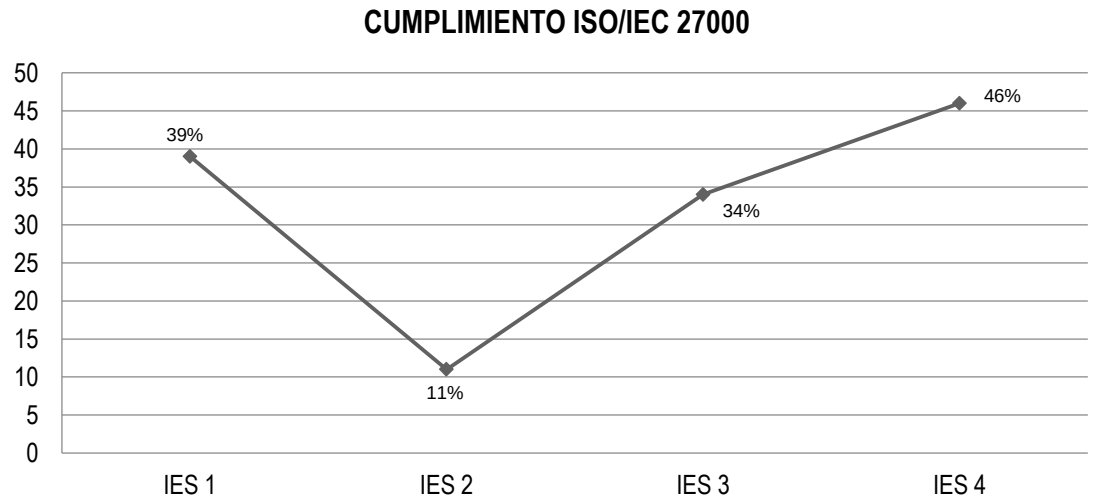


Gráfico 2. Cumplimiento de la norma INEN-ISO/IEC 27000

Luego de conocidos estos resultados se procede a la presentación de los niveles de riesgo y confianza que se obtuvieron de las evaluaciones aplicadas

MATRIZ DE RIESGO-CONFIANZA							
IES 1		**IES 2**		**IES 3**		**IES 4**	
RIESGO	**CONFIANZA**	**RIESGO**	**CONFIANZA**	**RIESGO**	**CONFIANZA**	**RIESGO**	**CONFIANZA**
42,30%	*57,70%*	*83,93%*	*16,07%*	*47,70%*	*52,30%*	*23,11%*	*76,89%*

Cuadro 1 .Matriz general porcentual de nivel Riesgo – Confianza

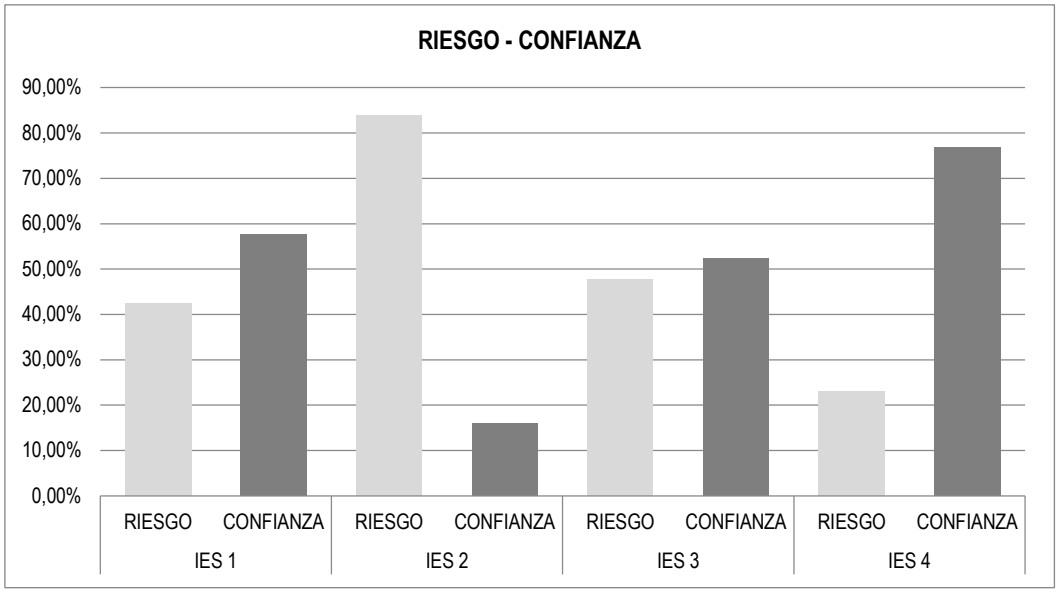


Gráfico 3. Nivel porcentual de Riesgo – Confianza de las IES públicas de Manabí

El **gráfico 3.** Muestra los niveles de riesgo - confianza en el cumplimiento de las normas y estándares que las instituciones de educación superior públicas de Manabí dan a estos, con lo que se determinó que la IES 1 cuenta un nivel de riesgo y confianza moderado 42,30% y 57,70% respectivamente, en el caso de la IES 2 su riesgo es alto con un 83,93% y su confianza es baja con un 16,07% lo que indica que es la institución con el nivel más alto riesgo, esto se debe a que su departamento de tecnología cuenta con pocos meses de creación y al poco acato que le dan a la norma, por otro lado la IES 3 se encuentra en un nivel moderado de confianza 52,30% y riesgo 47,70%, con respecto a la institución 4 es la mejor puntuada, con el nivel más alto de confianza correspondiente al 76,89% es la entidad que mayor acatamiento realiza sobre la ley, cuenta además con un nivel de riesgo de 23,11% lo que corresponde a un nivel bajo.

EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS

De conformidad a la evaluación del control interno aplicada a las cuatro universidades involucradas se obtuvieron los siguientes resultados.

UNIVERSIDAD	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO
IES 1	57,70 %	MODERADO	MODERADO
IES 2	16,07 %	BAJO	ALTO
IES 3	52,30 %	MODERADO	MODERADO
IES 4	76,89 %	ALTO	BAJO

Cuadro 2. Matriz de resultados de nivel de Riesgo - Confianza

COEFICIENTE DE CONCORDANCIA DE KENDALL

Item K	Preguntas	IES 1	IES 2	IES 3	IES 4	∑aij	A	A^2
1	Existen acuerdos de confidencialidad	1	0	2	4	7	-2	4
2	Se realizan con frecuencia copias de seguridad	4	1	2	4	11	2	4
3	Existen políticas de seguridad	2	1	2	4	8	-1	1
4	Se obliga al cambio de contraseñas frecuentemente	3	2	3	2	10	1	1
						36		**10**

Cuadro 3. Concordancia de preguntas similares de los cuestionarios aplicados

HALLAR EL VALOR DE A	HALLAR EL VALOR DE T
$\boldsymbol{A = \sum aij - T}$ $\boldsymbol{A = 7 - 9}$ $\boldsymbol{A = -2}$ **El mismo proceso se aplica para el resto de preguntas**	$T = \frac{\sum aij}{K}$ $T = \frac{36}{4}$ $T = 9$
REEMPLAZO DE LA FÓRMULA	
$\boldsymbol{w = \frac{12\sum A^2}{n^2\ 4(k^2 - 1)}}$ $\boldsymbol{w = \frac{12(10)}{4^2\ 4(4^2 - 1)}}$ $\boldsymbol{w = 0,13}$	

Cuadro 4. Reemplazo de fórmulas para el Coeficiente de Concordancia de Kendall

Con el dato obtenido en el **Cuadro 4.,** se concluye que el nivel de concordancia de las respuestas obtenidas equivale a 0,13.

CAPÍTULO III

HALLAZGOS Y RECOMENDACIONES

SITUACIÓN ACTUAL	CONCLUSIÓN	RECOMENDACIONES
Conforme a la evaluación realizada, se conoció que las instituciones cuentan con políticas y normas internas de cada institución, de las cuales no se tiene detalle alguno.	No existen normas que obliguen al cumplimiento de la ley y aseguren la efectividad de la seguridad de las bases de datos.	Adopción de la norma técnica ecuatoriana NTE INEN- ISO/IEC 27000, para que exista un mejor control y aseguramiento de la información almacenada en sus bases de datos.
En la mayoría de las instituciones en el mejor de los casos solo cuentan con el ambiente de producción, pero ninguna cuenta con el de desarrollo, pruebas y producción.	Se concluye que los datos académicos no son 100% seguros y confiables ya que se carecerían de credibilidad al ser usados en todos los ambientes tanto de desarrollo, prueba y producción.	Se recomienda dar cumplimiento a la norma estableciendo los diferentes ambientes propuestos, realizar además una copia de las bases de datos para que tanto desarrollo, prueba y producción trabajen bajo los mismos datos pero sin verse afectados los datos reales.
En la mayoría de los casos una vez que se da por terminada la relación laboral, no son eliminados sus usuarios y privilegios de manera inmediata.	Existen usuarios activos del personal que no forman parte de la institución, esto se pudo constatar por uno de los cuestionarios aplicados que hace referencia a este apartado.	Eliminar de manera inmediata los usuarios o cambiar su estado de activo a pasivo, para que los sistemas reconozcan éstos y revoque su acceso automáticamente, evitando la fuga de información o la pérdida de la misma.
Las instituciones no cuentan con acuerdos de confidencialidad, por ende sus empleados no conocen ni han firmado acuerdo alguno.	No existe un conocimiento por ende no se aplican acuerdos de confidencialidad en la mayoría de las instituciones de educación superior, lo que compromete sus datos y exentan a los responsables de su mala utilización.	Elaboración de acuerdos de confidencialidad, que den a conocer a cada persona involucrada con el manejo de datos sensibles, que la mala utilización o divulgación de los mismos estará sujeto a sanciones y amonestaciones, que podrán ir desde económicas hasta despidos, dependiendo del caso.
No existe control con el cambio periódico de las contraseñas de acceso de los sistemas, indistintamente del que fuere.	No existe regulación alguna que controle y obligue el cambio de contraseñas en un periodo de tiempo determinado, existiendo ocasiones donde los usuarios nunca han realizado cambio alguno.	Cumplir la normativa y obligar a todas las personas involucradas al cambio inmediato de sus contraseñas, además dar a conocer de la política que obliga al cambio de las mismas en periodos de tiempo no mayor a 6 meses.