UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO
MAESTRÍA EN GESTIÓN DE BASES DE DATOS

TEMA:

"LA ADMINISTRACIÓN DE LOS SGBD'S DE LOS SISTEMAS DE INFORMACIÓN Y SU INCIDENCIA EN EL CONTROL DE LAS SEGURIDADES DE LAS BASES DE DATOS DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSIÓN LATACUNGA"

Trabajo de Titulación

Previo a la obtención del Grado Académico de Magíster en Gestión de Bases de Datos

Autor: Ing. Milton Patricio Navas Moya
Director: Ing. Edwin Hernando Buenaño Valencia, Mg.

Ambato – Ecuador

2014

Al Consejo de Posgrado de la Universidad Técnica de Ambato.

El Tribunal de Defensa del trabajo de titulación presidido por el Ingeniero José Vicente Morales Lozada Magíster, Presidente del Tribunal e integrado por los señores Ingeniero Galo Mauricio López Sevilla Magíster, Ingeniero Jaime Bolívar Ruíz Banda Magíster, Ingeniero Kléver Renato Urvina Barrionuevo Magíster, Miembros del Tribunal de Defensa, designados por el Consejo Académico de Posgrado de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar la defensa oral del trabajo de titulación con el tema: "LA ADMINISTRACIÓN DE LOS SGBD'S DE LOS SISTEMAS DE INFORMACIÓN Y SU INCIDENCIA EN EL CONTROL DE LAS SEGURIDADES DE LAS BASES DE DATOS DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSIÓN LATACUNGA", elaborado y presentado por el señor Ingeniero Milton Patricio Navas Moya, para optar por el Grado Académico de Magíster en Gestión de Bases de Datos.

Una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de titulación para uso y custodia en las bibliotecas de la UTA.

Ing. José Vicente Morales Lozada, Mg.

Presidente del Tribunal de Defensa

Ing. Galo Mauricio López Sevilla, Mg.

Miembro del Tribunal

Ing. Jaime Bolívar Ruíz Banda, Mg.

Miembro del Tribunal

Ing. Kléver Renato Urvina Barrionuevo, Mg.

Miembro del Tribunal

AUTORIA DE LA INVESTIGACION

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de titulación con el tema: "LA ADMINISTRACIÓN DE LOS SGBD'S DE LOS SISTEMAS DE INFORMACIÓN Y SU INCIDENCIA EN EL CONTROL DE LAS SEGURIDADES DE LAS BASES DE DATOS DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATACUNGA.", le corresponde exclusivamente a: Ingeniero Milton Patricio Navas Moya, Autos bajo la dirección de Ingeniero Edwin Hernando Buenaño Valencia Magíster, Director del trabajo de titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ing. Milton Patricio Navas Moya.	Ing. Edwin Hernando Buenaño Valencia, Mg.
Autor	Director

DERECHOS DEL AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este trabajo de titulación como un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos de mi trabajo de titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

_____

Ing. Milton Patricio Navas Moya.

C.C. 0502029275

DEDICATORIA

Quiero dedicar este trabajo a la compañera de mi vida Tatiana eje principal de nuestro hogar, a mis hijas Camila y Mia razón de mi existencia y superación que éste paso alcanzado sirva para que ustedes busquen siempre la superación, a mi Padre mi mejor amigo que lindo es saber que siempre está ahí, a mi lado buscando siempre mi bienestar, que si me caigo me ayuda a levantar, para ustedes este logro con todo mi amor.

AGRADECIMIENTO

Agradezco a Dios por la salud y porque me da la oportunidad de crecer día con día, a mi esposa e hijas quienes sacrificaron muchas horas de compartir con su esposo y padre y más durante este trabajo de investigación en la cual tuvieron que quedarse solas porque yo alcance este escalón en mi vida profesional, mil disculpas por esos momentos pero que estén seguras que siempre en ausencia están presentes en mis pensamientos y en mi corazón.

A mis padres y hermanos que siempre me han enseñado que todo se consigue con sacrificio, y que en los buenos momentos están conmigo pero en los malos con más razón por eso siempre les estaré agradecido.

Finalmente agradecer a la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, volver a sus aulas me lleno nuevamente de mucho orgullo y más que encontré a mis amigos de siempre los cuales me guiaron durante este proceso muchas gracias de corazón mis entrañables amigos Clay Aldas y Hernando Buenaño, espero algún rato poder servirles de igual o mejor manera que ustedes lo hicieron.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN GESTIÓN DE BASES DE DATOS

TEMA: "LA ADMINISTRACIÓN DE LOS SGBD'S DE LOS SISTEMAS DE INFORMACIÓN Y SU INCIDENCIA EN EL CONTROL DE LAS SEGURIDADES DE LAS BASES DE DATOS DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATACUNGA."

Autor: Ing. Milton Patricio Navas Moya
Director: Ing. Edwin Hernando Buenaño Valencia, Mg.
Fecha: 28 Julio del 2014

RESUMEN EJECUTIVO

La investigación sobre la administración de los sistemas gestores de bases de datos y como estos incide sobre la seguridad de la información en las bases de datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, tiene como objetivo el generar una Guía Técnica, que ayude a la Administración de las seguridades en los sistemas de información aplicando el modelo COBIT 5, y que éste sea una herramienta para fortalecer las seguridades, mejorar los procesos dentro de la Unidad de Tecnologías de la Información y las Comunicaciones, haciéndolos seguros, y que se pueda garantizar la confidencialidad, integridad y disponibilidad de los datos.

El motivo que incentivo a desarrollar está guía técnica es el de poder tomar medidas de protección, que respondan a la Seguridad de la Información, es el propio interés de la Universidad o personas que administran los datos evitar que exista pérdida o modificación de los datos que puedan causar daños institucionales.

Descriptores: Aplicativos, Bases de Datos, Gestión Unificada de Amenazas, Modelo COBIT, Seguridades, Sistema Académico, Sistema Financiero, Sistemas Gestores de Bases de Datos, Unidad de Tecnologías de la Información y las Comunicaciones, Universidad de las Fuerzas Armadas ESPE, extensión Latacunga.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN GESTIÓN DE BASES DE DATOS

THEME: "DBMS MANAGEMENT OF INFORMATION SYSTEMS AND ITS IMPACT ON THE CONTROL OF SECURITIES OF DATABASE OF THE OF THE ARMED FORCES ESPE LATACUNGA UNIVERSITY"

Author: Ing. Milton Patricio Navas Moya

Directed By : Ing. Edwin Hernando Buenaño Valencia, Mg.

Date: July, 28 / 2014

EXECUTIVE SUMMARY

Research on the management of database management systems and data as these impact on the security of the information in the databases of the Armed Forces ESPE Latacunga University, aims to generate a Guide Technical, to help the Administration of securities in information systems using the COBIT 5 model, and it is a tool to strengthen the assurances, improve processes within the information Technologies and Communications Unit, making them safe, and that it can ensure confidentiality, integrity and availability of data.

The reason is that incentive to develop technical guide is the ability to take protective measures that respond to information security, is the interest of the University or persons who manage the data exists prevent loss or modification of institutional data can cause damage.

Keywords: Application, Databases, Unified Threat Management, COBIT Model, Securities, Academic System, Financial System, Management Systems Databases, Information Technology and Communication Unit, Armed Forces University ESPE Latacunga.

INTRODUCCIÓN

El constante cambio de tecnología ha hecho que cada vez las empresas e instituciones busquen más y nuevas formas de solucionar algunos inconvenientes de tipo tecnológico, es por estos motivos que se plantea como tema de investigación: La Administración de los SGBD's de los sistemas de Información y su incidencia en el control de las seguridades de las Bases de Datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga; la importancia del tema radica en hacer un análisis de su funcionamiento y la forma cómo están administradas, cómo está su construcción, el rendimiento, el número de transacciones que ejecutan y la forma como apoyan a la toma de decisiones de la Universidad.

La investigación sintetiza un análisis a las bases de datos de la Universidad, tomando su forma y diseño, su estructura y como fue planificada, para soportar la información que en este centro de estudios superior se genera. El realizar una auditoría a cualquier actividad siempre es motivo de análisis tanto crítico como beneficioso para una empresa o institución ya que se dejará ver posibles errores o cosas que se las realizan correctamente, todo esto con la finalidad de corregir lo incorrecto o potenciar los procesos que se los lleve adecuadamente.

La estructura de la investigación se encuentra de la siguiente manera:

El CAPITULO I. EL PROBLEMA DE INVESTIGACION, que contiene: El tema de la investigación, Planteamiento del Problema, la Contextualización, Análisis crítico, Prognosis, Formulación del problema, Interrogantes de la investigación, Delimitación del objeto de investigación, Justificación, Objetivos General y Objetivos Específicos.

El Capítulo II llamado MARCO TEÓRICO, contiene Antecedentes investigativos, Fundamentación filosófica, Fundamentación tecnológica,

Fundamentación legal, Categorías fundamentales, Hipótesis, y Señalamiento de variables de la Hipótesis.

El Capítulo III denominado METODOLOGÍA, se conforma con Modalidades básicas de la investigación, Niveles o tipos de investigación, Población y muestra, Operacionalización de variables, Plan de recolección de la información, métodos, técnicas y medios que han sido utilizados para obtener la información necesaria acerca de los problemas en la administración de las Bases de Datos de los Sistemas de Información.

El Capítulo IV ANALISIS E INTERPRETACION DE RESULTADOS: contiene el análisis e interpretación de resultados de la entrevista realizada al personal de la UTIC, también se presenta la demostración de la hipótesis basándose en cuadros estadísticos.

El Capítulo V: CONCLUSIONES Y RECOMENDACIONES, contiene las conclusiones y recomendaciones de la investigación del problema planteado.

El Capítulo VI: PROPUESTA, contiene. El resultado del desarrollo de la solución, que para este caso sería el protocolo de auditoría de las bases de datos de los Sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

CAPÍTULO I

EL PROBLEMA

1.1. Tema

La Administración de los SGBD's de los sistemas de Información y su incidencia en el control de las seguridades de las Bases de Datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga

1.2. Planteamiento del problema

La falta de una correcta administración y la falta de escalabilidad de los SGBD de los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga podrían incidir en las seguridades de las Bases de datos.

1.2.1. Contextualización

El presente trabajo resulta del interés entre la interacción de las Tecnologías de la Información y las Comunicaciones con un sector estratégico de la sociedad como es la Educación y el interés que esta conjunción viene despertando en todo el mundo. El sostenido desarrollo tecnológico durante todo este tiempo y particularmente en el sector de la educación, ha impuesto que el control se tenga que perfeccionar, ya que la información ocupa un lugar importante, tanto por su valor como por el volumen que se manejan en la sociedad moderna, por lo que resulta importante organizarla de forma eficiente con el fin de manipularla con mayor facilidad.

Esas tecnologías se presentan cada vez más como una necesidad en el contexto de sociedad donde los rápidos cambios, el aumento de los conocimientos y las

demandas de una educación de alto nivel constantemente actualizada se convierten en una exigencia permanente.

La relación entre las TICs y la educación tiene dos vertientes: Por un lado, los ciudadanos se ven abocados a conocer y aprender sobre las TICs. Por otro, las TICs pueden aplicarse al proceso educativo.

Con los constantes cambios que ha venido experimentando la Universidad ecuatoriana, ha hecho que muchos sistemas de Información sufran algunas modificaciones mismas que han ocasionado que en la institución colapsen o que rindan por debajo de lo esperado, en muchas ocasiones las aplicaciones no tuvieron mecanismos de escalabilidad o de actualización adecuadas para todos esos cambios que ha planteado el organismo rector de la educación superior.

Los sistemas de información que se manejan en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga son aplicaciones distribuidas, con distintos usuarios y donde toda esta información se encuentra centralizada en el servidor de aplicaciones en el Centro de Procesamiento de Datos (CPD) de la Unidad de Tecnologías de la Información y las Comunicaciones (UTIC), partiendo de este punto se requiere auditar la utilización de las bases de datos en sistemas de información con el fin de optimizar todos los procesos dentro de la Universidad.

La utilización de sistemas de gestión de bases de datos (SGBD) permite resolver estos problemas, brindando al investigador comodidad y eficiencia en el tratamiento de los datos.(Castilla Mesa 1991)

Por lo tanto el proyecto va a ser un aporte partiendo de una selección adecuada de métodos existentes los cuales ayudaran en la toma de decisiones por parte de los administradores de las Bases de datos de los sistemas de información, tratando de mitigar las causas en posibles efectos como lo muestra figura 1.1 del árbol de

problemas, el cual es un compendio de las causas y sus posibles efectos dentro del área de Desarrollo y Administración de aplicativos de la UTIC.

Figura 1.1. Árbol de Problemas. (Relación Causa - Efecto)(Navas P., 2014).

1.2.2. Análisis Crítico

El ineficiente control de las seguridades que tienen en la actualidad las bases de datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, están dadas debido a la creciente complejidad de los sistemas de información y que estos a su vez van acompañados por la deficiente administración de los SGDB de los sistemas de información, así como de un reducido número de personal en la gestión, además de que este personal no tiene la suficiente capacitación dentro de la administración y sobre la utilización de los distintos SGBD, los mismos que en muchos de los casos no son escalables y no cumplen con el rol preponderante que deben cumplir al momento de realizar una evaluación a la calidad de las Bases de Datos.

Todas estas causas han desembocado en consecuencias tales como que a medida que el tamaño de una Base de Datos crece, es mucho más eficiente almacenar varias

relaciones en un solo archivo y esto a su vez va causando información inconsistente, alteración y pérdida de información, todo esto desemboca en la generación de reportes con información no confiable, o inexactos que no son un aporte para las autoridades cuando se trata de una toma de decisión oportuna, aunque la mayoría de SGBD que en la Universidad se utilizan siguen una filosofía parecida y en el modo en que estas ideas son llevadas a la práctica pueden variar de unos a otros, sobre todo tipo y el número de registros que puedan almacenar de acuerdo al Sistema de información.

1.2.3. Prognosis

En caso de que siga existiendo el problema, con inconsistencia de la información en el sistema académico, falta de información en el sistema contable, o los reportes con datos no congruentes, el problema se va agudizar toda vez que las bases de datos van a seguir incrementando en número de registros, y que los requerimientos de parte de los usuarios van a aumentar buscando siempre mejorar los procesos que ayuden a la gestión de los recursos de la institución.

Se debe tomar en cuenta que todas estas aplicaciones están a su vez reglamentadas por estamentos externos a la Universidad como es el caso del Senescyt, o instituciones que regulan el sector administrativo económico público, por lo que se requiere la implementación de alternativas de seguridad con la finalidad de garantizar la información y que estos se vean reflejados tanto por los estamentos Universitarios como por los organismos de control de los recursos públicos como la Contraloría General del Estado.

Este crecimiento en el número de registros va ocasionar que los sistemas de información colapsen, que requieran de nuevas actualizaciones, de la realización de cambios en las estructuras de bases de datos para la consecución de objetivos planteados en las etapas preliminares de su desarrollo y que estos cambios sean

debidamente documentados con la finalidad de evitarse posibles contratiempos futuros al no tener información ordenada o incongruente.

1.2.4. Formulación del Problema

¿Incide la administración de los SGBD de los Sistemas de Información en el control de las seguridades de las Bases de Datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga?

1.2.5. Interrogantes de la Investigación

Para poder encontrar la solución a los problemas que se tienen en los DBMS de los sistemas de información de la UFA ESPE –L se plantea las siguientes directrices:

- ¿Qué problemas tienen en la actualidad los DBMS de los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga?

- ¿Cuáles son los controles de las seguridades en las bases de datos en la UFA-ESPE -L?

- ¿Existen alternativas de solución factibles al problema que se plantea?

1.2.6. Delimitación del Objeto de Investigación

Delimitación de Contenido

Campo: Gestión de Bases de Datos.

Área: Seguridad en Bases de Datos.

Aspecto: Seguridad de los Sistemas de Información de la UFA-ESPE-L

Delimitación Espacial

La investigación se desarrollará en las Universidad de las Fuerzas Armadas ESPE- Latacunga.

Delimitación Temporal

La investigación se lo efectuará en el período académico Mayo - Julio 2014

Unidad de Observación

- Director de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.
- Jefe de la Unidad de Tecnologías de la Información y las Comunicaciones

1.3.Justificación

La información es el bien más importante de toda institución, por lo que su seguridad debe ser la prioridad dentro de todo estudio, la administración de los SGBD que componen las bases de datos de los sistemas de información de la UFA-ESPE-L deben contar con controles relacionados para el acceso a las mismas, se debe demostrar la integridad de la información.

El interés de la Universidad es mitigar los riesgos asociados a la pérdida de datos y a la fuga de la información.

La importancia teórica práctica es que la información debe mantenerse confidencial y eso es responsabilidad de los administradores de las bases de datos

y de la Universidad en su conjunto, por esto los datos son convertidos en información en los SGBD en procesos académicos y no académicos que representan a la institución.

La novedad de la investigación se basa en la monitorización de las bases de datos, los procesos que permiten conocer quién o que las hizo, exactamente qué, cuándo, cómo y en la calidad de los SGBD que fueron utilizados para implementar las bases de datos considerando que no es inherente a la base de datos y que es difícilmente modificable por los usuarios, pudiendo ser analizada como la calidad de cualquier producto software utilizando normas de control como las ISO.

El impacto va estar en apoyar en el cumplimiento regulatorio de las seguridades, tratando de satisfacer los requerimientos de los usuarios y de los auditores de la información.

La Factibilidad del proyecto se va a partir de 3 premisas importantes como son:

Factibilidad Técnica: La Universidad de las Fuerzas Armadas ESPE extensión Latacunga, cuenta con los servidores dedicados a las Bases de datos y aplicaciones, todos los SGBD de ser el caso cuentan con el licenciamiento para cumplir con las actividades de almacenamiento, en cuanto a la investigación se cuenta con las facilidades de la información por parte del personal de gestión como por las autoridades universitarias.

Factibilidad Operativa: Basado en la experiencia del investigador y en los conocimientos adquiridos en Gestión de Bases de Datos, el apoyo de las personas que gestionan la información en la Universidad, la investigación se la puede realizar.

Factibilidad Económica: La Universidad de las Fuerzas Armadas ESPE extensión Latacunga, cuenta con el talento humano suficiente, con el material

necesario para la investigación, y el investigador aportará económicamente con lo que sea necesario para el desarrollo de la investigación.

1.4.Objetivos

1.4.1. Objetivo general

Determinar la incidencia de la Administración de los SGDB de los Sistemas de Información en el control de las seguridades de las Bases de Datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

1.4.2. Objetivos específicos

- Establecer la situación actual de los SGBDS en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

- Determinar las causas de los fallos y falta de seguridad en las bases de datos en los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

- Proponer una solución factible al problema en cuestión.

CAPITULO II

MARCO TEORICO

2.1.Antecedentes Investigativos

Una vez realizado una revisión de las tesis de las distintas Universidades que ofertan la carrera de Ingeniería en Sistemas, se encuentra que:

En la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, a nivel de posgrados existe una tesis denominada: "El análisis de riesgos informáticos y su incidencia en la seguridad e integridad de la Información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato", realizado por el Ing. Donald Eduardo Reyes Bedoya, que obtuvo como conclusión:

Los equipos y la información han sido víctimas de ataques que en mayor o menor medida han afectado a la información que manejan inclusive a la pérdida por robo de la misma, esto hace ver claramente que las medidas de seguridad con que se cuentan no están acordes a la necesidades y requerimientos poniendo en peligro la integridad y veracidad de la información. No se cuenta con capacitación en seguridades de los sistemas y además se desconoce las políticas de seguridad sobre los sistemas y equipos lo que da claramente la idea de una falta de una adecuada socialización y ejecución de políticas de seguridad.

En la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, a nivel de pregrado existe una tesis denominada: "Inyección SQL para detectar las vulnerabilidades de seguridad en las bases de datos SQL server 2005 en las farmacias Cruz Azul Vitalidad de la ciudad de

Ambato", realizado por David Israel Chicaiza Cazar. Donde obtuvo como conclusión principal:

La Solución al SQL Injection reside en una consistente y absoluta revisión y confrontación de todos los parámetros y cuestiones dirigidas a las Bases de Datos y la Programación/Diseño del sistema informático. Al ejecutar las consultas consulta en la base de datos, el código SQL inyectado se ejecutó logrando hacer un sinnúmero de cosas, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar código malicioso en el computador. No se puede implementar medidas de seguridad para la aplicación, puesto que no es posible tener acceso al código fuente del sistema, por tal motivo se vuelve necesario optar por mantener al sistema fuera del alcance de personas que tengan conocimiento del tema.

En la Facultad de Ingeniería en Electricidad y Computación de la Escuela Politécnica del Litoral, existe una tesis denominada "Base de Datos centralizada para Sistemas de Seguridad", realizado por Bruno Macías Velasco y Rolando Quijije Iduarte. Donde obtuvieron como conclusión principal la siguiente:

Estableciendo el alcance y elaborando una abstracción de la lógica de los Sistemas de Seguridades, hemos logrado obtener un diseño genérico de Base de Datos, capaz de soportar diferentes Sistemas de Seguridades.

2.2.Fundamentación Filosófica

En la actualidad no se atribuye a la filosofía un objeto propio de estudio. Este ejerce su actividad a través de las ciencias, que actúan directamente sobre la naturaleza en sentido amplio: desde el universo hasta el individuo pasando por la sociedad y la historia. Compartiendo con el criterio emitido por Jarro Janeth, "Constituye una actividad racional de reflexión sobre todos aquellos aspectos que se consideran fundamentales, en distintos ámbitos de la vida humana, que se desarrolla constituyendo sus propias reflexiones teóricas en los aspectos no

tratables científicamente o técnicamente, y sometiendo a crítica presupuestos, nociones fundamentales, creencias básicas, objetivos y métodos del trabajo científico o de la vida ordinaria" (Jarro, 2012)

Basado en esta realidad, para realizar la presente investigación, de debe ubicar en el paradigma filosófico Crítico propositivo porque la manera de investigar y de platear una la propuesta de solución al problema de investigación basado en la existencia de múltiples realidades socialmente construidas.

2.3.Fundamentación Legal

Este trabajo de investigación busca sustento legal en las siguientes leyes:

> *Art. 16.- Todas las personas, en forma individual o colectiva, tiene derecho a:*
> 2. *El acceso universal a las tecnologías de información y comunicación.*
>
> *Art. 18.- Todas las personas en forma individual o colectiva tienen derecho a:*
> *1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.*
> *2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondeos del Estado o realicen funciones públicas.*
> *No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negara la información.*

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones e incorporara a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, instituciones públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.
El Estado, a través del organismo competente, coordinará el sistema, establecerá los objetivos y políticas de conformidad con el Plan Nacional de Desarrollo, con la participación de los actores que lo conforman.

La Constitución de la República del Ecuador

Art 4. Literal c), que dice: Cuarto nivel o de posgrado destinado a la especialización científica o entrenamiento profesional avanzado. Corresponden a este nivel los títulos intermedios de posgrado de especialista y diploma superior y los grados de magíster y doctor.

Art 12 enciso b) manifiesta: "Promover la creación, desarrollo, transmisión y difusión de la ciencia, la técnica, la tecnología y la cultura".

Art. 32.- "Asignación de recursos para investigación, ciencia y tecnología e innovación.- Las instituciones del Sistema de Educación Superior podrán acceder adicional y preferentemente a los recursos públicos concursables de la pre asignación para investigación, ciencia, tecnología e innovación establecida en la Ley correspondiente".

La Republica del Ecuador y el Consejo de Educación Superior, emite las copias debidamente certificada del Estatuto de la Universidad de las Fuerzas Armadas (ESPE), aprobado mediante resolución RPC.SO.No. 248-2013, Adoptada en la Vigésima Cuarta sesión Ordinaria del Pleno del Consejo Superior, desarrollada el 26 de Junio del 2013.

Art. 1.- La Universidad de las Fuerzas Armadas "ESPE", es una institución de educación superior; con personería jurídica, de derecho público y sin fines de lucro; con autonomía académica, administrativa, financiera, orgánica y patrimonio propio. Como institución de educación superior de las Fuerzas Armadas es dependiente del Comando Conjunto de las Fuerzas Armadas en. Política institucional en el ámbito de educación superior, designación de autoridades ejecutivas; y asignación del personal militar; necesario para el funcionamiento de la Universidad, conforme al presente estatuto.

Ley Orgánica de Educación Superior (LOES)

Art 188. "La Unidad de tecnologías de la Información y Comunicación administra los recursos tecnológicos requeridos por la institución para el manejo de la información y mantener una adecuada comunicación, para lo cual ejecuta los procesos de gestión estratégica de la tecnología informática; de soporte técnico; de administración de redes y comunicaciones; de desarrollo, implantación y mantenimiento de aplicativos; y, de administración de software".

Art 189: "Es responsable de:

a. Realizar la gestión estratégica de la tecnología informática;

b. Dar soporte técnico en el ámbito de aplicación que corresponde;

c. Administrar las redes y las comunicaciones;

d. Desarrollar, implantar y mantener los aplicativos;

e. Administrar los aplicativos y bases de datos;

f. Proporcionar seguridad a la información de servidores; y,

g. Cumplir la normativa institucional y las resoluciones emitidas por los órganos competentes. "

Art. 190: "La Unidad de tecnologías de la Información y comunicación contara con:

a. Un director;

b. Personal administrativo: profesionales en tecnologías de información y comunicación; y,

c. *Personal administrativo de apoyo."*

Reglamento Interno de la Universidad de las Fuerzas Armadas ESPE

2.4.Categorías fundamentales

Red de Inclusiones Conceptuales

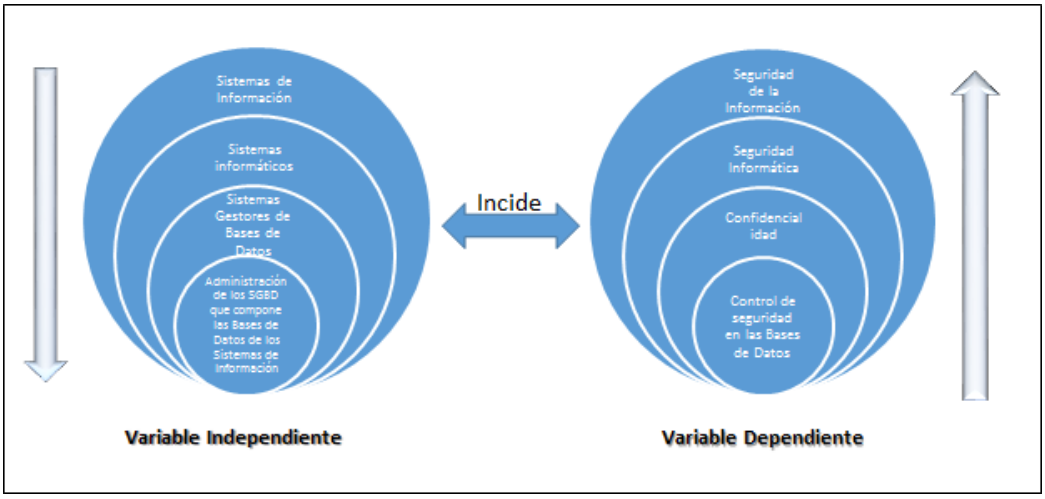


Figura 2.1.: Red de Inclusiones Conceptuales (Navas P., 2014)

Constelación de Ideas Variable Independiente

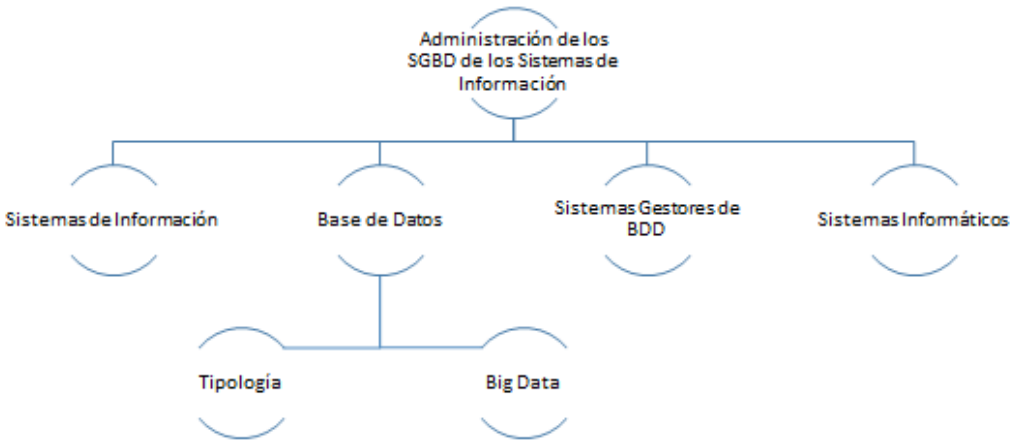


Figura 2.2.: Constelación de ideas variable Independiente (Navas P., 2014)

Constelación de Ideas Variable Dependiente

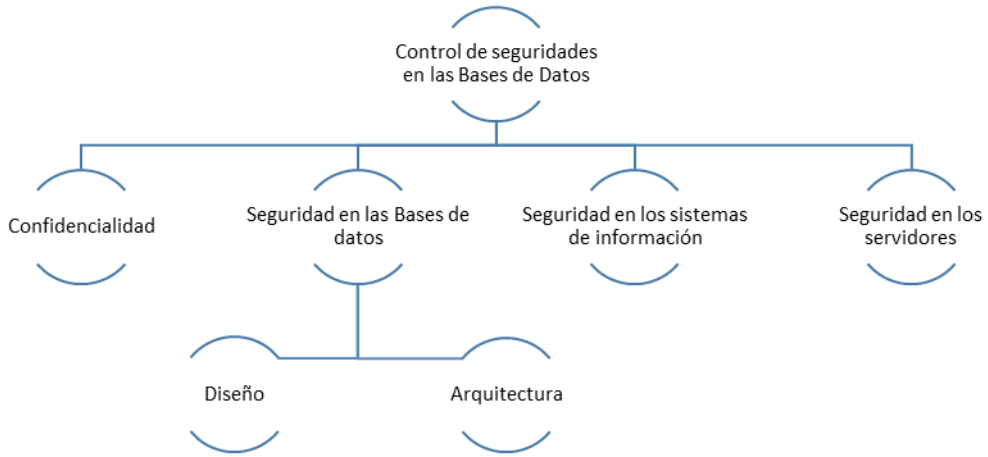


Figura 2.3.: Constelación de ideas Variable Dependiente (Navas P., 2014)

2.4.1. Categorías Fundamentales de las Variables Independientes

2.4.1.1. Bases de Datos

"Fondo común de información almacenada en una computadora para que cualquier persona o programa autorizado pueda acceder a ella, independientemente de su procedencia y del uso que haga". [1]

"Una Base de dato es un conjunto de datos almacenados sin redundancia innecesarias en un soporte informático y accesible simultáneamente por distintos usuarios y aplicaciones. Los datos deben de estar estructurados y almacenados de forma totalmente independiente de las aplicaciones que la utilizan [2]

Por lo tanto la Bases de datos puede ser considerada como un lugar donde almacenar una gran cantidad de información de forma organizada para que luego pueda ser consultada y utilizada de manera fácil. Entonces las bases de datos son sistemas formados por un conjunto de datos que están ubicados en discos que

permiten el acceso directo a ellos y un conjunto de programas que manipulen esa información.

Cada base de datos está compuesta de una o más tablas que guarde un conjunto de datos. Cada tabla tiene una o más columnas o filas. Las columnas guardan una parte de la información sobre los elementos que guardan en la tabla, las filas de las tablas son los registros que se generan en las empresas o instituciones.

Hay que tomar en cuenta que la independencia de la información es lógica y física, disponen de redundancia mínima, su acceso es concurrente y en muchos casos mantienen la integridad de los datos.

2.4.1.2.Sistemas Gestores de Bases de Datos

"Conjunto de elementos software con capacidad para definir, mantener y utilizar una base de datos". [3]

"Un sistema de gestión de bases de datos es un software o conjunto de programas que permite crear y mantener una bases de datos. El SGDB actúa como interfaz entre los programas de aplicación (Usuarios) y el sistema operativo. El objetivo principal de un SGDB es proporcionar un entorno a la hora de almacenar y recuperar la información de la base de datos". [4]

Los Sistemas de Gestión de bases de datos (SGDB) o inglés (DataBase Management System, DBMS), son un tipo de software específico y que como única función es la de servir de interfaz entre las bases de datos, el usuario y las aplicaciones que las utilizan. Se compone de un lenguaje de definición de datos, de manipulación de datos y un lenguaje de consulta. Además de que los SGDB ayudan en el control sobre la redundancia de los datos.

Mejora la integridad de los datos es decir que ayuda a la validez y consistencia de los datos almacenados, la integridad se expresa mediante restricciones o reglas que no pueden ser violadas, mejoran las seguridades de las bases de datos frente a usuarios no autorizados.

Mejora la productividad proporcionando muchas funciones estándar que el programador necesita escribir en un sistema de ficheros. El SGDB proporciona todas las rutinas de manejo de ficheros típicas de los programas de aplicación.

2.4.1.3.Sistemas Informáticos

"Un sistema informático está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos…) y con frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y el hardware)". [5]

Figura 2.4.: Sistemas Informáticos (Aguilera P. 2008).

. "Un sistema informático es un subsistema dentro del sistema de información, y está formado por todos los recursos necesarios para dar respuesta a un tratamiento automático de la información y aquellos otros que posibiliten la comunicación de la misma. En definitiva, por tecnologías de la información y las comunicaciones".[6]

2.4.1.4.Sistemas de Información

"Un sistema de Información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos". [7]

Figura 2.5.: Sistemas de Información (Aguilera P. 2008).

"Un sistema de información es un conjunto de recursos técnicos, humanos y económicos, interrelacionados dinámicamente, y organizados en torno al objetivo de satisfacer las necesidades de información de una organización empresarial para la gestión y la correcta adopción de decisiones". [8]

2.4.1.5. Big Data

"Big Data es un conjunto de datos que crece tan rápidamente que no pueden ser manipulados por las herramientas de gestión de bases de datos transaccionales, sin embargo el tamaño no es el único problema si nos enfrentamos a buscar una solución de almacenamiento también de captura, consulta, gestión y análisis de toda la información" [9]

"Big Data aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales. Big data no solo es

alguna cantidad en específico, ya que es usualmente utilizado cuando se habla en términos de grandes cantidades de datos.”

Big Data es un término que se utiliza por cuestiones de tamaño, además que es la oportunidad de hacer más grande a las empresas con una toma de decisiones más efectivas, además de que ayuda a las instituciones a tener mejores infraestructuras tecnológicas, ya que por el número de datos que se requiere almacenar y gestionar de mejor manera para la optimización económica, rápida y flexible.

Los Big Data se encargan de administrar grandes volúmenes de datos que se generan diariamente en las empresas o instituciones, la variedad de los datos ya que tiene la capacidad de combinar varía información en distintos formatos en las que se pueden presentar. La velocidad para el almacenamiento es muy importante ya que ayuda a reducir los tiempos de procesamiento y de reportes, la veracidad de la información está garantizada por la inteligencia de los datos, con la finalidad de obtener información verídica y útil que nos permita tomar decisiones.

2.4.2. Categorías Fundamentales de la Variable dependiente

2.4.2.1.Confidencialidad

“Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, estas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones”.

"Se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

De esta manera se dice que un documento es confidencial si y solo si puede ser sorprendido por la persona o entidad a quien va dirigida o este autorizada. En el caso de un mensaje esto evita que exista una intercepción de éste y que prueba ser leído por una persona, no autorizada".

La confidencialidad está en inmerso en términos de seguridad informática así como en la protección de la información, se podría decir que es una propiedad de la información que ayudan a garantizar el acceso sólo a las personas autorizadas.

Cuando se genera información que sea confidencial, los responsables deciden quiénes van a ser los que tienen derechos sobre estos datos, la información debe ser confidencial ya que incluye material que puede poner en riesgo la seguridad de una institución o una empresa, las precauciones deben ser mucho mayor, la confidencialidad de la información en bases de datos también debe protegerse, aunque no con medidas físicas, sino con mecanismos de cifrado y otras herramientas virtuales.

2.4.2.2.Seguridad de las Bases de Datos

Es la capacidad del Sistema para proteger los datos, servicios y recursos de los usuarios no autorizados, el fin de la seguridad es garantizar la protección o estar libre de todo peligro o daño y que en cierta manera es infalible. (Alva, 2009).

En la actualidad se conoce que lo más importante, son las seguridades de las base de datos, lo más importante en el proceso de aplicar soluciones que interactúen con información sensible. Todos confían en los sistemas de Administración de Bases de Datos (SGDB), para el almacenamiento y administración de la información de una empresa, si estas aplicaciones fallaran o se tornaran inseguras podrían causar

almacenar todos los datos que genere la institución. Para que esta actividad tenga la validez requerida se necesita que se tenga muchas consideraciones entre otras, la velocidad de acceso que es un proceso muy importante a la hora de ingresar los datos, otro de los factores muy importantes es el tamaño de la información que no pueda causar lentitud de los SGBD, el tipo de la información, la facilidad de accesibilidad de la información, la extracción y consulta de los datos.

Los principio básicos de un buen diseño de bases de datos es evitar la información duplicada, datos redundantes, porque malgastan el espacio y aumentan la probabilidad de producir errores e incoherencias. Se debe garantizar que la información ingresada sea correcta y sobre todo completa. Por lo tanto un buen diseño de bases de datos es el proceso más crítico de un sistema de información ya que dividir en tablas ayuda a reducir los datos redundantes y repetidos, proporcionando de esta manera el acceso a la información uniendo tablas mediante consultas y generando reportes que ayuden a tomar decisiones agiles, oportunas y que reflejen lo que se tiene en los sistemas de información.

2.4.2.3.Arquitectura

Según Gartner "se define como el diseño de los componentes lógicos y físicos de cómputo y las relaciones entre estos. La arquitectura define el hardware, software, métodos de acceso y protocolos usados a través del sistema. También se define como un marco de trabajo y un conjunto de lineamientos para construir un nuevo sistema".

La Arquitectura dentro de las bases de datos, es el diseño inteligente de las interfaces que ayuden a la interacción entre los datos y los usuarios de los sistemas, por lo tanto es un proceso interactivo, transversal que es parte fundamental dentro del diseño que apoyan a la consecución de los objetivos. La Arquitectura no es una

metodología de diseño ni un método, sino una técnica que puede ayudar a la producción de espacios de información.

Dentro de los campos que se toman en cuenta las arquitecturas deben cumplir con el procesamiento y dosificación de grandes cantidades de información que se producen a causa de la creación de nuevos sistemas de información que están siendo tomados en cuenta en páginas web y dispositivos móviles. El desarrollar y verificar procesos y diseños de la información con la finalidad de que los datos ingresados sean claros y precisos, la organización, estructuración la distribución y el diseño estructural se los sistemas de información pueden hacer que la lectura, recuperación, pueda ser agradable, eficaz y productivo.

2.5.Hipótesis

La administración de los SGBD de los sistemas de información incidiría en el control de las seguridades en las bases de datos en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

2.6.Señalamiento de variables e Hipótesis

Variable Independiente

La administración de los SGBD de los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

Variable Dependiente

El control de las seguridades en las bases de datos en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

CAPÍTULO III

METODOLOGÍA

3.1.Modalidad de Investigación.

En esta investigación se utilizó las siguientes formas de investigación: bibliográfica y de campo. La primera aportó con la recolección de datos científicos que se encuentran en libros y documentos publicados en Internet, mientras que es una investigación de campo porque permitió realizar la investigación sobre la administración de los SGDB de los sistemas de Información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga y su incidencia en el control de las seguridades de las Bases de Datos.

3.1.1. Investigación Documental- bibliográfica

La investigación es bibliográfica porque se realizará mediante la revisión de documentos oficiales, leyes y otros; mismos que permiten fundamentar la base legal y obtener información referente al tema correspondiente objeto de estudio y sobre la que se desarrollará la presente investigación.

3.1.2. Investigación de campo

La aplicación se lo realizará en la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, así como se obtendrá los criterios valiosos de las personas que administran estos sistemas, además que se realizaran entrevistas sobre la información recopilada a las personas que trabajan en la Unidad financiera y académica, y personas que toman decisiones en base a los sistemas.

Mediante esta modalidad de investigación va a permitir tomar en contacto directamente con la problemática actual en la universidad mediante el método planteado con el tema de investigación.

3.2.Niveles o tipos de Investigación

3.2.1. Exploratorio

La investigación es exploratoria porque se hace el análisis de los procesos de las seguridades de los SGBD de los Sistemas de información de la UFA-ESPE-L

3.2.2. Descriptivo

Permite determinar las causas por los que se ha planteado como problema las seguridades de los SGBD de las bases de datos en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

3.2.3. Correlacional

Es correlacional esta investigación porque busca la relación entre la variable independiente que es la Administración de los SGBDS que componen las bases de datos de los sistemas de información y la incidencia sobre variable dependiente que es el control de seguridades de las Bases de Datos.

3.3.Población y Muestra

Para la población de la presente investigación se ha tomado en cuenta las personas que administran los DBMS de los sistemas de información de la Universidad.

Así como las entrevistas que se les tomará a los dos jefes de Unidad como son la Financiera y la de tecnologías de la Información y las Comunicaciones.

Descripción	Población	%
Administrador de Bases de Datos	1	25%
Soporte a Sistemas de Información	1	25%
Jefes de Sección	2	50%

Tabla 3.1. Población a ser entrevistada (Navas P., 2014)

Como en la tabla se puede observar el número de personas que intervendrán en el trabajo de campo para el proyecto es reducido, lo que se hace es tomar el 100% de la población.

3.4.OPERACIONALIZACIÓN DE LAS VARIABLES

3.4.1. Operacionalización de la Variable Independiente: Administración de los SGBD que componen las bases de datos de los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMES BÁSICOS	TÉCNICAS E INSTRUMENTOS
La administración de los SGBD está orientado a la evaluación de aspectos relacionados con la eficiencia, seguridad y productividad de las fortalezas y debilidades de las bases de datos de los sistemas de información de la Universidad.	Evaluación de la eficiencia. Evaluación de la Seguridad. Evaluación de la Productividad. Bases de Datos en los Sistemas de Información.	Información consistente Reportes con datos consistentes Optimización de recursos Administración de las Bases de datos ágil y oportuna.	¿La información de los SGBD se almacena en datos estructurados? ¿Los SGBD disponen de seguridades propias para garantizar la información? ¿La información almacenada en los SGBD's, refleja en los procesos de ingreso y salida de la misma?	Entrevista Guía de la entrevista Análisis de Documentos

Tabla 3.2. Operacionalización de la Variable Independiente (Navas P., 2014)

3.4.2. Operacionalización de la Variable Dependiente: El control de las seguridades en las bases de datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMES BÁSICOS	TÉCNICAS E INSTRUMENTOS
La seguridad de la información implica protegerlos de operaciones indebidas que pongan en peligro su consistencia e integridad de cualquier tipo de persona, esto se logra con mecanismos que permitan estructurar y controlar el acceso y actualización de éstos.	Alteración de la información Acción de entes externos. Trastorno funcional del sistema	Informes y reportes inconsistentes Pérdida de información Servidor saturado.	¿Se presentan pérdidas o alteración de información en los sistemas? ¿Están identificados los factores físicos y lógicos del sistema? ¿Existe un plan de contingencias adecuado para proteger la información?	Entrevista Guía de la entrevista Análisis de Documentos

Tabla 3.3. Operacionalización de la Variable Dependiente (Navas P., 2014)

Técnicas e instrumentos

Entrevista.

Dirigido a personal directivo y técnico, elaborado con preguntas abiertas y que permitirán obtener información de los especialistas sobre las variables de estudio. Su instrumento será la guía de la entrevista.

Guía de Entrevista

Este instrumento ayudará a poder llevar una entrevista que esté acorde con el tema planteado y que la información que se pueda obtener de los directivos y administradores de Bases de Datos de la Universidad ayude a sacar adelante la investigación planteada.

Inspección

Se realizará inspecciones físicas de instalaciones y puestos de trabajo en el personal operativo para la evaluación de los riesgos.

Validez y confiabilidad

Los instrumentos serán sometidos a criterios de validez a través de la técnica de "juicio de expertos" mientras que la confiabilidad se lo hará con la aplicación de una "prueba piloto" a la Universidad.

Plan de Recolección de Información

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación.
¿De qué personas u objetos?	Personal administrativo y soporte de software.
¿Sobre qué aspectos?	Indicadores (matriz de operacionalización de variables)
¿Quién, Quiénes?	Milton Patricio Navas Moya
¿Cuándo?	Segundo Cuatrimestre del 2014
¿Dónde?	Universidad de las Fuerzas Armadas ESPE Latacunga
¿Cuántas veces?	Una para la obtención de la información para la Investigación
¿Qué técnicas de recolección?	Entrevista. Encuesta Observación.
¿Con qué?	Cuestionario Guías de entrevista
¿En qué situación?	Durante las jornadas de trabajo.

Tabla 3.5. Plan de Recolección de la Información (Navas P., 2014)

3.5.Plan de Procesamiento de Información

Los datos recogidos se transforman siguiendo ciertos procedimientos.

- Revisión crítica de la información recogida; es decir, limpieza de la información defectuosa: contradictoria, incompleta, no pertinente, etc.
- Repetición de la recolección, en ciertos casos individuales, para corregir fallas de contestación.
- Tabulación o cuadros según variables de cada hipótesis: cuadros de una sola variable, cuadro con cruce de variables, etc.
- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente, que no influyen significativamente en los análisis).
- Estudio estadístico de datos para presentación de resultados.

Análisis e Interpretación de Resultados

- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados, con apoyo del marco teórico, en el aspecto pertinente.
- Comprobación de hipótesis para la verificación estadística conviene seguir la asesoría de un especialista.
- Establecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

ANALISIS E INTERPRETACION DE RESULTADOS

4.1.Análisis e Interpretación de los Resultados

Para la obtención de los resultados del estudio de campo que consistió en la entrevista a las personas que dirigen la Unidad de tecnologías de la Información y las Comunicaciones así como a la persona que está encargada de la administración de los sistemas de información, y obteniendo información de algunos documentos que son importantes para la investigación ya que son reportes de algunas novedades presentadas entre el proceso y el sistema de información de la institución en donde se puede apreciar que existen algunas descoordinaciones que pueden ir en perjuicio de la Universidad.

En la UTIC en la actualidad trabajan los siguientes sistemas de información con sus respectivas bases de datos, que son las que se deben cuidar para evitar posibles alteraciones de la información.

Los sistemas de información que se detallan en la parte inferior son aquellos que se encuentran en producción dentro de la Universidad y que no todos son desarrollados internamente, algunos fueron adquiridos a empresas desarrolladoras, mismas que se encargan de dar el soporte, y por consiguiente también de las actualizaciones.

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATANCUNGA					
Sistemas de Información que en la actualidad trabajan en la UTIC					
N.	**SISTEMA**	**PROPIETARIO**	**ESTADO**	**BASE DE DATOS**	**DEPARTAMENTO**
1	Registro de Ingresos SISRIN	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	Fox Pro 8	Financiero
2	Ordenes de Pago	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	Fox Pro 8	Financiero
3	Sistema Escolastico de Inglés para niños ESCOING	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	Fox Pro 8	Idiomas
4	Sistemas de Control de Accesos Web Access	Software Libre	En producción	MySql	Biblioteca
5	Sistema de Gestión Escuela de Conducción	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Escuela de Conducción
6	Plataforma Virtual MOODLE	Software Libre	En producción	MySql	Académico
7	Software OTRS (Control de Recursos Informáticos)	Software Libre	En producción	MySql	UTIC
8	Sistema ALUMNI ESPEL	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Posgrados e Investigación
9	Sistema de Gestión de Laboratorios SGLAB	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Laboratorios
10	Sistemas de Gestión de Concurso de Proyectos INNOVATE	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Posgrados e Investigación
11	Sistema de Registro de Libros biblioteca Virtual	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Biblioteca
12	Sistema de Registro de Actividades Docentes SG-RAD	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Académico
13	Sistema Academico del programa ASEP Chevrolet	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	En producción	MySql	Talleres mecanicos
14	Modulo DIM Anexos y Formularios	Software Libre del SRI	En producción		Departamento Financiero
15	Sistema de Encuestas	Software Libre LimeSurvey	En producción	MySql	Academico

Tabla 4.1. Sistemas de Información en Producción UFA _ESPEL (Navas P., 2014)

De igual manera la Universidad cuenta con sistemas que fueron adquiridos a terceros con la finalidad de agilitar procesos y mejorar la atención a los usuarios y que la administración sea efectiva y en un menor tiempo.

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATANCUNGA					
Sistemas de Información que en la actualidad trabajan en la UTIC					
N.	**SISTEMA**	**PROPIETARIO**	**ESTADO**	**BASE DE DATOS**	**DEPARTAMENTO**
16	Sistema Contable Financiero Olympo	Empresa PROTELCOTELSA S.A.	En producción	Oracle 8i, Ms SQL SERVER 2008	Departamento Financiero
17	Sistema de Control biométrico SQUARENET	Empresa Squarenet	En producción	MySql	Talento Humano
18	Sistema de Gestión de Biblioteca SIABUC 9	Universidad de Colima Mexico	En producción	PostgreSQL 8.2	Biblioteca
19	Sistema Spontania	Universidad de Colima Mexico	En producción		Audiovisuales

Tabla 4.2. Sistemas de Información en Producción contratados a terceros UFA _ESPEL (Navas P., 2014)

En la actualidad la institución tiene algunos aplicativos que se encuentran ya fuera de producción, ya sea porque los sistemas anteriormente indicados suplen esa función o porque ya no se realiza algunos de esos procesos, y estos son:

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATANCUNGA

Sistemas de Información que en la actualidad trabajan en la UTIC

N.	SISTEMA	PROPIETARIO	ESTADO	BASE DE DATOS	DEPARTAMENTO
20	Sistema de Gestión de Rancho	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	Consulta	MySql	Talento Humano
21	Sistema de Activos Fijos SAF	Ministerio de Defensa de la FF.TT	Consulta	Fox Pro 2.6	Financiero
22	Sistema Academico de Carreras	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	Consulta	Sybase - SQL Server	Acádemico
23	Sistema Academico de Idiomas	Universidad de las Fuerzas Armadas ESPE extensión Latacunga	Consulta	Sybase - SQL Server	Acádemico
24	Sistema de Tributación SITAC	Empresa Asesor Contable	Consulta	Visual Fox Pro	Financiero
25	Sistema de Control Biometrico MOQASIST	Empresa TELECOM SYSTEM	Consulta	Visual Fox Pro	Talento Humano
26	Sistema Strategic	Empresa Strategic	Fuera de Producción	SQL Server 2000	
27	Sistema Contable SIGOC	Empresa PROTELCOTELSA S.A.	Fuera de Producción	Microsoft Access 95	
28	Sistema Escolástico de la MED	Universidad de las Fuerzas Armadas ESPE Matriz	Fuera de Producción	Sybase - SQL Server	

Tabla 4.3. Sistemas de Información fuera de Producción UFA _ESPEL (Navas P., 2014)

Entrevista con el Jefe de la Unidad de Tecnologías de la información y las Comunicaciones

Para realizar la entrevista a la Directora de la UTIC se procedió a revisar toda la información que se tiene sobre las actividades que se realizan en esta dependencia y que funciones desempeñan cada uno de los empleados que aquí laboran y según el manual de funciones, procesos y perfiles de la Universidad se tiene que el Jefe de UTIC.

En el reglamento Interno de la Universidad de las Fuerzas Armadas y en el Art 191: manifiesta las actividades del "Director de la Unidad de tecnologías de la Información y Comunicación será responsable de:

a. Planificar, organizar, dirigir y controlar las actividades de la Unidad, así como de la evaluación de sus resultados.
b. Gestionar el mejoramiento continuo y el desarrollo de la Unidad a su cargo;

c. Coordinar internamente con las unidades organizacionales correspondientes y externamente con organizaciones públicas y privadas la ejecución de las actividades de la unidad para el logro de sus objetivos;
d. Cumplir lo establecido en el Plan Estratégico Institucional y planes operativos anuales en su ámbito de gestión; y,
e. Cumplir la normativa institucional y las resoluciones emitidas por los órganos competentes".

GUIA DE ENTREVISTA A LA DIRECTORA DE LA UTIC.

N.	PREGUNTA	RESPUESTA
1.	¿En la institución los sistemas de información han tenido algún inconveniente de seguridad?	La Universidad si ha tenido problemas de seguridad particularmente en los sistemas financieros y en el escolástico, los mismos que fueron detectados y se han tomado las medidas necesarias, y se tienen también reportes de intentos de ingreso a través del UTM(Unified Threat Management) o Gestión Unificada de Amenazas de la institución.
2.	¿Conoce de algún computador que en la institución haya realizado algún ataque informático, y/o alterado la seguridad de las bases de datos de los Sistemas de Información?	En una ocasión se alteró información de las bases de datos del sistema de tesorería y que pudo ser comprobado a nivel de servidor en la bitácora de actividades, de que un usuario con privilegios distintos al cargo de la Sra. Tesorera había entrado a esa máquina y borro documentación en el sistema, lo cual fue denunciado ante las autoridades.
3.	¿Existen controles de seguridad, a nivel de bases de datos en los sistemas de información de la institución?	Tienen las seguridades básicas de control de usuario, más no existe una auditoría a la gestión de las contraseñas que ayude a garantizar la información.
4.	¿En los sistemas de información de la institución, tienen una adecuada gestión de contraseñas?	No, porque la gran mayoría de aplicativos se los realizo en FoxPro y carecen de algún tipo de auditoría de contraseñas, los más actuales en su gran mayoría no disponen de este tipo de

		controles y apenas maneja dos o tres tipos de usuario.
5.	¿Han existido ataques a la seguridad de los sistemas de información de la institución por descuido propio de la Unidad o alguien del personal técnico?	Por intereses personales, del personal técnico se alteró información de las bases de datos lo que perjudico a un usuario y se procedió a denuncias y a los respectivos consejos de disciplina con la finalidad de esclarecer estos temas.
6.	¿Han existido intentos de ataques informáticos externos a la institución, que hubieran podido alterar o modificar la información de las Bases de Datos?	En innumerables ocasiones se ha tenido reportes de intentos fallidos de ingreso a la información de la institución, más los dispositivos de seguridad realizaron su trabajo evitando de esta manera la alteración de la información.
7.	¿Existe una inadecuada utilización de los usuarios de los sistemas de información, que hubieran causado alguna alteración a los informes finales?	Al tratarse de una institución de educación y también militar, se tiene información que son compartidas y otras que se requiere llevar por separado, lo que en ocasiones genera ciertos problemas
8.	¿Considera oportuna la generación de una guía técnica integral y balanceada para la medición del desempeño que apoye a la mejora continua de los sistemas de información?	Considero oportuno que se pueda contar con una guía técnica ya que es muy importante que el personal técnico del área de desarrollo y administración de bases de datos pueda contar con un documento que ayude a la mejora de procesos.

Tabla 4.4. Guía de entrevista Jefe de la UTIC (Navas P., 2014)

ANALISIS, INTERPRETACION Y EVIDENCIAS DE LAS RESPUESTAS DE LA ENTREVISTA REALIZADA A LA JEFE DE LA UTIC

De acuerdo a las funciones que debe cumplir el Director de la UTIC, se procedió con una entrevista a la persona que se encuentra en esta posición y el cual manifiesta lo siguiente:

1. **¿En la institución los sistemas de información han tenido algún inconveniente de seguridad?**

La Universidad si ha tenido problemas de seguridad particularmente en los sistemas financieros y en el escolástico, los mismos que fueron detectados y se han tomado las medidas necesarias, y se tienen también reportes de intentos de ingreso a través del UTM (Unified Threat Management) o Gestión Unificada de Amenazas de la institución.

Análisis

La Jefe de la UTIC indica que si habido alteración de información a nivel de bases de datos, pero que fueron identificadas y que se tomaron las debidas medidas correctivas a este tipo de actitudes de algunas personas que no eran ajenas a la institución.

Interpretación

De acuerdo a la entrevista la jefa de la UTIC manifiesta que se han tenido problemas de seguridad, los mismos que son evidenciados en los anexos, que son detallados, más adelante, particularmente en los sistemas de información académico y financiero.

2. **¿Se conoce de que si de algún computador de la institución alguna vez ha realizado algún ataque informático, y que haya alterado la seguridad de las bases de datos de los Sistemas de Información?**

Si han existido este tipo de anormalidades y se presentó puntualmente en la máquina de tesorería, pero no fue detectado en la bitácora de los servidores y se revisó otras actividades propias de la computadora y del perfil de usuario y se pudo conocer de que fue manipulada con otro usuario, y de igual manera se tomó acciones legales en contra de la persona que cometió esa falta.

Análisis

Los problemas se presentan cuando existen usuarios de máquinas que manejan información relevante de la Universidad, y que sus sitios puedan tener documentos que tienen que cuadrar con lo que indican en el sistema tanto local, como el gubernamental.

Interpretación

Cuando suceden alteraciones de información, las seguridades propias de la institución se disparan ocasionando que los usuarios de la información pongan más empeño y controlen las contraseñas a ellos otorgadas, aunque los usuarios conocen que los aplicativos no tiene una gestión adecuada de auditoría de contraseñas de acuerdo a perfiles y procesos.

3. ¿Existen controles de seguridad, a nivel de bases de datos en los sistemas de información de la institución?

Según información proporcionada por la jefa de la UTIC los sistemas de información tienen las seguridades básicas de control de usuario, a nivel de SGBD no se tiene ningún tipo de seguridades.

Análisis

No se tiene un control de seguridades a nivel de SGBD's, porque las herramientas utilizadas para los aplicativos de la Universidad son antiguas o el UTM asegura los procesos y la información.

Interpretación

Los aplicativos de la Universidad no tienen seguridades a nivel de SGBD's, ya que se tratan de herramientas antiguas y porque los administradores de los sistemas de información son dependientes de las seguridades perimetrales.

4. **¿En los sistemas de información que se tienen en la institución se tiene una adecuada gestión de contraseñas?**

Dentro de la Universidad la gran mayoría de aplicativos se los realizo en FoxPro, MySQL o SQL Server 2000 porque el desarrollador dominaba estas herramientas y lo que se hizo fue en base a criterios propios del desarrollador.

Análisis

La Universidad cuenta con muchos sistemas antiguos y que fueron desarrollados en bases de datos Fox Pro, así como MySQL, y en otros casos SQL Server por lo que al pasar el tiempo estos SGBD no pudieron asegurar sus procesos de acuerdo a la realidad actual ver **Anexo 2**.

Interpretación

Los sistemas de información de la Universidad no tienen unas bases de datos seguras por lo que pueden ser blanco de ataques, tanto externos como internos, siempre y cuando se pueda pasar por alto la seguridad perimetral.

5. **¿Han existido ataques a la seguridad de los sistemas de información de la institución por descuido propio de la Unidad o alguien del personal técnico?**

Se han presentado problemas de alteración de información, los mismos que en su momento fueron denunciados y esclarecidos, esto porque existe dos sistemas que realizan una misma actividad, y ha ocasionado llamados de atención, a los implicados en la alteración de la información, como se puede ver en **el Anexo 1**.

Análisis

En ocasiones se puede tener algunas violaciones al código de ética de los profesionales lo que pueden ocasionar serios inconvenientes legales que van en perjuicio de la Universidad.

Interpretación

Los SGBD´s actuales de la Universidad, en los que están los aplicativos no soportan este tipo de seguridades ya que son muy antiguos y en otros casos no tenían en cuenta algunas seguridades.

6. ¿Han existido intentos de ataques informáticos externos a la institución, que hubieran podido alterar o modificar la información de las Bases de Datos?

En innumerables ocasiones se ha tenido reportes de intentos fallidos de ingreso a la información de la institución, más los dispositivos de seguridad realizaron su trabajo evitando de esta manera la alteración de la información.

Análisis

A nivel de seguridades la Universidad siempre ha estado equipado con dispositivos de alta tecnología a nivel de redes y servidores que han sido los que han cubierto los aplicativos de la institución.

Interpretación

Cuando se tiene dispositivos que cubren toda la institución de seguridad poco o nada interesa tener seguridades en los SGBD's pero a veces resulta contraproducente y se dan casos como los ya manifestados.

7. ¿Existe una mala utilización de los sistemas de información de parte de los usuarios que hubieran causado alguna alteración a los informes finales?

En algunas ocasiones si existen errores que no son notificados en su debido momento, lo que desencadena en reportes que no reflejan la realidad financiera y/o académica de la Universidad, ocasionando retardo al momento de tomar decisiones.

Análisis

En ocasiones se tienen problemas en los sistemas de información, particularmente en la digitación o eliminación involuntaria de algún registro que ocasiona retardo en la entrega de reportes que van hacia los directivos de la Universidad.

Interpretación

Los usuarios de los sistemas de información comenten muchos errores involuntarios como de digitación, eliminación de registros en los aplicativos que permiten realizar este tipo de acciones, pero que al final si alteran en los informes que se presentan a los directivos de la Universidad, como se puede observar en el **Anexo 1**.

8. ¿Considera oportuna la generación de una guía técnica integral y balanceada para la medición del desempeño que apoye a la mejora continua de los sistemas de información?

Considero oportuno que se pueda contar con una guía técnica ya que es muy importante que el personal técnico del área de desarrollo y administración de bases de datos pueda contar con un documento que ayude a la mejora de procesos

Análisis

Siempre la elaboración de trabajos que permitan mejorar los procesos de una institución va a ser bienvenidos y mucho más cuando se trata de trabajos de investigación que se basan en realidades vividas y que bajo estándares internacionales se las debe mejorar.

Interpretación

Las normas basadas en COBIT siempre han sido de gran importancia sobre lo que tiene que ver con gobernabilidad de las TI, y ahora más cuando estas ayudan a mejorar procesos para garantizar la seguridad de la información.

Guía de entrevista al Especialista 1 en Tecnologías de la Información: Área de desarrollo de nuevas aplicaciones y administración de base de datos.

N.	PREGUNTA	RESPUESTA
1.	¿Existió en alguna ocasión mal uso de los sistemas de información, por los usuarios del mismo?	En muchas ocasiones los usuarios de los sistemas de información realizan ingresos de información incorrecta por lo que los reportes no reflejan lo que en verdad se tiene.
2.	¿Las seguridades de las bases de datos se las hace a nivel de SGBD y auditorías propias de los sistemas de información o a nivel de servidores y/o redes de datos?	Las seguridades de los sistemas de información se las hace a través de un clúster de seguridad que tiene la escuela, el mismo que presta las seguridades tanto internas como externas.
3.	¿Han existido pérdidas de información o alteración de la misma de parte de usuarios de los sistemas?	Dentro de los sistemas en la actualidad no se han realizado, pero hubo algunos incidentes que ocasionaron la alteración de la información
4.	¿Cómo ha controlado los ataques de hackers, crackers, phising o pharming hacia sus bases de datos?	Alguna vez se presentó problemas en los dbf, pero después el clúster se ha encargado de evitar que puedan ingresar en la información importante de la institución.
5.	¿Las contraseñas asignadas a los usuarios son seguras y cumplen con parámetros necesarios para evitar la pérdida o alteración de la información?	Las contraseñas están cifradas en símbolos especiales, por lo que no se requiere de mayor cuidado toda vez que la mayoría de usuarios desconocen de esta realidad
6.	¿Considera oportuna la generación de una guía técnica integral y balanceada para la medición del desempeño que apoye a la mejora continua de los sistemas de información?	Siempre es recomendable tener documentos que puedan ayudar en la consecución de los resultados en los procesos planteados dentro de una unidad de tecnologías y que estos reflejen en la administración de la información.

Tabla 4.5. Guía de entrevista Administrador de las Bases de datos - UTIC (Navas P., 2014)

ANALISIS, INTERPRETACION Y EVIDENCIAS DE LAS RESPUESTAS DE LA ENTREVISTA REALIZADA AL ADMINISTRADOR DE LAS BASES DE DATOS.

1. **¿Existió en alguna ocasión mal uso de los sistemas de información, por los usuarios del mismo?**

En la institución se tiene personal altamente capacitado, pero en muchas ocasiones los usuarios de los sistemas de información realizan ingresos de información incorrecta por lo que los reportes no reflejan lo que en verdad se tiene, esto ocasiona que se tenga cierto nivel de inconformidad de parte de las autoridades de la Universidad.

Análisis

En una institución de educación superior todos sus empleados tienen una preparación muy alta, por lo que ingresos mal intencionados casi nunca se han presentado, información que no refleja la realidad de ese tipo si, ya sea por problemas en los papeles o por faltas en algún tipo de documento, o en inventarios físicos.

Interpretación.

La información mal ingresada por lo general obedece a documentos físicos mal elaborados, y que siempre son justificados por los empleados que hacen uso de los servicios o de los procesos de la Universidad.

2. **¿Las seguridades de las bases de datos se las hace a nivel de SGBD y auditorías propias de los sistemas de información o a nivel de servidores y/o redes de datos?**

La Universidad ha invertido en comprar equipos que ayuden a la seguridad de la información y dentro de esto se encuentran las seguridades de los sistemas de

información que se las hace a través de un clúster de seguridad, el mismo que presta las seguridades tanto internas como externas.

Análisis

Se tiene plena confianza en lo que pueda brindar el UTM, en cuanto a seguridades y administración de los distintos dispositivos de comunicaciones y computadores y por defecto al servidor de bases de datos en donde se encuentra toda la información de la Universidad.

Interpretación

Se piensa que un dispositivo de seguridad puede ayudar a garantizar la información, por lo que no se plantea migrar la información a motores de bases de datos de última generación y complementar con el UTM con que cuenta la institución a nivel de seguridad perimetral y que ofrece las seguridades necesarias como se puede observar en el **Anexo 3,** que es el reporte de posibles intrusiones hacia la Universidad.

3. ¿Han existido pérdidas de información o alteración de la misma de parte de usuarios de los sistemas?

Dentro de los sistemas en la actualidad no se han realizado este tipo de alteraciones, pero hubo algunos incidentes en años anteriores que ocasionaron la alteración de la información, pero que fueron detectados corregidos y en algunos casos tomados en cuanta para mejorar la seguridad de la información.

Análisis

Desde siempre ha existido la inquietud de los usuarios de querer alterar información o simplemente eliminarla, por malos ingresos o por evitar llamados de atención pero todos propósitos se han terminado con la implementación de seguridades y la posterior puesta en conocimiento de la comunidad universitaria.

Interpretación

Existe ya un control de las seguridades así sean estas a nivel de servidores o de UTM, y que está en conocimiento de todo el personal que labora en la Universidad que ha hecho que los intentos hayan quedado descartados internamente. Lo que ayuda a la administración de los sistemas en otros ámbitos ajenos a la alteración o eliminación de los datos.

4. ¿Cómo ha controlado los ataques de hackers, crackers, phising o pharming hacia sus bases de datos?

Antes las bases de datos se almacenaban en archivos que podrían ser abiertos en procesadores de texto u Hojas de cálculo y esto ocasionaba que los virus puedan infectar y posterior pérdida de información, más últimamente esto ha cambiado con los nuevos SGBD's.

Análisis

Este tema de código malicioso o virus en los aplicativos son muy comunes en la actualidad, pero en el pasado los virus atacaban información en archivos de hojas de cálculo de datos y sobre todo en procesadores de texto, lo que ocasionaba grandes pérdidas de información, hoy en día un UTM soluciona inconvenientes de seguridad a todo nivel, según se puede observar en el Anexo 3

Interpretación

La solución que brinda un UTM es una garantía para la Universidad, ya que no permite la filtración de código malicioso ni de posibles ataques de hackers o crackers, mas sin embargo algunos virus son detectados con antivirus que tienen suscripción la institución.

5. ¿Las contraseñas asignadas a los usuarios son seguras y cumplen con parámetros necesarios para evitar la pérdida o alteración de la información?

Las contraseñas están cifradas en símbolos especiales, por lo que no se requiere de mayor cuidado toda vez que la mayoría de usuarios desconocen de esta realidad.

Análisis

Dentro de la institución al conocerse de las seguridades que tiene en la actualidad, los aplicativos cuentan con seguridades básicas a nivel de gestión de contraseñas lo que no permite tener un control de que actividades realizan los usuarios de acuerdo al perfil de cada uno de ellos.

Interpretación

No se toman las debidas garantías en la asignación de contraseñas, porque las seguridades de dispositivos a otro nivel, lo que hace que sean seguras y que no permitan la alteración de la información.

6. ¿Considera oportuna la generación de una guía técnica integral y balanceada para la medición del desempeño que apoye a la mejora continua de los sistemas de información?

Siempre es recomendable tener documentos que puedan ayudar en la consecución de los resultados en los procesos planteados dentro de una unidad de tecnologías y que estos reflejen en la administración de la información.

Análisis

Tener una guía que ayude a la generación de procesos que ayuden a garantizar la información siempre es bueno, y si el objetivo es mejorar se la debe desarrollar y poner en práctica lo antes posible con el desarrollo de los nuevos aplicativos.

Interpretación

La generación de una guía técnica de seguridades dentro de la institución va a ser una ayuda para la mejora de procesos de seguridades físicas y lógicas, ya que de esta manera se va optimizar todos los recursos que se tienen dentro de la Universidad.

4.2.DEMOSTRACIÓN DE LA HIPÓTESIS

En el proyecto se pudo verificar que los sistemas de información aportan un gran valor a los procesos de gestión de actividades de los empleados de la Universidad, pero en la gran mayoría no son seguros debido a muchas circunstancias entre las que podemos citar están, los Sistemas Gestores de Bases de Datos(SGBD's), no garantizan la información que en ellos se almacenan, las versiones son muy atrasadas y que en algunos casos no son escalables, se confía en la seguridad perimetral para el aseguramiento de los procesos y por lo tanto de los datos como se lo puede ver en el **Anexo 2**.

La información fue alterada, lo que ocasionó retraso al cumplir con actividades propias de la institución **Anexo 3**, se tomaron medidas correctivas y más no preventivas que es lo recomendable siempre en cualquier lugar que disponga de tecnologías de la información, se pudo identificar algunas debilidades dentro de la administración de las seguridades al momento de la asignación de contraseñas a los usuarios, hechos que se deben a falta de políticas que ayuden a realizar estos procesos de manera eficaz.

El análisis revela que existen problemas que son fundamentales y que se requieren de toma de decisiones directivas **Anexo 1**, es decir que existen riesgos que no fueron oportuna y debidamente mitigados. En base a la información recabada y que fue tema de estudio se **acepta** la hipótesis: "La administración de los SGBD de los sistemas de información incidiría en el control de las seguridades en las bases de datos en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga", ya que se pudo demostrar mediante los anexos presentados.

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATANCUNGA

Niveles de Seguridad en los SGBD's de los Sistemas de Información

N.	SGBD	MANTENIMIENTO	AUDITORIA	VERSION	TIPO	SISTEMA OPERATIVO	HARDWARE	APLICACIONES
1	Fox Pro	Nivel B3	SI	8.0	N/A	Windows 2000	Computador personal	7
2	MySql	Nivel B3, C1	NO	4.0.24	Libre	Linux Centos	HP Proliant	2
3	MySql	Nivel B3, C1	NO	4.1.25	Libre	Windows 2008	DELL Power Edge	11
4	Oracle. Ms SQL SERVER	Nivel B3, C2	SI	8i, 2008	Professional	Linux Centos / Windows 2008	HP Proliant	1
5	PostgreSQL	Nivel B3, C2	SI	8.2	Libre	Linux Centos	HP Proliant	
6	Fox Pro	Nivel B3	NO	2.6	N/A	Windows 2008	DELL Power Edge	1
7	Sybase - SQL Server	Nivel B3	NO	7.0	Professional	Windows 2008	DELL Power Edge	3
8	SQL Server	Nivel B3	NO	2000	Professional	Windows 2008	DELL Power Edge	1
9	Microsoft Access	Nivel B3	NO	95	Professional	Windows 2008	DELL Power Edge	1

Tabla 4.6. Sistemas Gestores de Bases de Datos - UTIC (Navas P., 2014)

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1.Conclusiones

- La Universidad de las Fuerzas Armadas ESPE extensión Latacunga no cuenta con seguridades propias en los SGBD's de los sistemas de información.

- Los SGBD's de los sistemas de información de la institución no tienen una adecuada confidencialidad, integridad y disponibilidad, esto basado en los documentos recopilados en algunos departamentos de la Universidad.

- No se han realizado mediciones del desempeño de los SGBD's de los sistemas de Información, ni se han realizado evaluaciones de seguridad para detectar los problemas, hasta que éstos se presentan.

- En muchas ocasiones los reportes que entregan las distintas dependencias no coinciden con los sistemas de información gubernamental, lo que genera un retraso en los informes que se deben presentar a las autoridades de la Universidad matriz.

- Todas las seguridades de la información están dadas a nivel de servidores o de equipos UTM que aseguran la información y no existen seguridades a nivel de SGBD o de auditoría de aplicativos en las bases de datos.

- Se tienen un gran número de aplicativos desarrollados en herramientas que ya desaparecieron lo que ha ocasionado que no exista escalabilidad y en muchas ocasiones no se las siga utilizando ni siquiera como fuente de consulta.

- Se debe centralizar de mejor manera los procesos, en un solo sistema que cuente con las debidas seguridades y sobre todo que garantice cuales fueron los usuarios que realizaron las distintas actividades en estas aplicaciones.

5.2.Recomendaciones

- Los Sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga deberían ser migrados a herramientas de última generación o SGBD's que dispongan de seguridades propias, y que estas puedan garantizar la información.

- Al tratarse de una institución de Educación Superior y a la vez Unidad Militar los procesos deben cumplir esa dualidad, lo que se requiere es que se generen aplicativos que puedan servir de puente entre estos procesos para que no exista duplicidad de información.

- Además de las seguridades que proporciona el área de conectividad, redes y seguridades es importante que la institución cuide de mejor manera los SGBD's aplicando la norma Cobit, para que técnicos de otras áreas no puedan tener acceso a los datos que se encuentran en los Sistemas de Información.

- Desarrollar futuras aplicaciones bajo un mismo estándar particularmente de seguridad, esto haría que la información siempre este precautelada por los administradores de las Bases de Datos.

- En base a los criterios técnicos emitidos por el personal de la UTIC se recomienda realizar la implementación de una Guía Técnica para las seguridades de los sistemas de información.

- La Guía Técnica sugerida debería ser implementada en el modelo Cobit 5, que dentro de su portafolio de normas y estándares contiene los apartados de Seguridad de la información como medio para garantizar la Gobernabilidad de las Unidades de Tecnologías de la Información y las Comunicaciones.

CAPÍTULO VI

LA PROPUESTA

6.1.DATOS INFORMATIVOS

6.1.1. Título: "GUÍA TÉCNICA PARA LA ADMINISTRACIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN APLICANDO EL MODELO COBIT 5 EN LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSIÓN LATACUNGA"

6.1.2. Institución

Ejecutora: Universidad de las Fuerzas Armadas ESPE extensión Latacunga

6.1.3. Beneficiarios:

- Unidad de Tecnologías de la Información y las Comunicaciones de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga

6.1.4. Ubicación:

- **Provincia:** Cotopaxi
- **Cantón:** Latacunga
- **Dirección:** Quijano y Ordoñez S/N y Hermanas Páez

6.1.5. Equipo Técnico Responsable

- **Investigador:** Milton Patricio Navas Moya
- Especialistas de la Unidad.

6.2.Antecedentes de la propuesta

La Universidad de las Fuerzas Armadas ESPE extensión Latacunga es una institución de educación superior, por lo tanto los sistemas de información y las tecnologías en general cumplen un papel fundamental para lograr cumplir con los objetivos que estos se planteen, sin embargo en el proyecto se ha podido constatar que existen ataques a los datos de la institución y que estos cada vez son más frecuentes, por lo que basándose en la investigación que antecede, la Universidad urgentemente se plantea una guía técnica

para garantizar las seguridades dentro de las Bases de Datos de los sistemas que trabajan en la Unidad de Tecnologías de la Información y las Comunicaciones y de esta manera obtener de los aplicativos una mejora abrumante, y de parte de los técnicos un cambio de mentalidad hasta llegar a alcanzar una conducta proactiva y que el cambio refleje en la seguridad de la información.

Alcanzar esa proactividad seria administrar y realizar aplicativos con controles que ayuden a minimizar potenciales riesgos en la información y las posibles vulnerabilidades en los sistemas de información o de la infraestructura de seguridades de la institución.

6.3.Justificación

Ante los hechos de falta de seguridades suscitados en la Universidad que existen serios problemas de seguridad que deberían ser tomados en cuenta con la idea de mejorar todos los procesos y de esta manera garantizar la información y que los reportes generados reflejen la verdad de la situación institucional.

No hay que perder de vista la ausencia de seguridades de SGBD's a causa de las versiones caducas de los mismos por lo que se puede manifestar que es urgente un cronograma de actualización de los mencionados motores de bases de datos, mejorar la capacitación a los empleados técnicos con la finalidad de mitigar los posibles riesgos y amenazas existentes dentro de la institución, ya que en la actualidad y con el tiempo nos podemos dar cuenta que los ataques de virus o códigos maliciosos se vuelven más sofisticados y peligrosos para la integridad de los datos.

Para la Universidad de las Fuerzas Armadas ESPE extensión Latacunga se decidió aplicar en base a la experiencia del investigador y a trabajos de gobernabilidad de las Tecnologías de la Información y las Comunicaciones que se han implementado en la matriz y que son aplicados en la actualidad en la extensión, ya que de esta manera ayudara a la optimización del riesgo, los recursos, a transparentar los procesos y a los usuarios, ayudará en el marco de gestión de TI, gestionara la estrategia, la arquitectura de la

Institución, la innovación, los requisitos, archivos y sobre todo la continuidad de los principios institucionales.

Este modelo está basada en las mejores prácticas de los estándares de seguridades tales como:

Cobit 5 y la ISO/IEC 27001:2005

Separa la seguridad de la Información en dos procesos:

- Gestionar la seguridad
- Gestionar la seguridad de los servicios de la seguridad.

Cobit 5 y la ISO/IEC 38500:2008

Definen los procesos de la gestión de las Tecnologías de la Información

Cobit 5 y la ISO/IEC 31000:2009

Definen los principios de la gestión de riesgos, necesarios para poder implementar seguridades de la información.

Cobit 5 y CMMI

Define controles para el desarrollo y la adquisición de software CMMI a través de sus procesos, cumple con dichos controles, por lo tanto se complementan y en conjunto abarcan desde el desarrollo de software hasta la gestión de entrega y mantenimiento del mismo. Aunque la forma de evaluar la madurez se alinea según COBIT a lo que dice la norma ISO 15504.

Cobit 5 y la ISO/IEC 15504

Este estándar determina la capacidad de mejora del proceso de software, que básicamente es un modelo para la mejora y la evaluación del desarrollo y mantenimiento de los sistemas de información.

Basados en esos criterios la investigación se centrará en centrada en 3 ejes fundamentales para la investigación:

- Seguridad de la información
- Uso de identificadores de COBIT 5 para implementar la seguridad de la información en la práctica.
- Adaptación de COBIT 5 para la seguridad de la información al entorno institucional.

6.4.Objetivos

Objetivo General

Desarrollar una guía técnica para la administración de la seguridad de los sistemas de información aplicando el modelo COBIT 5 en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

Objetivos Específicos

- Mejorar los procesos de seguridad de la Información, mediante la definición de controles y lineamientos que deben cumplir las aplicaciones, sus administradores y usuarios, mediante la Guía Técnica.

- Mitigar los riesgos de seguridad existentes en los equipos donde reside la información, mediante la aplicación de la Guía técnica de aseguramiento de los datos en los sistemas de información.

- Socializar la guía técnica con las autoridades y administradores de los sistemas de información de la institución.

6.5.Análisis de Factibilidad

En la actualidad la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, dispone dentro de su planificación todos los datos y los elementos relevantes para llevar a cabo una guía técnica que ayude a la administración de las seguridades de los sistemas de información.

6.5.1. Factibilidad Técnica

Para desarrollar una guía técnica el investigador cuenta con el conocimiento necesario basado en experiencias y en información relevante de empresas certificadoras que garantizan las seguridades a todo nivel, con la tecnología para el desarrollo de un documento que pueda servir como base fundamental para que directivos, técnicos, usuarios de los sistemas de información que normen y regulen sus seguridades.

6.5.2. Factibilidad Organizacional

La Universidad al ser una institución de educación superior está comprometida con la investigación y el avance tecnológico, por lo que cualquier proyecto que ayude a mejorar los procesos tendrá garantizado su ejecución, y mucho más el presente tema, que es el desarrollo de un Guía Técnica que ayude a la administración de las seguridades en los sistemas de información.

6.5.3. Factibilidad Económica

Para la aplicación de la guía técnica de administración de seguridades de los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, económicamente procede al no requerir de la adquisición de licencia alguna, pues se basa en un estudio de una norma de gobernabilidad de la información y que no es necesariamente adoptada para tales efectos.

6.6.Fundamentaciones

Para establecer seguridades en los sistemas de información de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, se debe establecer políticas claras de seguridades de la información, se debe mantener los niveles de confidencialidad, disponibilidad e integridad de los datos, para lograr un adecuado análisis, un diseño de aplicativos claros, y un desarrollo con normas que estén de acuerdo a los objetivos y metas de la institución.

Para conseguir esto y basado en un análisis de normas y estándares de seguridad de la información se optó por el modelo COBIT 5, que es un excelente marco de referencia en lo que es el gobierno de tecnologías de la información que tiene como eje fundamental la tecnología y la información para la creación de una cadena de valor en las instituciones.

Con la adopción de Cobit 5 para la seguridad de la información podrá ayudar a reducir los perfiles de riesgos a través de una adecuada administración de la seguridad.

6.6.1. Filosófica

Para el proyecto y su realización se utilizó el paradigma filosófico crítico propositivo ya que se cuestiona las seguridades de los SGBD y sus sistemas de información, y en bases a esto se desarrolla una propuesta de solución al problema de seguridades latentes en la Universidad.

Para poder tener claro de lo que se trata el proyecto de investigación, hay que tener claros los conceptos, normas y estándares que están directamente involucradas, sobre los sistemas de información que se encuentran trabajando en la Universidad y que son un buen punto de partida para las seguridades.

Definiciones Generales

- **Administración de Seguridades**

Toda institución o empresa, lo que más se enfrentan es con desafíos de seguridad en este mundo contemporáneo, toda vez que tener la información integra es un proceso vital

que conlleva a gastar grandes cantidades de dinero y en ocasiones a llenarse de pesimismo por no llegar a alcanzar las metas planificadas. Siempre se pretende tratar preventivamente los problemas de seguridad.

Para atender los desafíos que es tener una guía técnica, que significa tener un nuevo modelo a seguir en lo que tiene que ver con la administración de las seguridades que integre los elementos diversos en cuanto SGBD's que protegen el activo más importante de la institución que es la información, todo estos dentro de una solución completa, única y que sea de fácil administración. Esta guía técnica de administración de seguridades se encarga de alinear las seguridades con las necesidades que tiene la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, para que se garantice las seguridades se plantea en la guía técnica cumpla con los tres ejes fundamentales que son: la administración de la identidad y el acceso del usuario, la administración de las amenazas y la administración de la información sobre seguridad.

Todos estos componentes deben ser abiertos, flexibles y fácilmente integrables con las soluciones que dispone en la actualidad la UTIC como lo son los servidores y el UTM (Unified Threat Management) o Gestión Unificada de Amenazas, que se debe tener claro es que la administración de las seguridades tiene que tener un enfoque preventivo y con respuestas según demanda a los eventos dentro del cambiante entorno de las seguridades.

La seguridad es un componente importante en las infraestructuras tecnológicas de la actualidad. Que en un entorno informático dinámico en donde la automatización de procesos es lo más aceptado, la reconfiguración e implementación de sistemas son permanentes lo más importante y fundamental es asegurar los procesos y por este medio la información. Basados en este antecedente la Universidad de las Fuerzas Armadas ESPE extensión Latacunga tiene que contar con:

- Protección de la información crítica contra códigos maliciosos, tales como virus y worms.
- La mitigación del riesgo, al reducir vulnerabilidades.
- La implementación de políticas de seguridad.

- El aprovisionamiento y mantenimiento automatizado de las identidades digitales
- El acceso conveniente y seguro a las aplicaciones por todos los usuarios.
- Soluciones integradas, con control centralizado de la infraestructura extendida de seguridad.
- El cumplimiento de las regulaciones planteadas.

Está guía técnica de seguridades de los Sistemas de Información es un modelo que requiere la participación de los administradores de bases de datos y desarrolladores, con la flexibilidad necesaria para alinear cada aspecto con los puntos de seguridad en la Universidad, satisfacer sus necesidades de automatización, simplificación y agilidad de los procesos. Adicionalmente debería proporcionar una visibilidad en tiempo real para los más diversos procesos de seguridad que ocurren en la unidad de tecnologías, permitiendo de esta manera una respuesta adecuada y en el momento justo.

La integración de los componentes considerados claves dentro de COBIT para la administración de las seguridades, en una solución preventiva ayudaría para alcanzar la eficiencia operativa y el cumplimiento de las regulaciones gubernamentales y también a optimizar los costos, disminuir los riesgos y asegurar las operaciones institucionales.

- **Seguridad de la Información**

Para obtener la seguridad de los datos debemos alcanzar las medidas preventivas y reactivas de la información dentro de los sistemas y las bases de datos buscando siempre proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos, pilares fundamentales de la Seguridad Informática.

Como consecuencia de esta iniciativa para mejorar la seguridad de la información se ha basado en COBIT para poder alcanzar lo siguiente:

- Integrar la seguridad de la información dentro de la Universidad.
- Comunicar decisiones vinculadas con el riesgo y crear conciencia entre los usuarios y administradores sobre los riesgos.

- Mejorar la prevención, detección y recuperación de la información
- Reducir los incidentes vinculados a la seguridad de la información.
- Adquirir un entendimiento más profundo sobre la seguridad de la información.

Obtener la aprobación de los directivos es siempre un problema entre los administradores cuando de seguridad de la información se trata, sin embargo la adquisición de las normas COBIT siempre es positivo ya que indirectamente trata el tema de gobernabilidad de las TI.

Entonces las políticas definidas en la investigación contienen aspectos básicos y específicos del modelo COBIT que están dirigidos a la Unidad de Tecnologías de la Información y las Comunicaciones.

- **Sistemas de Información**

Un sistema de información, son la combinación de elementos tecnológicos como el hardware, el software, las comunicaciones y las personas que utilizan todo ese recurso para planificar, controlar y coordinar la toma de decisiones dentro de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga. Todos los procesos tienen que ser propios de la institución, desarrollados para satisfacer necesidades específicas, cuidando siempre el desarrollo con normas y estándares de análisis y diseño.

La Universidad con la intensión de mejorar los procesos y servicios se basan en sistemas de información para llevar a cabo y gestionar sus operaciones, interactuando con los usuarios de la aplicación y estos a su vez con los estudiantes, o proveedores de servicios o productos y de esta manera estar a la vanguardia tecnológica como institución educativa publica Categoría A en el sistema nacional de la Educación Superior.

En la actualidad la Universidad cuenta con los aplicativos descritos en el anexo 4 para satisfacer sus necesidades de automatización de procesos y mejorar los servicios: **Ver Anexo 4.** En donde se detalla todos los sistemas de información que se tiene en la Universidad de las Fuerzas Armadas con sus respectivas actividades, lenguajes de

programación y bases de datos (Plataformas) en lo que fueron desarrollados , con sus respectivas versiones, el estado de cada uno de ellos si están o no en producción, si son fuente solo de consulta para cuadres anteriores a la fecha, el detalle de módulos desarrollados en cada uno de estos aplicativos, el detalle de los reportes del sistema, la versión del sistema, es decir si esta fue o no actualizado y por cuantas ocasiones de acuerdo a estándares de las fases de desarrollo de software.

De igual manera se puede encontrar los niveles de soporte que deben dar cada uno de los técnicos de la Unidad de Tecnologías de la Información (UTIC) de la Universidad, que son por niveles que deben estar debidamente organizados:

Nivel 1. Es el que está en contacto con los usuarios del sistema de forma directa y que está en capacidad de dar solución a cosas triviales, es decir un soporte de primera línea, o nivel básico.

Nivel 2. Está inmerso en el grupo de Help Desk (Atención en el sitio), en donde los técnicos deben dar soporte de acuerdo al arrea de conocimiento, es más especializado y necesariamente debe tener conocimiento informático, para este nivel la Universidad dentro de los perfiles que manejan solicita mínimo de 2 años de experiencia en posiciones similares o que tenga un cierto grado de complexión en el área de desarrollo o administración de sistemas de información.

Nivel 3. Este soporte está a nivel de back-end ya que los métodos de la solución son a nivel de expertos y análisis avanzado. Tienen a su cargo a los otros técnicos encargados de dar soporte 1 y 2 y se encarga de dar solución a problemas que jamás se hayan prestado anteriormente.

- **COBIT 5**

“Es un modelo para auditar la gestión y el control de los sistemas de información de las empresas o instituciones, es decir administradores de T.I., usuarios y los administradores o auditores que estén inmersos en el proceso. El COBIT es un modelo

de evaluación y monitoreo que enfatiza en el control del negocio y las seguridades de las T.I. que abarcan controles específicos de T.I. desde una perspectiva de negocios". [13]

"COBIT significa Objetivos de Control para Tecnologías de Información y tecnologías relacionadas (Control OBjectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países del mundo, desarrollado por ISACA (Information Systems Audit and Control Association)". [14]

COBIT fue lanzado en el años de 1996 como una herramienta de gobierno de las Tecnologías de la Información y que ha ido cambiando la forma en que trabajan los técnicos dentro de una empresa. Vinculando la tecnología informática y las 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 auditores.

Este modelo se lo puede aplicar a los sistemas de información de todas las empresas, incluyendo los computadores personales y las redes de datos. Está basado en la filosofía de que los recursos de 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.

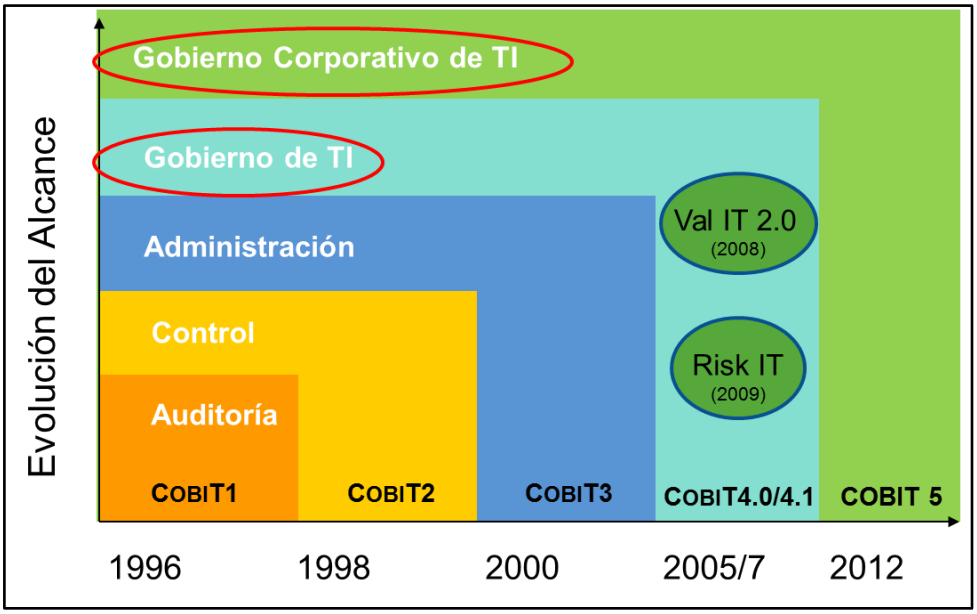


Figura 6.1. COBIT® 5(Isaca, 2012)

"Para Cobit 5 se describe 7 facilitadores / Habilitadores que son los factores que de manera individual o colectiva influyen para llegar a obtener este modelo y sobre todo que ayuda a la Gobernabilidad y la gestión de las seguridades en las Tecnologías de la Información T.I."[15]

1. Los principios, las políticas y los marcos son el vehículo para convertir el comportamiento deseado en orientación práctica para la gestión diaria.
2. Los procesos describen un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir un conjunto de resultados que sustenten el logro de las metas generales relacionadas con TI.
3. Las estructuras organizacionales son las entidades claves de toma de decisiones en una empresa.
4. La cultura, ética y el comportamiento de individuos y de la empresa son, a menudo, subestimados como un factor de éxito en las actividades de gobierno y gestión
5. La información es generalizada en cualquier organización e incluye toda la información producida y utilizada por las empresas. Se requiere la información

para mantener a la organización en funcionamiento y bien organizada, pero a nivel operativo, la información es con frecuencia producto clave de la misma empresa.

6. Los servicios, la infraestructura y las aplicaciones incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la empresa servicios y procesamientos de TI.
7. Las personas habilidades y competencias están vinculadas a las personas y son requeridas para la finalización exitosa de todas las actividades y para tomar decisiones correctas y aplicar medidas correctivas.

- **Universidad de las Fuerzas Armadas ESPE extensión Latacunga**

La Universidad de las Fuerzas Armadas "ESPE", es una institución de educación superior, con personería jurídica, de derecho público y sin fines de lucro, con autonomía académica, administrativa, financiera, orgánica y patrimonio propio. Como institución de educación superior de las Fuerzas Armadas es dependiente del Comando Conjunto de las Fuerzas Armadas en política institucional en el ámbito de educación superior, designación de autoridades ejecutivas; y asignación del personal militar necesario para el funcionamiento de la Universidad, conforme al presente estatuto.

El domicilio de la Universidad está en Quito y la Matriz principal en el Campus Sangolquí, con extensiones en Latacunga, Salinas, Guayaquil, Santo Domingo de los Tsáchilas y Galápagos; se rige por la Constitución de la República del Ecuador, la Ley Organiza de Educación Superior y su reglamento, Ley Organiza de Servicio Público, El Código de Trabajo, los reglamentos expedidos de acuerdo con la ley y normas emitidas por sus órganos de administración y autoridades.

El orden interno en la Universidad de las Fuerzas Armadas "ESPE", es de exclusiva competencia y responsabilidad de sus autoridades.

La Universidad de las fuerzas Armadas "ESPE", es una comunidad de autoridades militares y civiles, personal académico, estudiantes, personal administrativo y trabajadores. Su misión es formar académicos, profesionales e investigadores de

excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana, generar, aplicar y transferir el conocimiento; y , proporcionar e implementar alternativas de solución a los problemas del país, acordes con el Plan Nacional de Desarrollo; siendo su visión permanente ser una universidad líder en la gestión del conocimiento y tecnología en el sistema de educación superior del país, con prestigio internacional.

La Universidad de las Fuerzas Armadas "ESPE" cuenta con unidades de apoyo o soporte para la ejecución de diferentes actividades de los macro procesos de: Gestión Estratégica, Docencia, Investigación e Innovación, Vinculación con la Sociedad, Gestión de Postgrados, Gestión de talento Humano, Gestión Financiera, Gestión de Recursos Físicos, Gestión de Servicios Universitarios**, Gestión de Tecnología Informática y Comunicaciones**, gestión Jurídica, Gestión de Seguridad Integral, gestión de Mercado, Seguimiento y Mejora, Gestión de la Comunicación, Gestión Documental y otros macro procesos y procesos que sean necesarios para la administración de la universidad con flexibilidad, eficiencia y calidad.

MISION

Formar profesionales e investigadores de excelencia, creativos, humanistas con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana, generar y difundir el conocimiento y, proporcionar e implementar alternativas a los problemas del país con el plan Nacional de Desarrollo.

VISION

Líder en la gestión del conocimiento y de la tecnología en el Sistema Nacional de Educación Superior, con prestigio Internacional y referente de práctica de valores éticos, cívicos y de servicio a la sociedad.

Principios Filosóficos.

La Universidad de las Fuerzas Armadas "ESPE" conduce y desarrolla sus eventos y procesos mediante los siguientes principios:

- La Institución se debe fundamentalmente a la nación ecuatoriana; a ella orienta todo su esfuerzo contribuyendo a la solución de sus problemas mediante la formación profesional y técnica de los miembros de su población.
- Es una Institución abierta a todas las corrientes del pensamiento universal, sin proselitismo político ni religioso.

- La búsqueda permanente de la excelencia a través de la práctica de la cultura de la calidad en todos sus actos.

- La formación consciente, participativa y crítica con libertad académica y rigor científico, que comprenda y respete los derechos fundamentales del ser humano y de la comunidad.

- El cultivo de valores morales, éticos y cívicos, respetando los derechos humanos con profunda conciencia ciudadana; coadyuva a la búsqueda de la verdad y forma hombres de honor, libres y disciplinados.

- El mantenimiento de las bases históricas de la identidad nacional para incrementar el orgullo de lo que somos y así proyectamos al futuro.

- La conservación, defensa y cuidado del medio ambiente y el racional aprovechamiento de los recursos naturales; y,

- La práctica de los valores tradicionales de orden, disciplina, lealtad, justicia, gratitud y respeto, en el contexto de la responsabilidad, la honestidad, el autocontrol, la creatividad, el espíritu democrático, la solidaridad y la solución de los problemas mediante el diálogo y la razón.

Valores Institucionales

La conducta de todos y cada uno de los miembros de la comunidad politécnica, se mantendrá siempre bajo la práctica de los valores institucionales que se puntualizan a continuación.

- Honestidad a toda prueba.
- Respeto a la libertad de pensamiento.
- Orden, puntualidad y disciplina conscientes.
- Búsqueda permanente de la calidad y excelencia.
- Igualdad de oportunidades.
- Respeto a las personas y los derechos humanos.
- Reconocimiento a la voluntad, creatividad y perseverancia.
- Práctica de la justicia, solidaridad y lealtad.
- Práctica de la verdadera amistad y camaradería.
- Cultivo del civismo y respeto al medio ambiente.
- Compromiso con la institución y la sociedad.
- Identidad institucional.
- Liderazgo y emprendimiento.
- Pensamiento crítico.
- Alta conciencia ciudadana

En la actualidad la Universidad de las Fuerzas Armadas "ESPE" se encuentra el grupo de alto rendimiento categoría A. Una vez que se fusionaron la Escuela Politécnica del Ejército, la Universidad Naval "Rafael Moran Valverde", y el Instituto Tecnológico Aeronáutico.

- **Unidad de Tecnologías de la Información.**

La Unidad de tecnologías de la Información y las comunicaciones administra los recursos tecnológicos requeridos por la Institución para el manejo de la información y mantener una adecuada comunicación, para lo cual ejecuta los procesos de gestión estratégica de la tecnología informática; de soporte técnico, de administración de redes y comunicaciones; de desarrollo, implantación y mantenimiento de aplicativos; y, de administración de software.

Es responsable de:

a. Realizar la gestión estratégica de la tecnología informática;
b. Dar soporte técnico en el ámbito de aplicación que corresponde;
c. Administrar las redes y las comunicaciones;
d. Desarrollar, implantar y mantener los aplicativos;
e. Administrar los aplicativos y bases de datos;
f. Proporcionar seguridad a la información de servidores; y
g. Cumplir la normativa Institucional y las resoluciones emitidas por los órganos competentes.

La Unidad de Tecnologías de la Información y Comunicación contará con:

a. Un Director;
b. Personal administrativo, profesionales en tecnologías de información y comunicación; y,
c. Personal administrativo: de apoyo.

MISIÓN

Administrar y proveer de forma eficiente y segura los recursos y servicios de tecnologías de información y comunicaciones, de acuerdo a las necesidades institucionales y tendencias globales, cumpliendo normas y estándares internacionales.

VISIÓN

Ser reconocida como unidad estratégica de la Institución, contribuyendo al desarrollo, innovación y transferencia de Tecnologías de Información y Comunicaciones, cumpliendo normas y estándares internacionales, con responsabilidad social y del medio ambiente

Objetivos y Estrategias

- Mejorar los procesos de todas las unidades.
    - Actualizando y optimizando los procesos de la UTIC.

- Optimizar y mejorar la infraestructura física y tecnológica de la Institución.
    - Manteniendo, estabilizando y socializando el uso de los Sistemas Informáticos.
    - Apoyo tecnológico a la visibilidad y posicionamiento dentro de la web.

- Gestionar los servicios de tecnologías de información y comunicaciones en apoyo a las áreas académica, administrativa e investigación.
    - Ampliando la cobertura de infraestructura y servicios de red de la Universidad de las Fuerzas Armadas ESPE.
    - Elaborando y ejecutando proyectos de tecnologías de información y comunicaciones.
    - Elaborando políticas, normas y procedimientos para la gestión de Tic´s.

- Incorporar tecnología de última generación a los procesos tecnológicos y administrativos.
    - Actualizando e innovando los recursos de tecnologías de información y comunicaciones, de acuerdo a las necesidades de la Universidad de las Fuerzas Armadas ESPE.

En el anexo 2 podemos observar la matriz de procesos planteado para la Unidad de Tecnologías de la Información y las Comunicaciones en el cual se tiene La Gestión

Estratégica de las TI, como proceso principal acompañados de sus respectivos subprocesos, los objetivos de los subprocesos plateados, con el periodo del tiempo(periodicidad), las referencias de cada una de las actividades, así como los responsables de acuerdo a la denominación que tienen los especialistas dentro del reglamento de la institución.

La matriz con los niveles de seguridad que disponen los sistemas, están de acuerdo a las necesidades de los departamentos de la Universidad de la siguiente manera:

NIVEL A: Es considerado como de protección verificada, más avanzada ya que debe contener todo tipo de seguridad y haber pasado todos los niveles, es decir el diseño, control y verificación, mediante métodos formales para garantizar la seguridad en los procesos.

NIVEL B1: Llamado también como seguridad etiquetada es un subnivel de los niveles de seguridad de B, y soporta seguridad multinivel, así como la ultra secreta, cada usuario que ingresa a un objeto debe tener permiso expreso para poder hacerlo y viceversa, es decir que cada usuario tiene sus objetos asociados.

NIVEL B2: Es el de protección estructurada ya que se requiere que se etiquete cada objeto de nivel superior por ser el padre de un objeto inferior, un sistema debe ser capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas, y el administrador es quien debe asignar permisos y anchos de banda para sus transacciones.

NIVEL B3: Refuerza a los dominios de seguridad con la instalación de un hardware, el administrador es quien asigna memoria y utiliza el hardware para asignar a cada usuario los lugares y objetos a lo que se puede acceder.

NIVEL C1: El de Protección discrecional requiere una identificación de usuarios para tener acceso a distinta información, cada usuario puede administrar su información de

forma privada y diferenciando entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

NIVEL C2: Protección de acceso controlado, es para solucionar las posibles debilidades que pueda tener el C1, la diferencia radica que este lleva una auditoría de accesos o intentos fallidos de acceso a objetos. Requiere de una auditoría que es utilizada para llevar registros de todas las acciones de seguridad

NIVEL D: Compone solamente una división de seguridad y que está reservado para sistemas de información que han sido evaluados y que no cumplen con ninguna especificación de seguridad.

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATANCUNGA

Niveles de Seguridad en los SGBD's de los Sistemas de Información

N.	SISTEMA	SGBD	MANTENIMIENTO	AUDITORIA	VERSION	TIPO	SISTEMA OPERATIVO	HARDWARE
1	Registro de Ingresos SISRIN	Fox Pro	Nivel B3	SI	8.0	N/A	Windows 2000	Computador personal
2	Ordenes de Pago	Fox Pro	Nivel B3	NO	8.0	N/A	Windows 2000	Computador personal
3	Sistema Escolastico de Inglés para niños ESCOING	Fox Pro	Nivel B3	NO	8.0	N/A	Windows 2000	Computador personal
4	Sistemas de Control de Accesos Web Access	MySql	Nivel B3, C1	NO	4.0.24	Libre	Linux Centos	HP Proliant
5	Sistema de Gestión Escuela de Conducción	MySql	Nivel B3, C1	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
6	Plataforma Virtual MOODLE	MySql	Nivel B3, C2	SI	4.1.25	Libre	Linux Centos	HP Proliant
7	Software OTRS (Control de Recursos Informáticos)	MySql	Nivel B3, C1	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
8	Sistema ALUMNI ESPEL	MySql	Nivel B3	SI	4.1.25	Libre	Windows 2008	DELL Power Edge
9	Sistema de Gestión de Laboratorios SGLAB	MySql	Nivel B3, C1	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
10	Sistemas de Gestión de Concurso de Proyectos INNOVATE	MySql	Nivel B3	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
11	Sistema de Registro de Libros biblioteca Virtual	MySql	Nivel B3, C2	SI	4.1.25	Libre	Windows 2008	DELL Power Edge
12	Sistema de Registro de Actividades Docentes SG-RAD	MySql	Nivel B3, C1	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
13	Sistema Academico del programa ASEP Chevrolet	MySql	Nivel B3	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
14	Modulo DIM Anexos y Formularios		Nivel B3	NO		Libre		
15	Sistema de Encuestas	MySql	Nivel B3	NO	4.0.25	Libre	Windows 2008	DELL Power Edge
16	Sistema Contable Financiero Olympo	Oracle. Ms SQL SERVER	Nivel B3, C2	SI	8i, 2008	Professional	Linux Centos / Windows 2008	HP Proliant
17	Sistema de Control biométrico SQUARENET	MySql	Nivel B3, C2	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
18	Sistema de Gestión de Biblioteca SIABUC 9	PostgreSQL	Nivel B3, C2	SI	8.2	Libre	Linux Centos	HP Proliant
19	Sistema Spontania		Nivel B3	NO				
20	Sistema de Gestión de Rancho	MySql	Nivel B3	NO	4.1.25	Libre	Windows 2008	DELL Power Edge
21	Sistema de Activos Fijos SAF	Fox Pro	Nivel B3	NO	2.6	N/A	Windows 2008	DELL Power Edge
22	Sistema Academico de Carreras	Sybase - SQL Server	Nivel B3	NO	7.0	Professional	Windows 2008	DELL Power Edge
23	Sistema Academico de Idiomas	Sybase - SQL Server	Nivel B3	NO	7.0	Professional	Windows 2008	DELL Power Edge
24	Sistema de Tributación SITAC	Visual Fox Pro	Nivel B3	SI	8.0	Professional	Windows 2008	DELL Power Edge
25	Sistema de Control Biometrico MOQASIST	Visual Fox Pro	Nivel B3	NO	8.0	Professional	Windows 2008	DELL Power Edge
26	Sistema Strategic	SQL Server	Nivel B3	NO	2000	Professional	Windows 2008	DELL Power Edge
27	Sistema Contable SIGOC	Microsoft Access	Nivel B3	NO	95	Professional	Windows 2008	DELL Power Edge
28	Sistema Escolástico de la MED	Sybase - SQL Server	Nivel B3	NO	7.0	Professional	Windows 2008	DELL Power Edge

Tabla 6.1. Sistemas de Información con niveles de seguridad a nivel de SGBD - UTIC (Navas P., 2014)

6.7.Metodología

Para la metodología del proyecto se ha basado en la investigación científica, se toma en cuenta la documentación recopilada en la institución, la experiencia de los técnicos de la UTIC así como del investigador, que con esto lo que se plantea es desarrollar un guía técnica que ayude a garantizar la seguridad de la información que se genera en esa dependencia de la Universidad.

Definición del proyecto

Para la elaboración del proyecto se plantea:

Principios, Políticas y Marcos

- Este ítem es la manera como convertir lo deseado en una guía práctica para la gestión diaria de las seguridades.

Procesos

- Legal Normativo
- Panorama de Amenazas
- Tecnología
- Gobierno
- Sociocultural

Niveles de madurez de la seguridad de la Información

- Política
- Roles y responsabilidades
- Automatización
- Alcance
- Informes

Servicios, Infraestructura y aplicaciones

Personas, Habilidades y competencias

6.8.Planeamiento del Proyecto

6.8.1. Principios, Políticas y Marcos

Para la implementación de políticas de seguridad hay que prever muchos aspectos referentes a como se encuentran estructurado los comités de seguridades en la institución y cuáles serían los planes de contingencia en caso de presentarse problemas de seguridad para lo cual hay que tener en cuenta los siguientes aspectos:

- Los principios, las políticas y los marcos son el medio para convertir el comportamiento deseado en orientación práctica para la gestión diaria.

- Los procesos describen un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir en conjunto de resultados que sustenten el logro de las metas generales relacionadas con TI.

- Las estructuras organizacionales son las entidades claves de toma de decisiones en la Universidad.

- La cultura, la ética y el comportamiento de individuos y de la empresa son, a menudo, subestimados como un factor de éxito, en las actividades de gobierno y gestión.

- La información es generalizada en cualquier organización e incluye toda la información producida y utilizada por la Universidad. Se requiere de muchos datos para que funcione adecuadamente y bien administrada, pero a nivel operativo, la información es la parte medular de la Universidad.

- Los servicios, la infraestructura y las aplicaciones incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la empresa servicios y procesamiento de TI.

- Las personas habilidades y competencias están vinculadas a las personas y son requeridas para la finalización exitosa de todas las actividades y para la toma de decisiones correctas y aplicar medidas correctivas.

En base a lo expuesto sobre el modelo de COBIT se plantea la creación de comités con el personal de la UTIC que ayuden en la tarea de Gestionar la seguridad de la información:

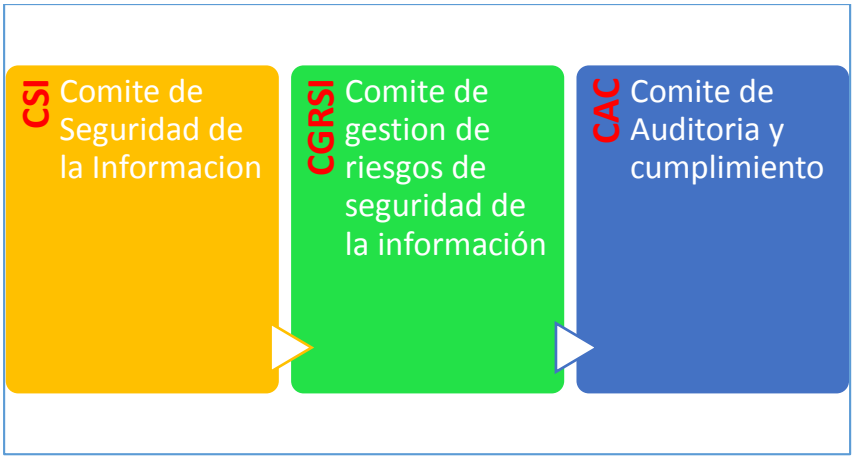


Figura 6.2. Comité de Seguridad de la Información (Navas P., 2014)

Por lo que se plantea la creación de un comité de seguridad de la información tomando en cuenta el número de equipos y usuarios que dispone en la actualidad la Universidad, y los mismos que no alcanzan para formar un comité de riesgos, teniendo en cuenta de igual manera el número reducido de personal técnico con que cuenta la UTIC, basado un análisis en consenso con la Jefe de la Unidad el comité quedaría de la siguiente manera:

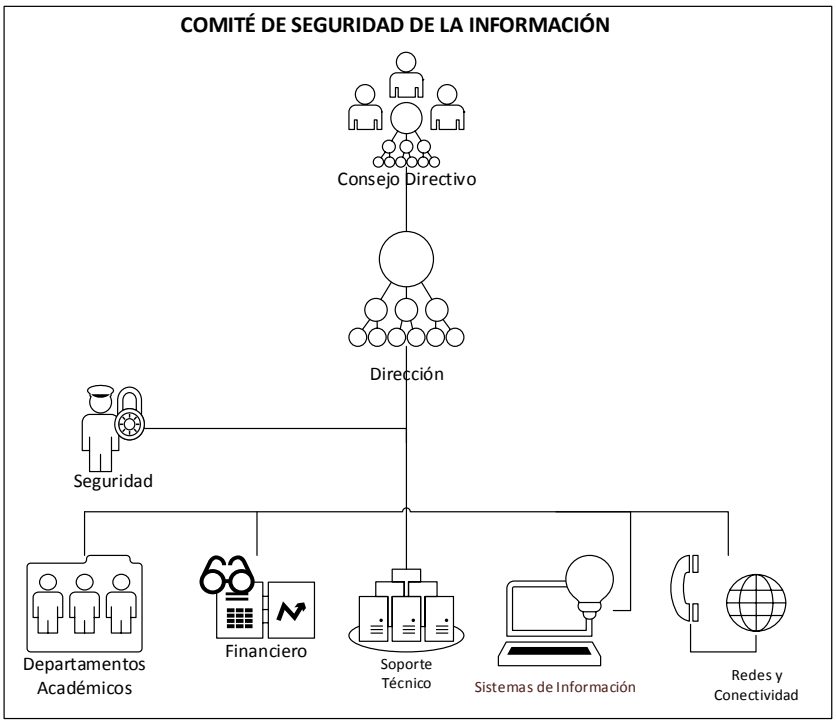


Figura 6.3. Comité de Seguridad de la Información UFA-ESPE- L (Navas P., 2014)

Dentro de los roles y las funciones que se debe cumplir para garantizar la seguridad de la información se plantea una matriz en la que se debe cumplir con las especificaciones y las normas vigentes.

TAREAS DE SEGURIDAD DE LA INFORMACIÓN	Seguridad de la Información	Bases de Datos	Redes de Datos	Soporte	Desarrollo
Administración	A	A	M	B	M
Políticas, procesos y estándares	A	A	A	A	A
Estrategia	A	A	A	B	M
Evaluación de riesgos (Definición)	M	M			B
Evaluación de riesgos (Ejecución)	M	A	A	B	A
Gestión de seguridad de la información	A	A	A	B	M
Arquitectura de seguridad	A	M	M	M	M
Tecnología de Seguridad	A	M	M	B	M
Desarrollo seguro	B	M	B	B	A
Operaciones y entrega de servicios	M	A	B	A	B
Gestión de proyectos	M	A	A	A	B
Auditoría, revisión y monitorio	A	M	A	M	M
Respuesta a incidentes	A	A	A	A	M
Entorno legal y normativo	A	A	A	A	A
Conocimiento, educación y capacitación	A	A	A	A	A
Nomenclatura: **A:** Alta **M:** Media **B:** Baja					

Tabla 6.2. Roles y Seguridades en la UTIC (Navas P., 2014)

Procesos

Los procesos tienen la propiedad de describir un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir un conjunto de resultados respaldando el logro de las metas generales relacionadas con TI. La Administración de seguridad de la información plantea unos procesos de seguridades que están basado en 21 componentes:

1. Seguridad de la aplicación
2. Criptografía
3. Monitoreo
4. Gestión de incidentes
5. Seguridad académica en línea
6. Gestión de Software malicioso (malware).
7. Protección de datos
8. Ciclo de vida del desarrollo de software
9. Gestión de proveedores (terceros)
10. Planificación de continuidad del negocio
11. Privacidad
12. Gestión de identidades y acceso
13. Gestión de riesgos
14. Seguridad física
15. Concientización
16. Gobierno
17. Política
18. Gestión del ciclo de vida de los activos
19. Rendición de cuentas y propiedad
20. Configuración del sistemas
21. Seguridad de la red.

Principios de seguridad de la Información de la Universidad de las Fuerzas Armadas según COBIT 5

PRINCIPIO	OBJETIVO	DESCRIPCION	ESTADO	EVIDENCIA
1. Soporte a la Universidad				
Concentrarse en la Administración	Garantizar que la seguridad de la información esté integrada a las actividades del negocio	Las personas que integran la continuidad de seguridad de la información complementen el negocio con claves y procesos de gestión de riesgos. Ellas deberían adoptar un enfoque de consultoría respecto de la seguridad de la información brindando su respaldo a los objetivos institucionales planteados por la Universidad por medio de la asignación de recursos, programas y proyectos. Se debe proporcionar consultorías de alto nivel, enfocadas a la institución, para proteger la información y ayudar a gestionar el riesgo de la información tanto ahora como en un futuro.		Estrategia de Seguridad de la información
Ofertar calidad y valor a los usuarios de los sistemas de información.	Garantizar que la seguridad de la información ofrezca valor y satisfaga los requerimientos de la Universidad.	Las partes interesadas tanto internas como externas deben estar comprometidas a sostener una comunicación periódica de modo que se sigan cumpliendo los requerimientos cambiantes de seguridad de la		Estrategia de Seguridad de la información

		información. Promover el valor de la seguridad de la información financiera como académica permitiendo tomar decisiones a los directivos que a su vez permitan colaborar con el éxito de la visión para la seguridad de la información.		
Cumplir los requerimientos legales y regulatorios relevantes.	Garantizar que se cumpla las obligaciones legales, que se gestionen las expectativas de las partes interesadas, y que se eviten sanciones civiles o penales.	Se deben identificar las obligaciones de cumplimiento, se las debe traducir en requerimientos específicos de seguridad de la información y comunicar a las autoridades de la Universidad. Las sanciones asociadas al incumplimiento deben ser claramente comprendidas. Los controles deber ser monitoreados, analizados y actualizados de modo que cumplan con los requerimientos legales y regulatorios nuevos o actualizados.		Estado de cumplimiento de ISO 27001
Proporcionar datos exactos y oportunos sobre el ejercicio de la seguridad de la información	Apoyar los requerimientos de la Universidad y tener una buena gestión de los riesgos de la información.	Los requerimientos para la entrega de datos sobre el desempeño de la seguridad de la información deben estar claramente definidos y sustentados con las métricas más relevantes y adecuadas (cumplimiento, incidentes, estado de		Informe mensual de gestión de la seguridad de la información

		control y costos) y alineados con los objetivos de la Universidad. La información debe obtenerse de manera periódica, uniforme y rigurosa par que continúe siendo precisa y los resultados pueden presentarse para cumplir los objetivos de las partes interesadas que correspondan.		
Evaluar las amenazas actuales y futuras hacia la información	Analizar y evaluar las amenazas emergentes de seguridad de la información de modo que se pueda adoptar acciones oportunas e informadas para mitigar el riesgo	En la actualidad las tendencias más importantes y las amenazas específicas a la seguridad de la información se deben categorizar en un marco integral estándar que abraque un amplio espectro de temas como son los aspectos políticos, legales, económicos, socioculturales y técnicos. Las personas deben compartir y profundizar sus conocimientos sobre las amenazas venideras a fin de abordar proactivamente sus causas, en lugar de sus síntomas.		Revisión y pruebas periódicas a la seguridad de la información
Promover la mejora continua en seguridad de la información	Reducir los costos, mejorar la eficacia y la eficiencia y promover una	Los modelos deben estar en constante cambio dentro de la Universidad al tratarse de un centro de estudios e investigación, y que junto		Indicador clave del desempeño, estos informes deben ser presentados mensualmente y

	cultura de mejora continua en seguridad de la información.	con las amenazas en evolución, exigen la adaptación de técnicas de seguridad de la información y la mejora continua de su nivel de eficacia. Se debe mantener el conocimiento sobre las técnicas de seguridad de la información más recientes aprendiendo de los incidentes y vinculándose con organizaciones de investigación independientes.		anualmente de acuerdo a la gestión.
2. Defensa de la Institución				
Adoptar un enfoque basado en el riesgo	Garantizar que el riesgo sea tratado de una manera consistente y eficaz	Se debe examinar las opciones para abordar el riesgo vinculado con la información de modo que se puedan tomar decisiones fundamentales y documentadas sobre el tratamiento del riesgo implica elegir una o más opciones, que habitualmente incluyen: • Aceptar el riesgo (El jefe de la UTIC, debe aprobar que ha aceptado el riesgo y que no se requiere ninguna acción). • Evitar los riesgos decidiendo que no se persiga una iniciativa en particular		Sistema de gestión de seguridad de la Información SGSI y la evaluación de riesgos

		• Transferir los riesgos, en la actualidad se tiene el cyberoam, pero no es la solución sino más bien tercerizar las seguridades a una empresa sería lo ideal particularmente los sistemas ERP Académico. • Mitigar el riesgo siempre que se apliquen las medidas adecuadas de seguridad de la información, mediante controles de acceso, monitoreo de red y gestión de incidentes.		
Proteger información clasificada	Evitar la divulgación de la información clasificada, que hay que tener en cuenta que se trata de una unidad militar a parte de Universidad	La información se debe identificar y luego clasificar de acuerdo a su nivel de confidencialidad, entre las que se tiene la clasificada como secreta, restringida, interna y pública. La información confidencial se debe proteger en todas sus etapas de su ciclo de vida, a partir de la creación y hasta su destrucción, empleando los controles que correspondan, como la encriptación y las restricciones de acceso.		Políticas y estándares de seguridad de la información
Concentrase en aplicaciones	Priorizar la escasez de recursos de	Comprender el impacto que puede tener en la Universidad que		Políticas y estándares de seguridad de la información

críticas de la Universidad	seguridad de la información protegiendo las aplicaciones de la universidad sobre las que un incidente de seguridad de la información podría tener el mayor impacto en la institución.	ocasionaría una falta de integridad o disponibilidad de información importante manipulada por las aplicaciones de la institución, mismas que pueden ser procesadas, almacenadas o transmitidas, ayudara a establecer el nivel de criticidad. Posteriormente, pueden determinarse los requerimientos de recursos de seguridad de la información y puede establecerse la prioridad de proteger las aplicaciones que son más críticas para el éxito de la organización.		
Desarrollar sistemas seguros	Desarrollar sistemas de calidad y económicos en los cuales se pueda confiar, es decir aquellos que sean consistentemente seguros, precisos y sobre todo que tengan un alto grado de confiabilidad.	La seguridad de la información debe ser integral para las fases de alcance, diseño, desarrollo y prueba del ciclo de vida de desarrollo de sistemas. Las buenas prácticas de seguridad de la información deben estar medidas por una prueba de rigurosidad de debilidades en cuanto a la seguridad de la información, la revisión entre pares, y sobre todo la capacidad de lidiar errores, excepciones y condiciones de emergencia, todas estas deben tener un rol		Estándares de seguridad de la información

		fundamental en todas las etapas del proceso de desarrollo.		
3. Promover un comportamiento responsable respecto de la seguridad de la información.				
Actuar de una manera profesional y ética	Asegurar que las actividades relacionadas con la seguridad de la información se realicen de manera confiable responsable y eficiente.	La seguridad de la información se basa en la capacidad de los profesionales que tenga una institución ya que de ellos depende del éxito o fracaso de la precautelación de la información, ya que es el llamado a realizar sus funciones con responsabilidad y con un claro entendimiento del modo en que su integridad impactara directamente sobre la información que se les encarga proteger. Los profesionales de seguridad de la información tienen que tener el compromiso con un alto nivel de calidad en su trabajo y demostrar, a la vez, un comportamiento uniforme y ético y respeto por las necesidades de la empresa, otras personas y la información confidencial que en ocasiones son a titulo personal.		Verificación de antecedentes
Promover una cultura positiva respecto de la seguridad de la información	Ejercer una influencia positiva respecto de la seguridad de la	Se debe hacer énfasis en lograr que la seguridad de la información sea una pieza clave de la Universidad y que los		Reuniones del comité de seguridad de gestión de la seguridad de la información SGSI,

	información sobre el comportamiento de los usuarios finales, reducir la probabilidad de que ocurran incidentes de seguridad de la información y limitar su posible impacto en la Universidad.	usuarios se concienticen cada vez más sobre la seguridad de la información y en garantizar que estos tengan las destrezas necesarias para proteger la información clasificada o crítica y los sistemas. Las personas deben reconocer el riesgo que corre la información que tienen en su poder y deben estar facultados para tomar las medidas que sean necesarias para protegerla.		propuesto en el proyecto.

Tabla 6.3: Principios de seguridad de la Información de la Universidad de las Fuerzas Armadas según COBIT 5 (Navas P., 2014)

Niveles de madurez de la Seguridad de la Información.

Se creó un modelo de madurez de seguridad de la información, que está definido básicamente por cinco niveles, de igual manera para garantizar la seguridad se han definido ocho atributos para los componentes del aseguramiento de la información.

El seguimiento de cada uno de los componentes se basa en este modelo, que la Universidad de las Fuerzas Armadas ESPE extensión Latacunga debe utilizar según el modelo de madurez para obtener unos resultados adecuados y de esta manera construir el concepto del benchmarking (proceso sistemático y continuo del producto) dentro de la institución. Esta Guía técnica permite detectar áreas que requieren mejoras y los ejercicios de evaluación deben ser evaluadas en un taller entre todos los implicados:

Autoridades, Técnicos, usuarios de los aplicativos, de esta manera se podrá demostrar que existe una comunicación saludable entre todos los implicados en asegurar la información que esto derivara en un sentido de participación y transparencia respecto de la misión, visión y objetivos institucionales.

Está guía técnica se utilizará estrictamente para análisis de brechas internas y para identificar áreas de mejoras. Es importante hacer notar que el proyecto fue pensado en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, y que no podrá ser prenda de garantía para aseguramiento de la información de terceros, empresas o instituciones ajenas a la realidad de esta institución.

El modelo de madurez que se plantea a continuación es creado con la finalidad de que se cree urgentemente el ya planteado SGSI institucional, para la satisfacción de sus necesidades exclusivas de definición de planes de mejoras específicas. Este modelo de madurez además de estar basado en COBIT toma las mejores prácticas del modelo de Aseguramiento de procesos y en la norma ISO/IEC 15504.

Modelo de madurez de la seguridad de la información

Columna 1	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Inicial	En desarrollo	Definido	Gestionado	Optimizado
Política	Ausencia de política	Política limitada	N/A	Tramites	Limitado
Roles y responsabilidades	No definida	No definida	No definida	En tramites	N/A
Automatización	Manual	Regular	Baja	Ninguna	N/A
Alcance	No implementado	Limitado	Normal		
Eficacia	N/A	Poca	Poca	Avanzado	Mínima
Gestión de incidentes	Sin seguimiento	Ninguna			Avanzada
Medición	Sin medición	Bajo control	Poca	Media	Ninguna
Informes	Sin informes	Controlado	N/A	Avanzada	Bajo
Nomenclatura: **N/A:** No Aplica					

Tabla 6.4: Modelo de madurez de la Seguridad de la información (Navas P., 2014)

Servicios, infraestructura y aplicaciones.

Los servicios, la infraestructura y las aplicaciones incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la Universidad los servicios y procesamientos de TI.

La Universidad de las Fuerzas Armadas ESPE extensión Latacunga emplea cinco tecnologías diferentes, alrededor de estas tecnologías se desarrollan distintos servicios, infraestructuras y aplicaciones. Como se pudo observar en la matriz de madurez de la seguridad de la información. Lo que se debe es realizar una adecuada actualización continua del nivel de madurez, que tenga en cuenta atributos tales como la automatización, la eficacia, la gestión de incidentes y la medición,

garantiza un monitoreo muy pormenorizado de los servicios. Todos los proyectos que sean planteados para la Universidad deberán cumplir con las matrices planteadas para mejorar la calidad de las seguridades y prestaciones de la información para obtener una mejor fuente de consulta y reportes agiles y oportunos.

Información

La información es generalizada en cualquier institución y está a la vez incluye todos los datos producidos y utilizados por la Universidad, se requiere de la información para poder mantener a la institución en funcionamiento y bien gobernada, pero esto se lo debe realizar a nivel operativo, la información es el producto clave de la misma.

La información confiable es un factor clave para la gestión de la seguridad. Generalmente la información se presenta por medio de documentos de entes superiores o desde la matriz, pero en esos casos los términos de estrategia, presupuesto, plan y políticas son las que influyen en la elaboración de aplicativos que ayuden a la administración. Los requerimientos de seguridad de la información se obtienen por medio de un formulario de aceptación de riesgos y estos serán sometidos a una revisión del comité de la gestión de seguridad de la información SGSI, que se planteó en este proyecto. Este debe ser preparado de acuerdo al formato planteado, los informes de revisión de seguridad de la información incluyen hallazgos de auditoría, informes de madurez, análisis de amenazas, informes de vulnerabilidades, registros de riesgo de la información, informes de brechas e informes de incidentes y problemas relacionados con la seguridad de la información.

Para la guía técnica se debe tomar muy en cuenta el modelo de madurez el cual nos proporciona entradas adicionales para la información de buena calidad. Se han creado varias métricas y mediciones de seguridad de la información basadas en el

marco de la norma ISO 27004 que define los procesos para auditoría Informática, que sus prácticas están resumidas en COBIT , el cual está tomado en cuenta de igual manera en algunos puntos del cuadro de mando de la institución desde el año 2012.

Personas, habilidades y competencias

Las personas, las habilidades y las competencias están ligadas a los técnicos y autoridades de la UTIC y que son requeridas para la finalización exitosa de todas las actividades y que sirven para tomar decisiones correctas y aplicar medidas correctivas.

El proyecto plantea una serie de técnicas para crear conciencia sobre la seguridad y desarrollar habilidades y competencias dentro del staff de técnicos de la Unidad de Tecnologías de la Información y las Comunicaciones.

Red de Seguridad

La red de seguridad se encuentra albergando todo lo relevante como políticas, estándares, guías, planes de continuidad, etc.

El esquema propuesto en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, son los que tienen que trabajar en miras de precautelar las seguridades de la infraestructura tecnológica.

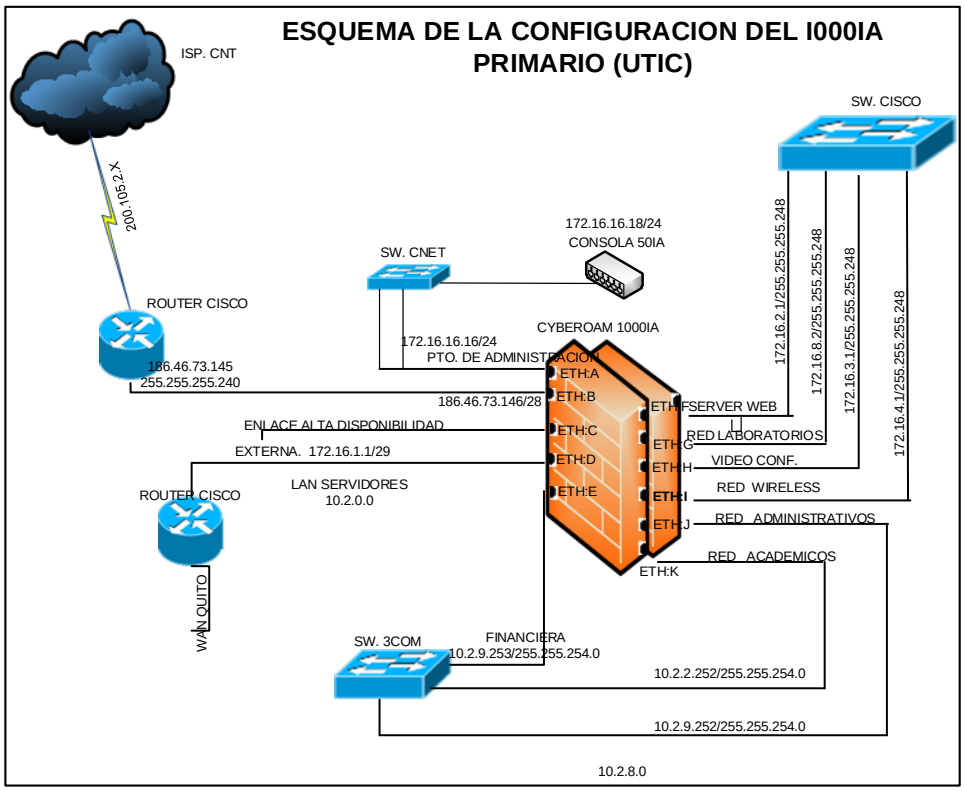


Figura 6.4: Esquema de la configuración del IOOOIA PRIMARIO UTIC (Navas P., 2014)

Para garantizar este modelo se debe tener como política la creación de áreas físicas seguras que garanticen la seguridad de la información, resguardando los activos que se encuentran dentro del perímetro universitario de seguridad física y del entorno ambiental, con la utilización de las redes inalámbricas.

El comité de Seguridad planteado debe establecer seguridades dentro de las cuales se deberá proteger los activos que procesen información. El perímetro de seguridad como se lo ha llamado deberá ser un espacio con límites y restricciones claramente definidas.

Dentro de la propuesta se menciona el trato con terceros y los servicios que estos deben prestar y cómo podemos garantizar la confidencialidad, esto se debe dar de acuerdo a una revisión y monitorización al cumplimiento de acuerdos establecidos

entre la Universidad y la empresa contratada para garantizar que los servicios entregados cumplan con las políticas de seguridad establecidas por la Institución.

Con esto lo que estamos consiguiendo es que le nivel de seguridad de la información de los servicios que prestan los proveedores externos cumplan con las exigencias de la Universidad, y mitigar al máximo los posibles riesgos, y cumplan con los acuerdos de privacidad previamente acordado.

Se deberá verificar que las seguridades, los niveles de entrega y las definiciones de los servicios sean implementados, y que éstos sean los adecuados y siempre respetando las políticas institucionales. Las empresas que hacen outsourcing, de igual manera deberán tener un perfil de auditoría para precautelar la información y las actividades que realizaren los proveedores dentro de la institución.

Para poder alcanzar la redundancia en la seguridad de la infraestructura tecnológica de la universidad se plantea una alternativa de aseguramiento con otro equipo redundante del primero, con esto si fallara la primera opción, el segundo subiría sus servicios y no alteraría de ninguna manera las actividades, ni de los técnicos ni de los usuarios y sin pérdida de tiempo y otros recursos seguiría el funcionamiento.

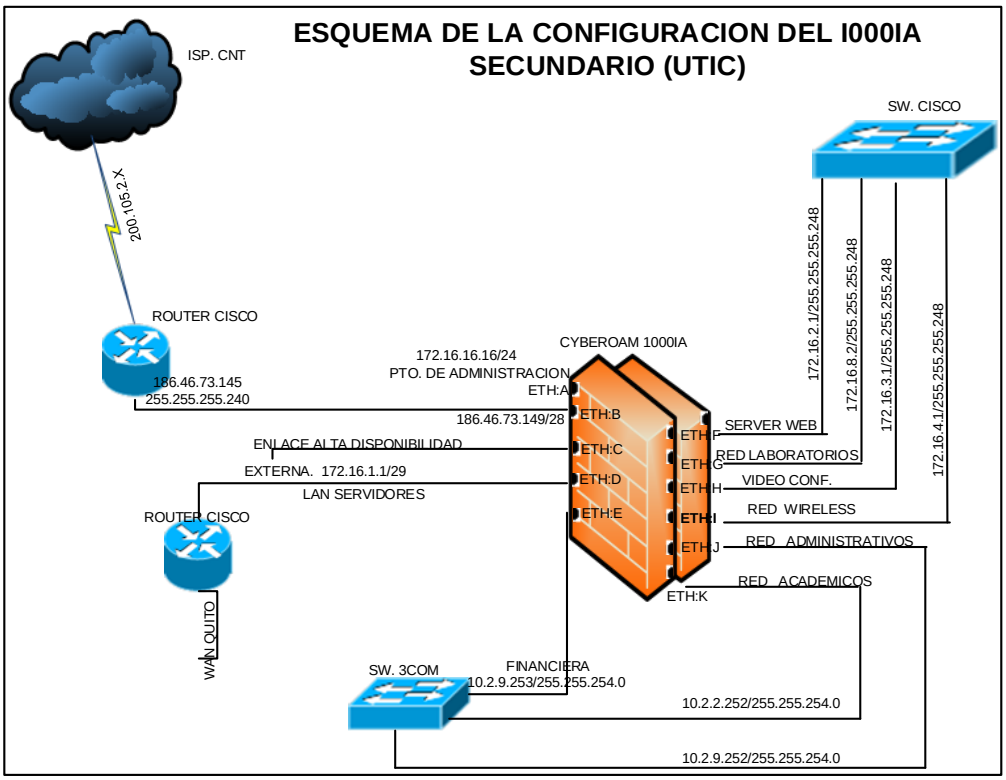


Figura 6.5: Esquema de la configuración del IOOOIA SECUNDARIO UTIC (Navas P., 2014)

Planificación y aprobación de Sistemas (Aplicativos).

Para la planificación se debe tener como política, la planificación, preparación y proyección de requerimientos a futuro para la disponibilidad y capacidad de los recursos óptimos para el desarrollo de la Universidad.

Analizar y sobre todo documentar los requerimientos operacionales de los futuros usuarios de nuevos sistemas antes de proceder con su diseño, desarrollo e implementación.

Con estas actividades lo que se pretende es reducir el riesgo de potenciales fallas en los sistemas de información institucionales cuando están en producción. Monitoreando los recursos existentes y realizando proyecciones a futuro de los

requerimientos de capacidad para el desarrollo, en estas proyecciones se debe tomar en cuenta la posibilidad de nuevas actividades de la Universidad, requerimientos adicionales del sistema y las tendencias tecnológicas.

Se deberá tener en cuenta los recursos sensibles o de mayor costo para la Universidad, identificando y previniendo los puntos de falencia y determinar al personal indispensable requerido para la adecuada operatividad de los sistemas. Acordando, estableciendo y documentando los criterios de aceptación y actualización para el desarrollo de nuevos aplicativos, los mismos que serán probados durante el desarrollo y antes de la aceptación formal del sistema.

Deberán ponerse en producción los sistemas de información solamente después de la aceptación formal del comité del SGSI (Seguridad en la Gestión de los Sistemas de Información), las actualizaciones deberán ser verificadas por el Administrador de Sistemas de Información y en caso de generar duda alguna de ellas deberá ser puesto en conocimiento del comité, todas las aceptaciones deberán ser documentadas y firmadas en las áreas que estén involucradas, tomando en cuenta:

- Requisitos técnicos del desempeño del sistema
- Procedimientos de recuperación de errores y planes de contingencia
- Preparación y pruebas de procedimientos operativos
- Controles de seguridad acordados con el comité de SGSI.
- Manuales de procedimientos
- Planes de continuidad

Se deberá asegurar por parte del comité que la instalación del nuevo sistema no podrá incidir de ninguna manera en aplicativos anteriores que tengan que ver o no

con el propuesto. Tomar en cuenta las medidas de aseguramiento de la información ha sido tomado en cuenta para la puesta en producción de los nuevos sistemas.

Se debe planificar en conjunto con todas las áreas que intervinieron en el desarrollo del sistema y con los usuarios del mismo para recibir el entrenamiento y capacitación para la operación y uso de nuevos sistemas que incluyan los controles adecuados para evitar el error de los usuarios, mostrando el proceso de desarrollo de los aplicativos en todas sus etapas.

Con la finalidad de garantizar, se debería monitorear los sistemas de información y registrar todos los eventos en logs y demás datos que generen los sistemas de información con la finalidad de precautelar el procesamiento.

Revisar que los controles implementados sean los efectivos y que las políticas de seguridad de la información se están cumpliendo de una manera adecuada, detectando las actividades no autorizadas o que no cumplan con los objetivos planteados por el SGSI para el procesamiento de la información.

Todos los logs que se van a generar deberían estar registrados en un log de auditoría, almacenando lo siguiente:

- El nombre del usuario
- Hora y fecha de cada actividad de los usuarios en el sistema
- Detallar el evento a realizar, excepción o evento de seguridad de la información como inicio y finalización de la sesión del usuario o identificación del servidor o estación de trabajo.
- Si existe la posibilidad se debería registrar la ubicación o los intentos fallidos de acceso al sistema o a otros recursos.

- Acciones de eliminación, actualización o altas de registros deben ser registrado en algún log del sistema.
- Los logs de auditoría no podrán ser borrados jamás y bajo ningún concepto se podrá alterar la información que ahí se almacene.
- Para todas las actividades el comité de gestión de seguridad de la información, determinara el nivel de auditoría que se requiere para verificar actividades en los usuarios, los accesos y todas las propiedades que se quieran utilizar en las aplicaciones.

- Los sistemas de alertas o fallas deberán incluir: los mensajes de alerta, excepciones de logs del sistema, alarmas de manejo de la red, alarmas en actividades por sistemas de control de acceso.

- Como los archivos de los logs van a contener abundante información, se debe analizar la información importante y sacar un respaldo en otro sitio para poder ser utilizada en herramientas de auditoría.

- Para controlar los accesos a las aplicaciones y a la información, debemos restringir el acceso lógico a los datos y el software de aplicaciones, evitando de esta manera el ingreso no autorizado a los datos de los sistemas de información.

APLICACIÓN DE LA GUÍA TÉCNICA EN LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSIÓN LATACUNGA PARA EL PROCESO DE SEGURIDADES PREVENTIVAS A SISTEMAS DE INFORMACION Y BASES DE DATOS.

a. OBJETIVO

Planificar, organizar, dirigir, evaluar y retroalimentar las actividades estratégicas para la implementación de los servicios de TIC´s e implementar las acciones de seguridad preventivas, disuasivas y reactivas que permitan proteger la información dentro de la Comunidad Universitaria.

b. ALCANCE

Inicia con el análisis de la situación actual y finaliza con la seguridad de la información.

c. RESPONSABLE

Planificador y Administrador de Proyectos TIC´s

d. REQUISITOS LEGALES

- Plan Estratégico Institucional
- Reglamento Orgánico de la ESPE
- Normas Técnicas Informáticas de la Contraloría General del Estado
- Plan Operativo Anual de la ESPE
- Reglamento General Sustitutivo para el manejo y administración de Bienes del sector público.
- Instructivo para el Manejo, Fijación de Plazos de Conservación y Transferencia Documental, según la Orden de Rectorado No. 2009-288-ESPE-a-3.

e. POLÍTICAS INTERNAS

- Revisión y actualización de la tecnología existente de los recursos y servicios de TIC´s
- Para el Subproceso Seguridad de la Información se aplicarán las políticas siguientes, puesto que no tiene diagrama de flujo:
    - Los administradores de los servicios y aplicaciones son los responsables de generar los respaldos de la información de cada uno de los servicios y aplicaciones.
    - Se llevará un registro cronológico mensual de la información de las bases de datos, el mismo que reposará en la Secretaría de la UTIC.
    - Se llevará un registro cronológico semestral de la información de los aplicativos y/o configuraciones de servicios críticos, el mismo que reposará en la Secretaría de la UTIC.
    - Los respaldos físicos de bases de datos, aplicativos y/o configuraciones de servicios críticos

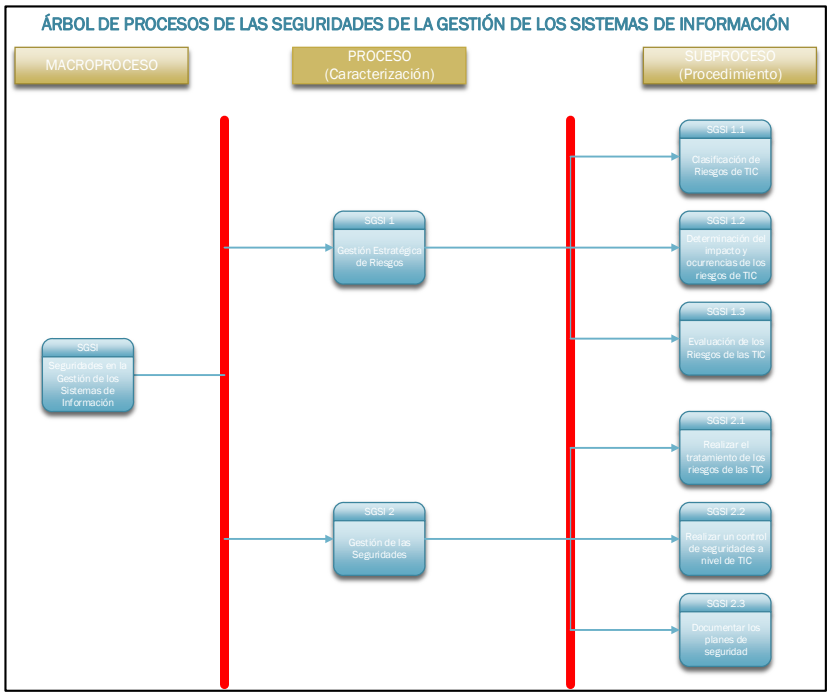


Figura 6.6: árbol de procesos de las seguridades (Navas P., 2014)

f. SUBPROCESOS

Asegurar la disponibilidad y la integridad de los datos en los sistemas de Información de la Universidad, como se puede observar en el siguiente cuadro:

RESPONSABLE	La Unidad de tecnologías de la Información y las Comunicaciones
ALCANCE	Inicia: Con la solicitud de verificación de la información Termina: Con la evaluación de las Seguridades
OBJETIVO	Asegurar la disponibilidad y la integridad de los datos en los sistemas de Información de la Universidad
INDICADOR	Ver Indicadores
REQUISITOS LEGALES	**REQUISITOS SEGÚN LA NORMA**
• Ley Organiza de Educación Superior. • Normas técnicas Informáticas de la Contraloría General del Estado. • Reglamentos y normas generales del Gobierno. • Reglamento institucional • Políticas de la Guía Técnica del Aseguramiento de los Datos.	• Infraestructura tecnológica • Planificación del proceso • Determinación de los requisitos • Revisión de los requisitos relacionados • Planificación del diseño y desarrollo • Elementos de entrada para el diseño y el desarrollo • Resultados • Revisión de los resultados • Verificación • Validación • Control de la producción y de la prestación del servicio • Validación de la producción y de la prestación del servicio • Seguimiento y Aseguramiento de los procesos
RECURSOS CRITICOS	**HERRAMIENTAS**
Recurso Humano Recurso Tecnológico Recursos Financieros	Mejora Continua Lista de revisión y aprobación de documentos Lista maestra de registros

Recursos de Infraestructura			
PROVEEDOR	**ENTRADA**	**PROCESO**	**SALIDA**
• Director • Desarrollo Institucional • Empresas de TIC´s • Comunidad Universitaria	Garantizar que la seguridad de la Información esté integrada a las actividades de la Universidad.	Adoptar un enfoque de consultoría respecto de la seguridad de la información brindando su respaldo a los objetivos institucionales planteados por la Universidad por medio de la asignación de recursos, programas y proyectos.	Estrategia de Seguridad de la Información (No Cumple)
• Personal de técnicos de la UTIC	Ofertar calidad y valor a los usuarios de los sistemas de información.	Los actores internos como externos de la Universidad deberán estar comprometidos a sostener una comunicación periódica de modo que se sigan cumpliendo los requerimientos cambiantes de seguridad de la Información.	Estrategia de Comunicación para garantizar la Seguridad de la Información (Cumple)
• Director • Desarrollo Institucional • Contraloría General del Estado • CEAACES • Comunidad Universitaria	Garantizar el cumplimiento de las obligaciones legales, que se gestionen las expectativas de las partes interesadas, y que se eviten sanciones.	Identificar las obligaciones de cumplimiento, se las debe traducir en requerimientos específicos de seguridad de la información y comunicar a las autoridades de la Universidad. Las sanciones asociadas al incumplimiento deben ser claramente comprendidas.	Estado de Cumplimiento de procesos. (Cumple Parcialmente)
• Director • Personal técnico de la UTIC • Comunidad Universitaria	Apoyar los requerimientos de la Universidad y tener una buena gestión de los riesgos de la información	Los requerimientos para la entrega de datos sobre el desempeño de la seguridad de la información deben estar claramente definida y sustentada con las métricas más relevantes, adecuadas y alineados con los objetivos de la Universidad.	Informe Mensual de Gestión de la Seguridad. (No Cumple)
	Analizar y evaluar las amenazas emergentes de seguridad de la	Las amenazas específicas a la seguridad de la información se deben categorizar en un marco integral estándar que abarque	Revisión y pruebas periódicas a la Seguridad de

• Personal técnico de la UTIC	información de modo que se pueda adoptar acciones oportunas e informadas para mitigar el riesgo.	un amplio espectro de temas como son los aspectos políticos, legales, económicos, socioculturales y técnicos.	la Información. (No Cumple)
• Director • Desarrollo Institucional • Contraloría General del Estado • CEAACES • Comunidad Universitaria	Reducir los costos, mejorar la eficacia y la eficiencia y promover una cultura de mejora continua en seguridad de la información.	Los modelos deben estar en constante cambio dentro de la Universidad al tratarse de un centro de estudios e investigación, y que junto con las amenazas en evolución, exigen la adaptación de técnicas de seguridad de la información y la mejora continua de su nivel de eficacia.	Indicador clave del desempeño, informes presentados mensualmente y anualmente de acuerdo a la gestión. (Cumple Parcialmente)

Tabla 6.5: Subproceso de Aseguramiento de la Información (Navas P., 2014)

g. INFORMACIÓN CUANTITATIVA

SUBPROCESO	VOLUMEN		TIEMPO PROMEDIO (minutos)
	CANTIDAD	UNIDAD	
Gestión de Proyectos y requerimientos de TIC	1	Proyecto	259200
	1	Adquisición	27000
Gestión de Riesgos de TIC	6	Solicitud	129600
Seguridad de la Información	1	Monitoreo ejecutado en BD	1440

Tabla 6.6: Información Cuantitativa (Navas P., 2014)

APLICACIÓN DE LA GUÍA TÉCNICA EN LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSIÓN LATACUNGA PARA EL PROCESO DE SEGURIDADES PREVENTIVAS A SISTEMAS DE INFORMACION Y BASES DE DATOS.

a. OBJETIVO

Administrar los aplicativos (Sistemas Informáticos) de la Institución, con la finalidad de garantizar su disponibilidad y funcionamiento adecuado, así como la integridad, confidencialidad y seguridad de la información almacenada en la Base de Datos.

b. ALCANCE

Inicia con la recepción del aplicativo, una necesidad, problema detectado o con el monitoreo, y concluye con la verificación de que el aplicativo se encuentra funcionando correctamente.

c. RESPONSABLE

Especialista en Tecnología de Información y Comunicación.

Desarrollador de Sistemas de Información de la UTIC

d. REQUISITOS LEGALES

- Leyes Nacionales
- Reglamentos Institucionales
- Órdenes de Rectorado
- Directivas

e. POLÍTICAS INTERNAS

- Los funcionarios seleccionados para la administración de aplicativos o bases de datos deben cumplir con requisitos de conocimientos, así como un elevado nivel de valores morales (honestidad, ética, responsabilidad, etc.).

- Los responsables de los aplicativos así como de las base de datos deberán realizar el monitoreo del funcionamiento adecuado de dichos ítems.
- Se deben realizar pruebas de funcionamiento a las actividades técnicas que lo requieran.

f. SUBPROCESOS

El proceso de Administración de Aplicativos y Base de Datos tiene los siguientes subprocesos:

PROVEEDOR	ENTRADA	SUBPROCESO	OBJETIVO	PRODUCTO / SERVICIO / RESULTADO	CLIENTE	PERIODICIDAD
Proceso: Desarrollo, Implantación y mantenimiento de Aplicativos. Subproceso: Atención a solicitud de Aplicativos	Aplicativo Necesidad o problema detectado	Administración de aplicativos	Mantener operativos los aplicativos de la universidad	Aplicativo funcionando adecuadamente(monitoreo)	Comunidad Universitaria	Diaria (Cumple)
Subproceso: Seguridades en bases de datos	Necesidad de seguridades	Administración de seguridades	Garantizar el aseguramiento de la información en los SGBD	Resultado de la solicitud	Comunidad Universitaria	Diaria (Cumple parcialmente)
Subproceso: Asistencia Técnica	Solicitud	Atención a solicitud de aplicativos	Resolver las solicitides de usuarios reportadas por soporte técnico	Resultado de la solicitud	Comunidad Universitaria	Diaria (Cumple)
Comunidad Universitaria	Necesidad de almacenamiento en bases de datos	Administración de bases de datos	Garantizar el funcionamientocorrecto y disponibilidad de las bases de datos así como la integridad, confidencialidad y seguridad de la información almacenada en la misma	Bases de datos funcionando correctamente (monitoreo)	Comunidad Universitaria	Diaria (Cumple)
Jefe Financiero	Requerimiento	Administración sistemas contables		Sistema modificado	Comunidad Universitaria	Diaria (Cumple)

Tabla 6.7: Subproceso Actualización de procesos (Navas P., 2014)

h. REGISTROS CONTROLADOS

REGISTRO	UBICACIÓN	RECUPERACION		RETENCIÓN	DISPOSICIÓN
		ORDEN	ACCESO		
Sistema	Equipo Servidor - UTIC	Configurable	Abierto	Indefinida	
Bitácora	Equipo Servidor - UTIC	Configurable	Abierto	Indefinida	
Memorando(Disponiendo actualización del Sistema Contable)	Unidad Financiera	Cronológico Numérico	Abierto	Un año	Archivo General
Notificación de actualización del Sistema Contable	Unidad Financiera	Cronológico Numérico	Abierto	Un año	Archivo General

Tabla 6.8: Registros controlados (Navas P., 2014)

i. INFORMACIÓN CUANTITATIVA

SUBPROCESO	VOLUMEN		TIEMPO PROMEDIO (minutos)
	CANTIDAD	UNIDAD	
Administración de aplicativos	1	Monitoreo ejecutado en aplicativos	80
Diagnóstico y solución de problemas	6	Solicitud	15
Administración de bases de datos	1	Monitoreo ejecutado en BD	80
Administración y mantenimiento de sistema contable		Sistema modificado	

Tabla 6.9: Información Cuantitativa de la Actualización de aplicaciones (Navas P., 2014)

j. INSTRUCCIONES ACLARATORIAS

SUBPROCESO ADMINISTRACION Y MANTENIMIENTO DEL SISTEMA CONTABLE EN EL DEPARTAMENTO FINANCIERO.

Identificar o receptar el requerimiento para actualización o mantenimiento del Sistema Contable.

CONCLUSIONES

- La implementación de la guía técnica, mejoró la planificación del proceso de seguridad de los datos en los sistemas de información al ser tomados en cuenta las buenas prácticas del modelo de COBIT, en la aplicación de los procesos y subprocesos de la UTIC.

- Los controles aplicados a las actualizaciones y cambios en los sistemas de información cubren las necesidades de seguridad de los datos en los departamentos de la institución, con procesos definidos para cada actividad para los administradores y personal técnico de la unidad.

- La guía técnica ayudó a mitigar los riesgos de seguridad de los datos en los sistemas de información, mediante acciones seguras, organizadas, transparentes y buscando siempre la optimización de los recursos.

- Se socializó la guía técnica con los administradores de los sistemas de información; quienes lo acogieron, entendiéndolo en todas sus etapas.

- La Unidad de Tecnología de la Información y las Comunicaciones de la Universidad al momento no cuenta con el personal capacitado en las nuevas tendencias tecnológicas en seguridades de la información, ni con un comité que ayude en los procesos para garantizar los datos.

- Las nuevas aplicaciones al momento no cuentan con un análisis y diseño que ayuden a la seguridad de la información a través de los SGBD's, al tratarse de herramientas de versiones antiguas.

- La UTIC no cuenta con un plan de contingencias ante potenciales ataques a las seguridades de los datos de los sistemas de información, no se tiene el suficiente personal para planificación de actividades extras a las técnicas.

- Es necesario plantear un plan de riesgos a nivel de Unidad, ya que se desconoce de medidas que ayuden a mejorar los procesos y que se puedan mitigar todos los atentados que se puedan presentar en los sistemas de información.

RECOMENDACIONES

- Implementar las mejores prácticas del modelo de COBIT para cubrir otros segmentos y procesos que puedan ser complemento con el actual documento.

- Controlar que se cumplan todas las actividades de seguridad dentro de la UTIC, con la finalidad de que se pueda tener todos los procesos asegurados y evitando posibles ataques.

- Minimizar los riesgos a las seguridades a todo nivel, es lo que se debe plantear la institución, mediante monitorios constantes y que concluyan con procesos que funcionen correctamente.

- Aplicar la presente guía técnica, para la planificación y administración de las seguridades, por parte del personal técnico de la UTIC.

- Capacitar al personal técnico de la Institución que estén en capacidad de administrar las seguridades como prioridad, y que estén en capacidad de generar estrategias para la mejora continua dentro de la UTIC.

- Migrar los datos de las aplicaciones que son desarrolladas en la Universidad a SGBD´s de última generación que dispongan de las seguridades necesarias para garantizar la información que se genera en los distintos departamentos, implementando auditoría a los objetos de estos aplicativos

- Aplicar inmediatamente la Guía Técnica de aseguramiento de los datos en los sistemas de información, para que sus resultados se vean reflejados en los procesos de la institución.

- Elaborar un plan de contingencia basado en el modelo COBIT que sea un complemento, a la Guía técnica planteada, y de esta manera, tener organizados los procesos universitarios.

- Para la gestión de riesgos se plantea la elaboración de una guía basada en las normas de ITIL, que resultan un complemento adecuado dentro de la institución con la guía técnica que se encuentra planteada.

BIBLIOGRAFIA

Gómez Vieites, A.; Suárez Rey, C. (2005). Sistemas de Información: herramientas prácticas para la gestión empresarial (5.ª ed.). Madrid: Ra-Ma Editorial.

Joana, J. M.ª; Gracia, R.; Bolart, J.; García, A. L. (2011). Gestión con éxito de grandes proyectos de transformación, el caso del ICS. Barcelona: Editorial Profit.

Kotter, J. (1996). Leading change. Boston Mass., EE.UU.: Harvard Business School Press.

Marcos, S. y otros (2010). "Sistemes d'informació (a les organitzacions)". Escanejant la informàtica. Barcelona: Editorial UOC.

MÉNDEZ, C. (1993). "Metodología. Guía para elaborar Diseños de Investigación en Ciencias Económicas, Contables, Administrativas**".** Edit. De Gasso, Barcelona.

MORALES, Víctor. (1994). "*Planeamiento y análisis de investigaciones".* Eldorado Ediciones. Caracas. Venezuela.

O'Brien, J. A.; Marakas George, M. (2006). Management Information Systems (7.ª ed., cap. 7 y 8). Nueva York: McGraw-Hill Irwin.

Pastor J.A; Franch X.I.; Sistach F. "Methodological ERP acquisition. The SHERPA experience" (2002). En: J. de Bol (ed.). The Guide to IT Service Management. Londres (RU): Addison- Wesley.

Pinto, J.; Millet, I. (1999). Successful information system implementation: the human side (2.ª ed.). Pennsilvania: PMI.

Rodríguez, J. R.; Lamarca, I. (2011). Sistemas de información y procesos de Negocio. Dirección Estratégica de Sistemas y Tecnologías de la Información. Barcelona: Eurecamedia.

Rodríguez, J. R.; Mariné, P. (2010). Gestión de proyectos (caps. 1, 2 y 8). Barcelona: Eurecamedia.
Simón, M. y otros (2010). "Sistemes d'informació (a les organitzacions)". En: Escanejant la informàtica. Barcelona: Editorial UOC.

REFERENCIAS

[1][3] Pons O, Marín N, Medina J, Acid S, Vila M., 2009, Introducción a las Bases de datos. El Modelo Relacional.

[2][4]Ángel Cobo Yera, 2008, Diseño y programación de Bases de datos.

[**5] [7] Purificación Aguilera, 2008,** Seguridad Informática.

[6] [8] Carmen de Pablos, José Joaquín López Hermoso Agius, Santiago Martín-Romo Romero, Sonia Medina Salgado 2011, Organización y transformación de los sistemas de información en la empresa.

[9] (http://www.analiticaweb.es/que-es-big-data/, Pérez Víctor Sept 2013)

[10]BARRANCO Fragoso Ricardo. IT Specialist for Information Managemnet, IBM Software Group Mexico Junio 2012,
http://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/)

[11] Álvaro Gómez Vieites (2013), Seguridad en Equipos Informáticos

[**12] Jesús Costas Santos (2011),** Seguridad Informática

[13] Jairo Rene Navarro Bustos 2012, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

[14] [15] © 2012 ISACA. Todos los derechos reservados. Para pautas de uso, ver www.isaca.org/COBITuse

DIRECCIONES ELECTRONICAS

Universidad de las Fuerzas Armadas ESPE (Julio 2014).
http://www.espe.edu.ec/portal/portal/main.do?sectionCode=118

Universidad de las Fuerzas Armadas ESPE extensión Latacunga (Julio 2014).
http://espe-el.espe.edu.ec/

Consejo de Educación Superior (Mayo 2014).
http://www.ces.gob.ec/

Consejo de Evaluación, Acreditación y Aseguramiento de la calidad de la Educación Superior (Mayo 2014).
http://www.ceaaces.gob.ec/sitio/

Secretaria de educación Superior, Ciencia, Tecnología e Innovación (Julio 2014).
http://www.educacionsuperior.gob.ec/

ISACA Trust in, and value from, Information systems (Julio 2014).
https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=CjwKEAjwgYKfBRDvgJeylem9xDUSJACjeQ7AJuo1NZE59bvrFA8iTMb2hytIiaaA18JGJL_Kz1EnIRoCFRbw_wcB

El rol de Cobit 5 en la estrategia de seguridad Informática (Julio 2014).
http://searchdatacenter.techtarget.com/es/reporte/El-rol-de-CobIT-5-en-la-estrategia-de-seguridad-informatica

Gestion de Riesgos usando Cobit 5 (Junio, 2014)
http://francoitgrc.wordpress.com/2013/09/27/gestion-de-riesgos-usando-cobit-5/

Figura 6.2: Esquema de la configuración del IOOOIA SECUNDARIO UTIC (Navas P., 2014)

ANEXOS

ANEXO 1.

DESCUADRE EN EL SISTEMA ENTRE BODEGAS Y SISTEMA FINANCIERO POR MAL MANEJO DEL SISTEMA FINANCIERO

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA
EXTENSIÓN LATACUNGA

SECCIÓN DE FINANZAS

Memorando Nro. ESPE-EL-SF-2014-0737-M

LATACUNGA, 14 de julio de 2014

PARA: Ing. Luis Fernando Alvarado Espinoza
Guardalmacén

ASUNTO: Disponiendo Justificar y Conciliar Saldos Contables.

El sistema de bienes SAF presenta una diferencia de $ 26.268,00 (VEINTE Y SEIS MIL DOSCIENTOS SESENTA Y OCHO DÓLARES CON 00/100 CVTS), con los saldos contables; razón por la cual, agradeceré a usted señor Servidor Público justificar y conciliar con contabilidad mencionados valores hasta el 181000-JUL-014.

Atentamente,
DIOS, PATRIA Y LIBERTAD

Capt. de INT. César Eduardo Navas Jurado
JEFE SECCIÓN DE FINANZAS

Elaborado por: VICTORIA CAROLINA ALMENDARIZ TERÁN

Sede Latacunga – Cotopaxi, Quijano Ortoñez y Hermanas Páez

* Documento generado por Quipux

1/1

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA
EXTENSIÓN LATACUNGA

SECCIÓN DE FINANZAS

Memorando Nro. ESPE-EL-SF-2014-0738-M

LATACUNGA, 14 de julio de 2014

PARA: Ing. Alicia Marianela Robayo Espin
Contadora

ASUNTO: Disponiendo

Mediante el presente, agradeceré a usted señora Servidora Pública, conciliar los saldos del sistema SAF con los saldos contables; a fin, de continuar con la carga de matrices en el sistema e-SIGEF, de acuerdo a los valores que genera el mencionado sistema.

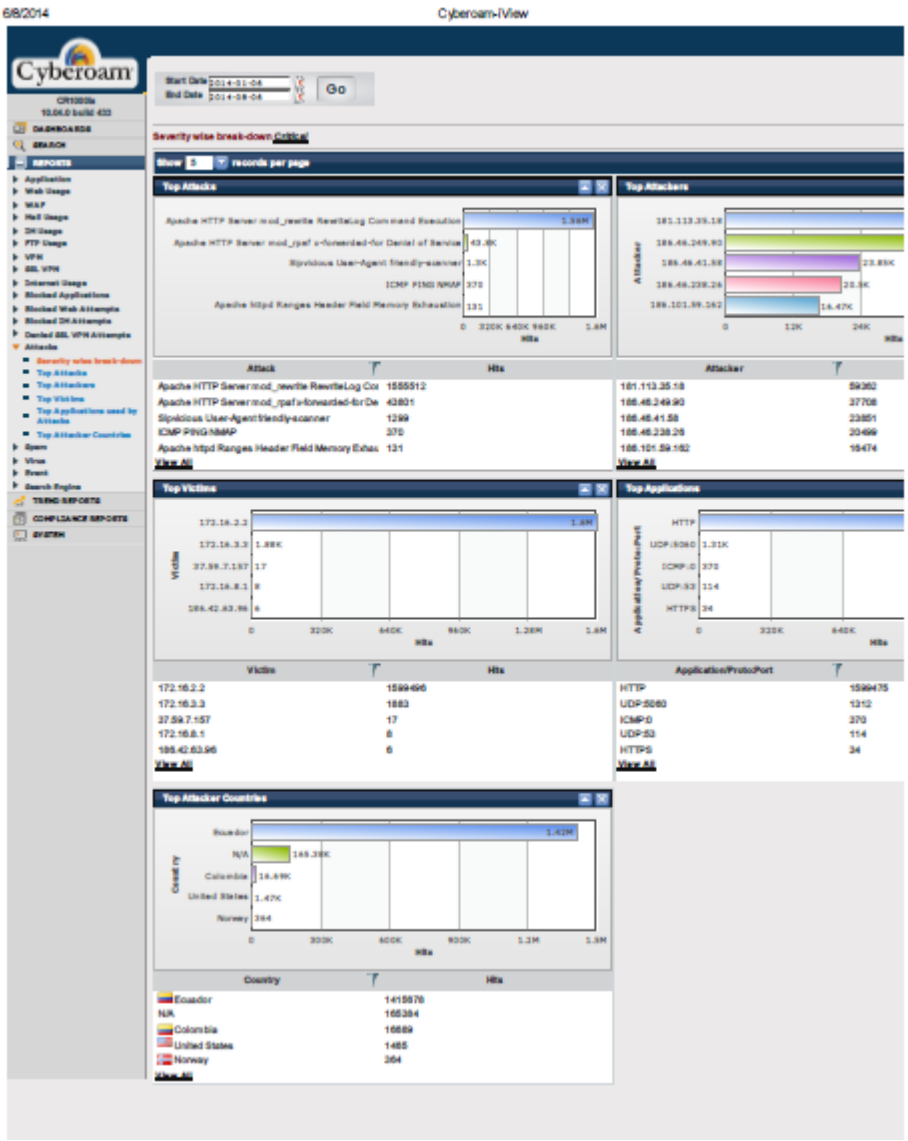
Atentamente,
DIOS, PATRIA Y LIBERTAD

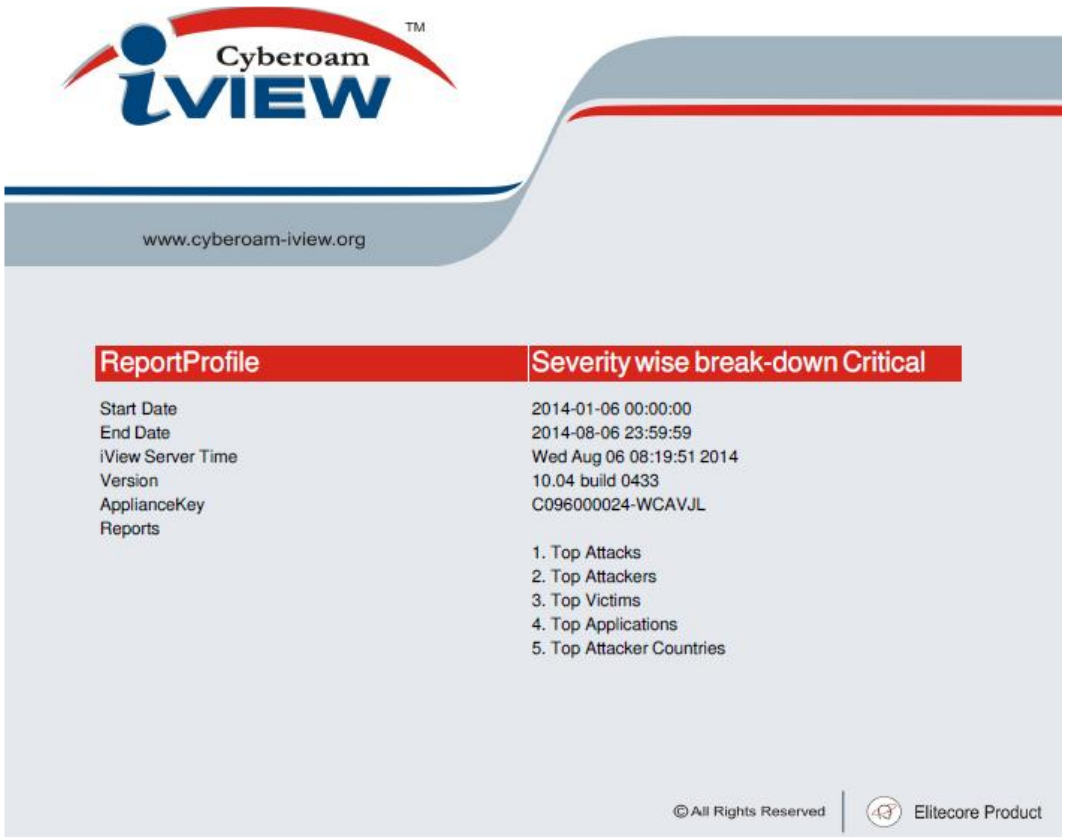
Capt. de INT. César Eduardo Navas Jurado
JEFE SECCIÓN DE FINANZAS

Elaborado por: VICTORIA CAROLINA ALMENDARIZ TERÁN

ANEXO 2.

CONTROL DE ATAQUES AL CYBEROAM (CLUSTER DE SEGURIDAD PERIMETRAL).




Cyberoam
iVIEW
www.cyberoam-iview.org
ReportProfile
Severity wise break-down Critical
Start Date
End Date
iView Server Time
Version
ApplianceKey
Reports
2014-01-06 00:00:00
2014-08-06 23:59:59
Wed Aug 06 08:19:51 2014
10.04 build 0433
C096000024-WCAVJL
1. Top Attacks
2. Top Attackers
3. Top Victims
4. Top Applications
5. Top Attacker Countries
© All Rights Reserved
Elitecore Product

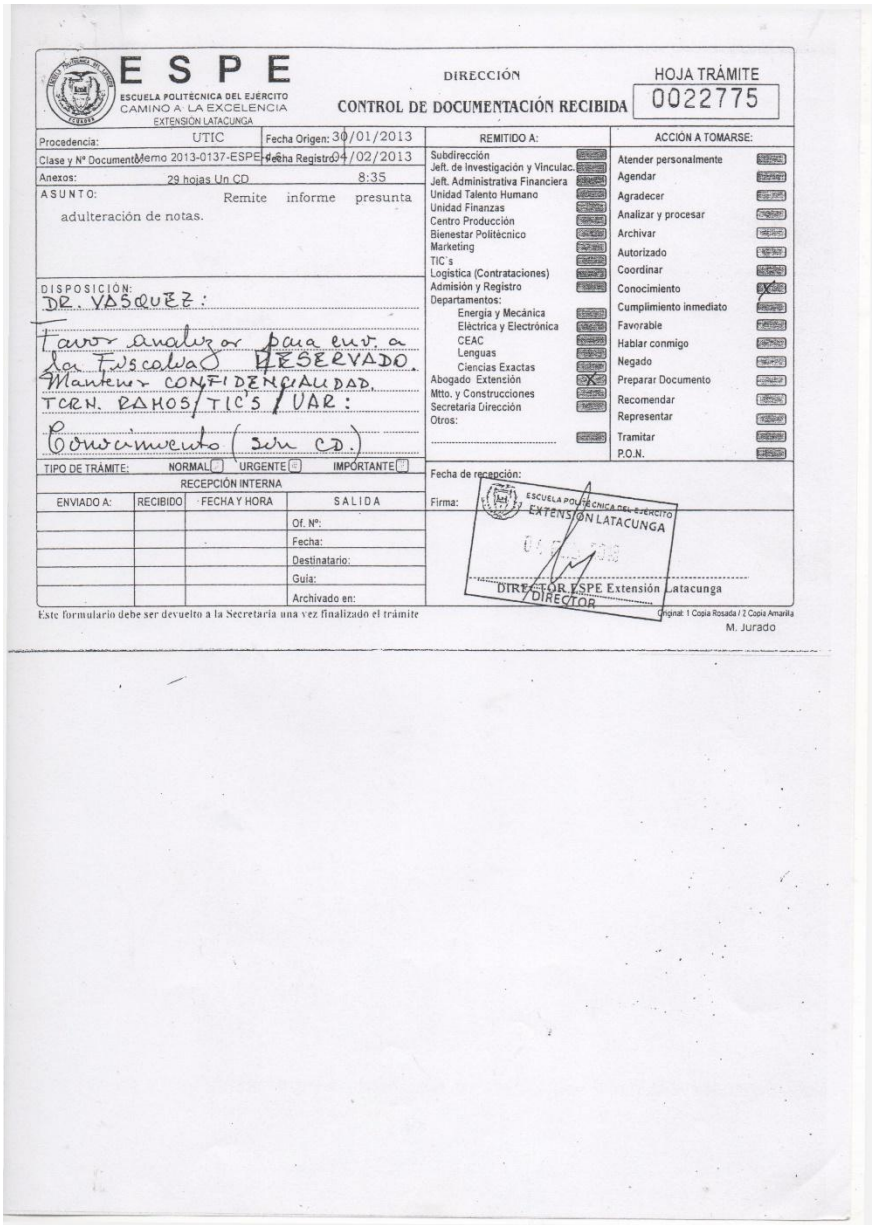
1. Top Attacks

Attack	Hits
Apache HTTP Server mod_rewrite RewriteLog Command Execution	1555459
Apache HTTP Server mod_rpaf x-forwarded-for Denial of Service	43801
Sipvicious User-Agent friendly-scanner	1299
ICMP PING NMAP	370
Apache httpd Ranges Header Field Memory Exhaustion	131
Blue Coat BCAAA Stack Buffer Overflow	77
DNS named version attempt	61
Microsoft Internet Explorer Malformed IFRAME Buffer Overflow	57
DNS Query Type ANY - isc.org	52
Microsoft Office TIFF Image Converter Heap Buffer Overflow	51
NMAP SCAN -sS window 1024	35
MS-SQL Worm propagation attempt	20
NMAP SCAN -sS window 4096	19
HTTPS/SSL Renegotiation DoS	15
SHELLCODE x86 setuid 0	14
Sipvicious User-Agent sundayddr	13
NMAP SCAN -sS window 3072	11

libpng png_decompress_chunk Integer Overflow	7
NMAP SCAN -sS window 2048	7
SIP Brute-force Attack (OPTIONS SIP Scan)	5
TROJAN ZeroAccess Outbound udp traffic detected	4
Plesk Apache Zeroday Remote Exploit Vunerability	4
Flexera FlexNet Publisher License Server Manager lmgrd Stack Buffer Overflow	3
SHELLCODE x86 setgid 0	3
Microsoft Windows TCP-IP Stack Denial of Service	2
TFTP Get	1
DNS Query Type ANY - ripe.net	1

ANEXO 3.

DOCUMENTOS PRESUMIBLE ALTERACION DE CALIFICACIONES DE PARTE DE LOS ESTUDIANTES AL SISTEMAS ESCOLASTICO.



E S P E
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA
EXTENSIÓN LATACUNGA

DIRECCIÓN
CONTROL DE DOCUMENTACIÓN RECIBIDA

HOJA TRÁMITE
0022775

Procedencia: UTIC
Fecha Origen: 30/01/2013
Clase y Nº Documento: Memo 2013-0137-ESPE
Fecha Registro: 04/02/2013
Anexos: 29 hojas Un CD
8:35

ASUNTO: Remite informe presunta adulteración de notas.

DISPOSICIÓN:
DR. VASQUEZ:
favor analizar para env. a la Fiscalia RESERVADO.
Mantener CONFIDENCIALIDAD.
TCRN. RAMOS/TIC'S/UAR:
Conocimiento (sin CD.)

TIPO DE TRÁMITE: NORMAL ☐ URGENTE ☒ IMPORTANTE ☐

RECEPCIÓN INTERNA

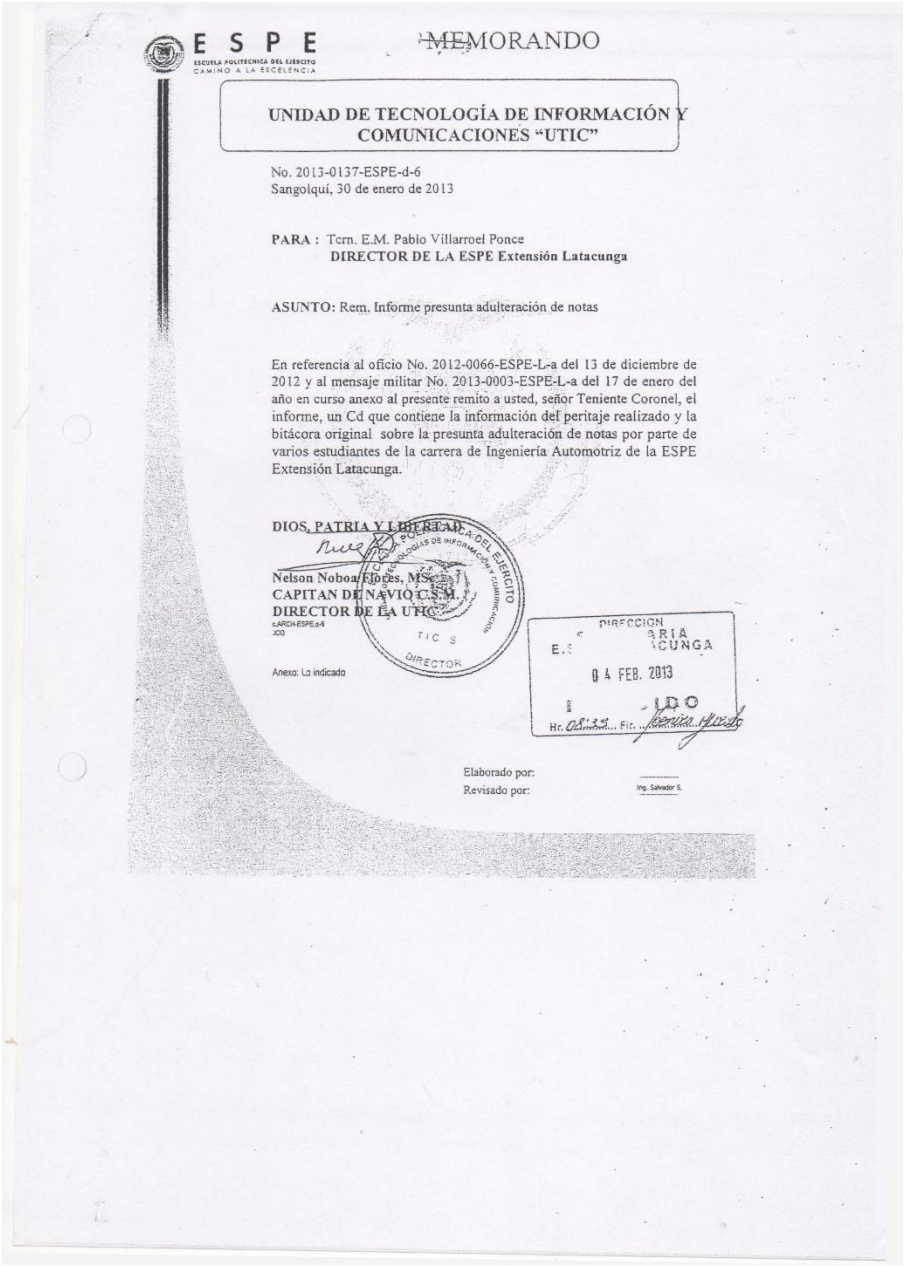
ENVIADO A:	RECIBIDO	FECHA Y HORA	SALIDA
			Of. Nº:
			Fecha:
			Destinatario:
			Guía:
			Archivado en:

REMITIDO A:
Subdirección ☐
Jefe. de Investigación y Vinculac. ☐
Jefe. Administrativa Financiera ☐
Unidad Talento Humano ☐
Unidad Finanzas ☐
Centro Producción ☐
Bienestar Politécnico ☐
Marketing ☐
TIC´s ☐
Logística (Contrataciones) ☐
Admisión y Registro ☐
Departamentos:
Energía y Mecánica ☐
Eléctrica y Electrónica ☐
CEAC ☐
Lenguas ☐
Ciencias Exactas ☐
Abogado Extensión ☒
Mtto. y Construcciones ☐
Secretaría Dirección ☐
Otros: ☐

ACCIÓN A TOMARSE:
Atender personalmente ☐
Agendar ☐
Agradecer ☐
Analizar y procesar ☐
Archivar ☐
Autorizado ☐
Coordinar ☐
Conocimiento ☒
Cumplimiento inmediato ☐
Favorable ☐
Hablar conmigo ☐
Negado ☐
Preparar Documento ☐
Recomendar ☐
Representar ☐
Tramitar ☐
P.O.N. ☐

Fecha de recepción:
Firma:
ESCUELA POLITÉCNICA DEL EJÉRCITO EXTENSIÓN LATACUNGA
DIRECTOR ESPE Extensión Latacunga
DIRECTOR

Este formulario debe ser devuelto a la Secretaría una vez finalizado el trámite
Original: 1 Copia Rosada / 2 Copia Amarilla
M. Jurado



E S P E
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA

MEMORANDO

UNIDAD DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES "UTIC"

No. 2013-0137-ESPE-d-6
Sangolquí, 30 de enero de 2013

PARA : Tcrn. E.M. Pablo Villarroel Ponce
DIRECTOR DE LA ESPE Extensión Latacunga

ASUNTO: Rem. Informe presunta adulteración de notas

En referencia al oficio No. 2012-0066-ESPE-L-a del 13 de diciembre de 2012 y al mensaje militar No. 2013-0003-ESPE-L-a del 17 de enero del año en curso anexo al presente remito a usted, señor Teniente Coronel, el informe, un Cd que contiene la información del peritaje realizado y la bitácora original sobre la presunta adulteración de notas por parte de varios estudiantes de la carrera de Ingeniería Automotriz de la ESPE Extensión Latacunga.

DIOS, PATRIA Y LIBERTAD

Nelson Noboa Flores, MSc.
CAPITAN DE NAVIO C.S.M.
DIRECTOR DE LA UTIC

cARCH-ESPE-d-6
JDD

Anexo: Lo indicado

DIRECCION
E.S ARIA
CUNGA
04 FEB. 2013
RIDO
Hr. 08:39 Fir.

Elaborado por:
Revisado por: Ing. Salvador S.

ANEXO 4

MATRIZ DE LA PROPUESTA DE ACTIVIDADES DEL PESONAL DE LA UTIC DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSION LATACUNGA

VER. 1

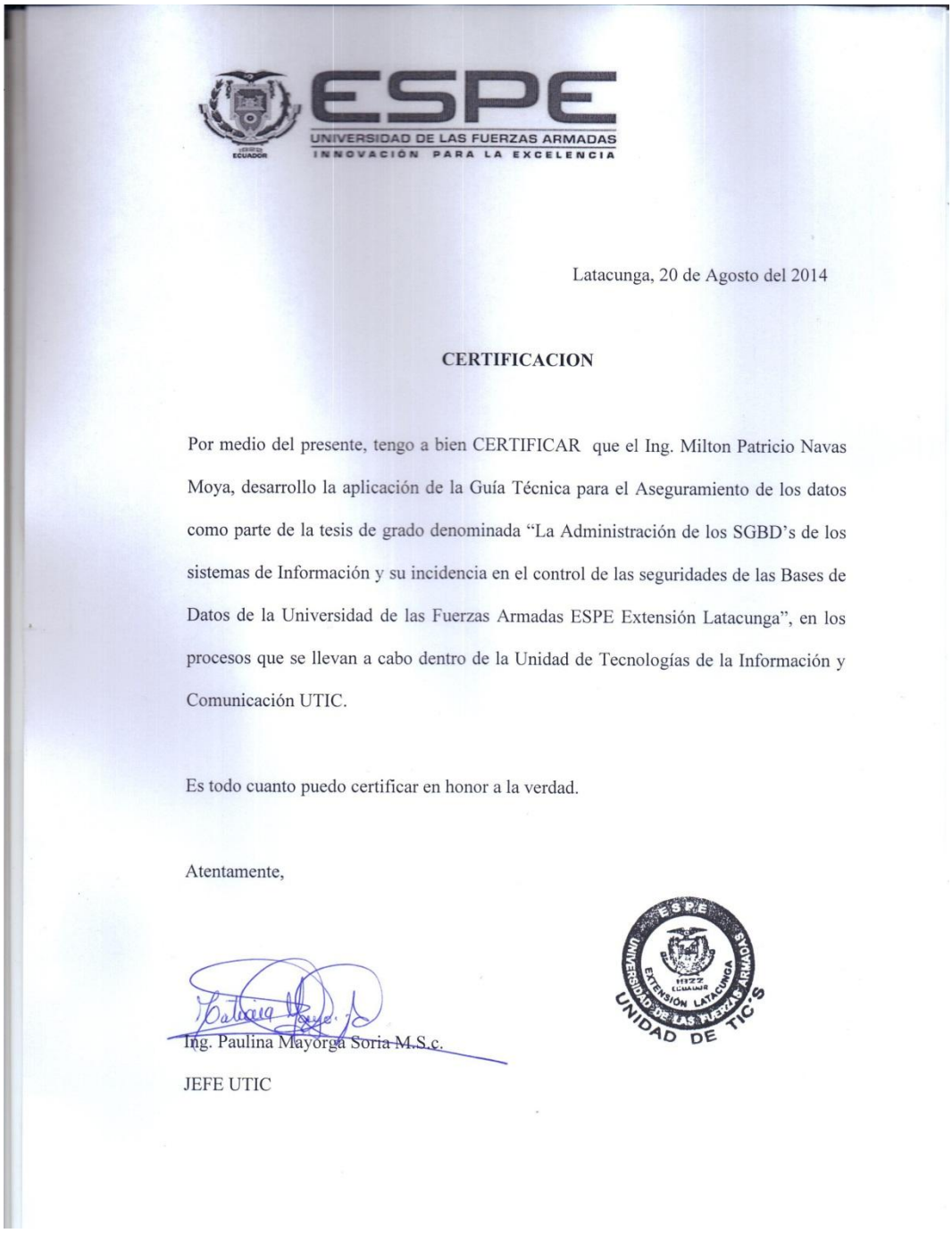
UNIVERSIDAD DE FUERZAS ARMADAS ESPE - EXTENSIÓN LATACUNGA

MATRIZ DE PROCESOS DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNCACIÓN

	PROCESO	SUBPROCESO	OBJETIVO	PERIODICIDAD	REFERENCIA DE ACTIVIDADES A DESARROLLAR	RESPONSABLE	RECURSO HUMANO	RESPONSABLE ACTUAL
1	Gestión Estratégica de Tecnologías de Información y Comunicaciones	Gestión de Proyectos y Requerimientos de TIC´s	Coordinar con las áreas de TIC´s y elaborar, gestionar y ejecutar los proyectos y requerimientos de tecnologías de información y comunicaciones, con el fin de solventar las necesidades institucionales	Anual, mensual	Elaborar y gestionar proyectos de TIC'S (Plan anual de compras y Plan operativo anual) Elaborar Plan de infraestructura Tecnológica Controlar el cumplimiento de estándares y directrices sobre los equipos de infraestructura tecnológica que se adquieren. Coordinación sobre tecnologías con Proveedores	Especialista	1 EGT1	
		Gestión de Riesgos de TIC´s	Analizar la situación actual a nivel de riesgos de tecnologías de información y comunicaciones, planificar e implementar el plan de contingencias y plan de seguridad informática, para garantizar la confidencialidad, integridad y disponibilidad de la información.	Anual	Elaboración y supervisión de la Ejecución de Plan de Contingencias y Plan de Seguridad Informática	Especialista		
		Gestión de requerimientos sobre aplicativos desarrollados y administrados en la ESPE Matriz	Realizar las gestiones y seguimiento pertinente para que se incluyan nuevos requerimientos o necesidades de los usuarios que utilizan los aplicativos desarrollados y Administrados por la UTIC de la ESPE Matriz	mensual	Sistema Banner - Académico (pregrado, postgrado) Sistema Banner - Autoservicios Sistema Banner- Portal Luminis Sistema Banner Administrativo (RRHH), Digitalización, Workflow, Sistema Médico, Sistema de Evaluación Docente, Correo Institucional a través de MIESPE Licenciamiento de software institucional para servidores y clientes.	Especialista		
9	Desarrollo, implantación y administración de aplicativos y bases de datos	Desarrollo de Aplicativos	Analisis y diseño de aplicativos, construccion de aplicativos	semestral	Desarrollo de sistemas de información cerrados.	Especialista	1 EGT4	
10		Administración de aplicativos y Base de Datos	Administrar los aplicativos (Sistemas informáticos) de la Institución, con la finalidad de garantizar su disponibilidad y funcionamiento adecuado, así como la integridad, confidencialidad y seguridad de la información almacenada en la Base de Datos. ejecutar las acciones correctivas para mantener los servicios funcionales e implementar nuevas soluciones	diaria	Micrositos, Plataforma virtual moodle, Sitio Web sistemas de terceros : Olympo , Syabac, Sist. Biométrico, Spontanea Sistemas Propietarios de la institución: Sistema Rancho, Sistema Gestión Docentes, Sistema de Egresados y Graduados , Sistema Escuela de Conducción, Sistemas fuera de Producción a nivel de consultas , Repositorios Digitales de archivos Biblioteca,	Especialista	1EGT4	

ANEXO 5

CERTIFICADO DE APLICACIÓN DE LA PROPUESTA



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Latacunga, 20 de Agosto del 2014

CERTIFICACION

Por medio del presente, tengo a bien CERTIFICAR que el Ing. Milton Patricio Navas Moya, desarrollo la aplicación de la Guía Técnica para el Aseguramiento de los datos como parte de la tesis de grado denominada "La Administración de los SGBD's de los sistemas de Información y su incidencia en el control de las seguridades de las Bases de Datos de la Universidad de las Fuerzas Armadas ESPE Extensión Latacunga", en los procesos que se llevan a cabo dentro de la Unidad de Tecnologías de la Información y Comunicación UTIC.

Es todo cuanto puedo certificar en honor a la verdad.

Atentamente,

ESPE EXTENSIÓN LATACUNGA UNIVERSIDAD DE LAS FUERZAS ARMADAS UNIDAD DE TIC'S

Ing. Paulina Mayorga Soria M.S.c.

JEFE UTIC

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Latacunga, 20 de Agosto del 2014

CERTIFICACION

Por medio del presente, tengo a bien CERTIFICAR que el Ing. Milton Patricio Navas Moya, desarrollo la aplicación de la Guía Técnica para el Aseguramiento de los datos como parte de la tesis de grado denominada "La Administración de los SGBD's de los sistemas de Información y su incidencia en el control de las seguridades de las Bases de Datos de la Universidad de las Fuerzas Armadas ESPE extensión Latacunga", en los procesos que se llevan a cabo dentro de la Unidad de Tecnologías de la Información y las Comunicaciones UTIC.

Es todo cuanto puedo certificar en honor a la verdad.

Atentamente,

Ing. Milton Chango

Técnico en Mantenimiento de Sistemas.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
EXTENSIÓN LATACUNGA
UNIDAD DE TIC'S