

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

**FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**

**ESCUELA DE INGENIERÍA EN SISTEMAS INFORMÁTICOS**

**PROPUESTA DE MEJORES PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES MÓVILES**

Trabajo de titulación presentado para optar al grado académico de:

**INGENIERO EN SISTEMAS INFORMÁTICOS**

**AUTORES:** Cevallos Muñoz Fausto Danilo

Sigüenza Plaza Ángel Javier

**TUTOR:** Ing. Jorge Menéndez

Riobamba-Ecuador

2016

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

**FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**

**ESCUELA DE INGENIERÍA EN SISTEMAS INFORMÁTICOS**

El Tribunal de Trabajo de Titulación certifica que: El trabajo de investigación “PROPUESTA DE MEJORES PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES MÓVILES”, de responsabilidad de los señores Ángel Javier Sigüenza Plaza y Fausto Danilo Cevallos Muñoz, ha sido minuciosamente revisado por los Miembros del Tribunal, quedando autorizada su presentación.

Dr. Miguel Tasambay PhD. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DECANO

Dr. Julio Santillán Castillo. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DIRECTOR DE ESCUELA

Ing. Jorge Menéndez . \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DIRECTOR DEL TRABAJO

DE TITULACIÓN

Ing. Natalia Layedra. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MIEMBRO DEL TRIBUNAL

Nosotros, Ángel Javier Sigüenza Plaza y Fausto Danilo Cevallos Muñoz somos responsables de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Fausto Danilo Cevallos Muñoz Ángel Javier Sigüenza Plaza

**DEDICATORIA**

Dedico este trabajo a mis padres y hermanos quienes me han permitido crecer brindándome su apoyo incondicional, a mi esposa y mi hijo quienes se han convertido en el motor que me impulsa a cumplir las metas y anhelos trazados, a todos mis amigos que de una forma u otra siempre han estado en los momentos más difíciles, a todos ustedes les dedico, con mucho aprecio, este esfuerzo que finaliza una etapa crucial como estudiante y marca el inicio de mi vida profesional.

Fausto.

Dedico esta tesis  A. DIOS, a San Luis, patrono de Guasuntos, quienes estuvieron conmigo a lo largo de la carrera y en la realización de la tesis. A mis  padres quienes me dieron vida, educación,  y cariño. A mis amigos y a todas esas personas que en algún momento fueron importantes y me dieron su apoyo y que sin duda me han ayudado a la culminación de esta tesis. A todos ellos se los agradezco desde el fondo de mi corazón. Para todos ellos hago esta dedicatoria.

Javier.

**AGRADECIMIENTO**

Agradezco de forma infinita y con el mayor aprecio a mi familia que siempre me brinda su apoyo incondicional, a mis amigos que nunca han fallado en estar siempre presentes, agradezco a mis maestros por los cuales he aprendido a ser un profesional, de manera especial agradezco a los miembros de CIMOGSYS por la oportunidad de representarlos a través de este Trabajo de Titulación, a la FADE que siempre me permite crecer laboralmente, agradezco a mi Tutor por todos los conocimientos que he podido adquirir en esta etapa final como estudiante, gracias.

Fausto.

Quiero expresar mi más grande agradecimiento al Ing. Giovanni Alarcón por su importante aporte y participación en el desarrollo de esta tesis, por abrirnos las puertas del Centro permitiéndonos hacer uso de su espacio físico, también agradezco a mi Director de Tesis Ing. Jorge Menéndez, por su tiempo y paciencia las cuales han sido fundamentales para concluir con éxito esta tesis, a mis padres quienes estuvieron en los difíciles días como estudiante y a mis maestros quienes transmitieron su conocimiento a lo largo de la carrera en especial al Dr. Julio Santillán y la Dra. Narcisa Salazar, por quienes siento una profunda gratitud y admiración como Personas y como Docentes.

Javier.

**CONTENIDO**

[RESUMEN xi](#_Toc447784644)

[SUMMARY xii](#_Toc447784645)

[INTRODUCCIÓN 1](#_Toc447784646)

[Antecedentes 2](#_Toc447784647)

[Justificación 4](#_Toc447784648)

[Justificación Teórica 4](#_Toc447784649)

[Justificación Práctica 5](#_Toc447784650)

[Objetivos 6](#_Toc447784651)

[Objetivo General 6](#_Toc447784652)

[Objetivos Específicos 6](#_Toc447784653)

[1. MARCO TEÓRICO 7](#_Toc447784654)

[1.1. Disponibilidad 7](#_Toc447784655)

[1.2. Accesibilidad 8](#_Toc447784656)

[1.3. Buenas Prácticas, Normas y Estándares 9](#_Toc447784657)

[1.4. Dispositivo Móvil 13](#_Toc447784658)

[1.5. Sistema Operativo Móvil 16](#_Toc447784659)

[1.6. Aplicación Móvil 16](#_Toc447784660)

[1.7. Vulnerabilidad 19](#_Toc447784661)

[1.8. Amenaza 21](#_Toc447784662)

[1.9. Gestión del Riesgo 23](#_Toc447784663)

[1.10. Ataques 26](#_Toc447784664)

[1.11. Tipos de Ataques 28](#_Toc447784665)

[1.11.1. Basados en el Navegador 29](#_Toc447784666)

[1.11.2. Ataques por Teléfono o Mensajes de Texto 29](#_Toc447784667)

[1.11.3. Ataques basados en Aplicación 30](#_Toc447784668)

[1.11.4. Ataques Basados en el Sistema Operativo 31](#_Toc447784669)

[1.11.5. Ataques Basados en la Red 31](#_Toc447784670)

[1.11.6. Ataques Basados en el Servidor 32](#_Toc447784671)

[1.11.7. Ataques a la Base de Datos 32](#_Toc447784672)

[2. MARCO METODOLÓGICO 33](#_Toc447784673)

[2.1. Operacionalización Metodológica Variable Independiente 35](#_Toc447784674)

[2.2. Operacionalización Metodológica Variable Dependiente 36](#_Toc447784675)

[3. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 37](#_Toc447784676)

[3.1. Buenas Prácticas de Seguridad 37](#_Toc447784677)

[3.1.1. Dimensión Capa de Base de Datos 37](#_Toc447784678)

[3.1.2. Dimensión Capa de Reglas del Negocio 41](#_Toc447784679)

[3.1.3. Dimensión Capa Física de Transporte 46](#_Toc447784680)

[3.1.4. Dimensión Capa de Presentación 53](#_Toc447784681)

[3.2. Disponibilidad de Información 59](#_Toc447784682)

[3.2.1. Dimensión Accesibilidad 59](#_Toc447784683)

[4. PROPUESTA DE MEJORES PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES MÓVILES 66](#_Toc447784684)

[4.1. Estado Inicial de la Facultad de Administración de Empresas 66](#_Toc447784685)

[4.2. Estado Inicial del Centro de Investigación en Modelos de Gestión y Sistemas Informáticos 67](#_Toc447784686)

[4.3. Mejores Prácticas de Seguridad Para el Desarrollo de Aplicaciones Móviles 67](#_Toc447784687)

[4.3.1. Capa de Almacenamiento de Datos 70](#_Toc447784688)

[4.3.2. Capa de Lógica del Negocio 71](#_Toc447784689)

[4.3.3. Capa de Transporte 73](#_Toc447784690)

[4.3.4. Capa de Presentación 73](#_Toc447784691)

[4.4. Desarrollo de la aplicación móvil del Sistema de Gestión de Información, haciendo uso de buenas prácticas de seguridad, implementada en la Facultad de Administración de Empresas. 76](#_Toc447784692)

[4.4.1. Beneficios Tangibles e Intangibles 77](#_Toc447784693)

[4.4.2. Especificación de Requerimientos 79](#_Toc447784694)

[4.4.3. Estimación 80](#_Toc447784695)

[4.4.4. Estudio de Factibilidad 87](#_Toc447784696)

[4.4.5. Personas y Roles 90](#_Toc447784697)

[4.4.6. Planificación 91](#_Toc447784698)

[4.4.7. Desarrollo de la aplicación 95](#_Toc447784699)

[CONCLUSIONES 108](#_Toc447784700)

[RECOMENDACIONES 109](#_Toc447784701)

[BIBLIOGRAFÍA 110](#_Toc447784702)

[ANEXO A – MODELO DE ENCUESTAS 115](#_Toc447784703)

[ANEXO B – MANUAL TÉCNICO DE LA APLICACIÓN 116](#_Toc447784704)

[ANEXO C – MANUAL DE USUARIO 117](#_Toc447784705)

**ÍNDICE DE TABLAS**

[Tabla 2‑1 Operacionalización Conceptual de las Variables 34](#_Toc444817426)

[Tabla 2‑2 Operación Metodológica Buenas Prácticas de Seguridad 35](#_Toc444817427)

[Tabla 2‑3 Operacionalización Metodológica Disponibilidad de Información 36](#_Toc444817428)

[Tabla 4‑1 Buenas Prácticas de Seguridad para el Desarrollo de Aplicaciones 68](#_Toc444817429)

[Tabla 4‑2 Buenas Prácticas de Seguridad para la Capa de Almacenamiento de Datos 71](#_Toc444817430)

[Tabla 4‑3 Buenas Prácticas de Seguridad para la Capa de Lógica del Negocio 71](#_Toc444817431)

[Tabla 4‑4 Buenas Prácticas de Seguridad para la Capa de Transporte 73](#_Toc444817432)

[Tabla 4‑5 Buenas Prácticas de Seguridad para la Capa de Presentación 74](#_Toc444817433)

[Tabla 4‑6 Factores de Esfuerzo 82](#_Toc444817434)

[Tabla 4‑7 Valor de Factores de Esfuerzo 83](#_Toc444817435)

[Tabla 4‑8 Factores de Escala 85](#_Toc444817436)

[Tabla 4‑9 Hardware Requerido 88](#_Toc444817437)

[Tabla 4‑10 Software Requerido 88](#_Toc444817438)

[Tabla 4‑11 Personal Técnico Requerido 89](#_Toc444817439)

[Tabla 4‑12 Factibilidad Económica 90](#_Toc444817440)

[Tabla 4‑13 Integrantes y Roles del Proyecto 91](#_Toc444817441)

[Tabla 4‑14 Product Backlog 92](#_Toc444817442)

[Tabla 4‑15 Sprint Backlog 94](#_Toc444817443)

[Tabla 4‑16 Historia Técnica 96](#_Toc444817444)

[Tabla 4‑17 Tarea de Ingeniería 96](#_Toc444817445)

[Tabla 4‑18 Prueba de Aceptación 97](#_Toc444817446)

**ÍNDICE DE FIGURAS**

[Figura 1‑1 Tipos de Amenazas Informáticas 22](#_Toc444817447)

[Figura 1‑2 Ciclo de Vida ISO 27005 vs ISO 31000 24](#_Toc444817448)

[Figura 3‑1 Indicador Inyección SQL 38](#_Toc444817449)

[Figura 3‑2 Indicador Privilegios 39](#_Toc444817450)

[Figura 3‑3 Indicador Ejecución de Comandos de SO 40](#_Toc444817451)

[Figura 3‑4 Resumen de la Dimensión Base de Datos 41](#_Toc444817452)

[Figura 3‑5 Indicador Ataques de Fuerza Bruta 42](#_Toc444817453)

[Figura 3‑6 Indicador Ataques XSS 43](#_Toc444817454)

[Figura 3‑7 Indicador Ataques DoS 44](#_Toc444817455)

[Figura 3‑8 Indicador Validación de Formularios 45](#_Toc444817456)

[Figura 3‑9 Resumen Dimensión de Reglas de Negocio 45](#_Toc444817457)

[Figura 3‑10 Indicador de Encriptación de datos 46](#_Toc444817458)

[Figura 3‑11 Indicador Certificados SSL 47](#_Toc444817459)

[Figura 3‑12 Cantidad de Problemas SSL Identificados 48](#_Toc444817460)

[Figura 3‑13 Indicador Espionajes de Paquetes Identificados 49](#_Toc444817461)

[Figura 3‑14 Cantidad de Ataques de Envenenamiento DNS 50](#_Toc444817462)

[Figura 3‑15 Indicador Secuestro de Sesiones 51](#_Toc444817463)

[Figura 3‑16 Indicador Hombre en el Medio 52](#_Toc444817464)

[Figura 3‑17 Resumen Dimensión Capa de Transporte 52](#_Toc444817465)

[Figura 3‑18 Indicador de Permisos Inintencionados 53](#_Toc444817466)

[Figura 3‑19 Cantidad de operaciones no asignadas identificadas 54](#_Toc444817467)

[Figura 3‑20 Indicador Hombre en el Móvil 55](#_Toc444817468)

[Figura 3‑21 Indicador Ataque Clickjacking 56](#_Toc444817469)

[Figura 3‑22 Cantidad de Ataques de Suplantación de Identidad 57](#_Toc444817470)

[Figura 3‑23 Cantidad de Aplicaciones creadas en las Facultades 58](#_Toc444817471)

[Figura 3‑24 Resumen Dimensión Capa de Presentación 59](#_Toc444817472)

[Figura 3‑25 Uso del SGC fuera de horario de oficina 60](#_Toc444817473)

[Figura 3‑26 Uso del SGC en la ESPOCH 60](#_Toc444817474)

[Figura 3‑27 Uso del SGC fuera de la ciudad de Riobamba 61](#_Toc444817475)

[Figura 3‑28 Uso de SGC fuera del País 62](#_Toc444817476)

[Figura 3‑29 Uso del SGC en la Web 63](#_Toc444817477)

[Figura 3‑30 Uso del SGC en el Móvil 63](#_Toc444817478)

[Figura 3‑31 Uso del SGC en la Televisión 64](#_Toc444817479)

[Figura 3‑32 Uso del SGC en autos 64](#_Toc444817480)

[Figura 4‑1 Forma de Aplicar las Propuestas de Seguridad 75](#_Toc444817481)

[Figura 4‑2 Puntos de Función 81](#_Toc444817482)

[Figura 4‑3 Factor de Esfuerzo 84](#_Toc444817483)

[Figura 4‑4 Factores de Escala 85](#_Toc444817484)

[Figura 4‑5 Diagrama de Despliegue 97](#_Toc444817485)

[Figura 4‑6 Interfaz de Inicio de Sesión 99](#_Toc444817486)

[Figura 4‑7 Página de Inicio 99](#_Toc444817487)

[Figura 4‑8 Menú de los Sistemas de Gestión 100](#_Toc444817488)

[Figura 4‑9 Mapas de Procesos 101](#_Toc444817489)

[Figura 4‑10 Interfaces de Auditoría de Procesos 102](#_Toc444817490)

[Figura 4‑11 Interfaz de Auditoría de Criterios 102](#_Toc444817491)

[Figura 4‑12 Gráfico de Seguimiento del Proyecto 107](#_Toc444817492)

# RESUMEN

En la ESPOCH (Escuela Superior Politécnica de Chimborazo), la Facultad de Administración de Empresas tiene sistemas informáticos que poseen problemas de disponibilidad y accesibilidad de información, con la finalidad de resolver dichos inconvenientes, se realizó una revisión bibliográfica de las buenas prácticas de seguridad: *Secure Mobile Development, Security Premier, Top Ten Mobile Risks* emitidas por NowSecure y la Open Web Application Security Project, se ha encuestado a las áreas de gestión sobre los parámetros de seguridad, que emplean en el desarrollo de sus aplicaciones y los inconvenientes que han tenido al emplearlos, dando como resultado que el conocimiento de las vulnerabilidades (53,28%), es muy superior a la de prevención de las mismas (9,02%) y al registro de las ocurrencias de ataques, lo que demuestra que la ESPOCH tiene riesgos que pueden ser explotados a corto o largo plazo, por lo que se ha emitido una propuesta de mejores prácticas de seguridad para la creación de la aplicaciones móviles que consta de 119 políticas las cuales han sido divididas en 4 capas: Capa de Almacenamiento de Datos, Capa de Lógica del Negocio, Capa de Transporte y Capa de Presentación, por lo que se recomienda implementar esta metodología, con el fin de mitigar dichas amenazas.

**Palabras** **claves**: VULNERABILIDAD, RIESGOS, SEGURIDAD, ANDROID, IOS.

# SUMMARY

In ESPOCH (Polytechnic School of Chimborazo) the Faculty of business administration has computer systems that have problems of availability and accessibility of information, in order to solve these problems, a literature review of good safety practices, is done: Secure Mobile Development Premier, Security Premier, Top Ten Mobile Risks, issued by NowSecure and Open Web Application Security Project, has surveyed the areas of management on the security parameters that are used in the development of their application and inconveniences have had to use them, resulting that knowledge of vulnerability (53,28%) is much higher than the prevention of it (9,02%) and registration of occurrence of attack, which shows that ESPOCH has risks that can be exploited in a short or long term, so it has issued a proposal of best security practices for developing mobile application consisting of 119 policies, which are divided into four layers: data storage layers, business logic layer transport layer and presentation layer, so it is recommended that this methodology should be implemented in order to mitigate these threats.

# INTRODUCCIÓN

Ecuador es un país que busca continuamente mejorar la calidad de la educación, por lo que, a través de la Ley Orgánica de Educación Superior, en sus artículos 93 y 94, establece los métodos de evaluación a las universidades y designa al CEAACES (Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior) como entidad evaluadora, implementando de esta manera un proceso de acreditación continua, a la que deben regirse las IES (Instituciones de Educación Superior) (LOES, Título IV, Capítulo 1, articulo 93-94, 2010).

La ESPOCH (Escuela Superior Politécnica de Chimborazo) siendo una institución de educación pública, ha formado parte de los procesos de acreditación nacional, actualmente obtiene la categoría B en el ranking de IES (CEAACES, 2013), posterior a las acreditaciones de las universidades e instituciones politécnicas, continúan las evaluaciones por carreras, de forma que actualmente las facultades se encuentran cursando esta etapa.

La FADE (Facultad de Administración de Empresas) para dar cumplimiento a las normativas vigentes de evaluación de calidad, ha implementado un SGI (Sistema de Gestión de Información), proyecto que cuenta con la dirección de CIMOGSYS (Centro de Investigación en Modelos de Gestión y Sistemas Informáticos), el sistema informático permite evaluar el cumplimiento de las actividades internas, proyectos e indicadores de acreditación por facultades y escuelas, esta información es clave para la administración y mejora continua de las carreras en la facultad.

El SGI no posee alta disponibilidad de información, debido a problemas como buscar puntos de conexión a internet o conectividad inalámbrica en la facultad, oficinas y dependencias, inconvenientes que retrasan la visualización de la información en cualquier momento, como una ponencia o la solución de un conflicto desde alguna localidad remota, para evitar estos impases y agilizar la gestión de información se desarrollará una aplicación móvil.

Las aplicaciones móviles facilitan mucho el día a día de los empresarios, puesto que, se han convertido en una oficina virtual, permitiendo así visualizar reportes y generar conferencias, por estos y otros beneficios una aplicación móvil disminuye el problema de disponibilidad de información, la aplicación para la FADE se desarrollará sobre Apache Cordova y estará disponible para los sistemas operativos móviles Android y iOS.

Dado que la información a mostrar en la aplicación móvil es sumamente sensible para la toma de decisiones, deberá mantener alto grado de confidencialidad e integridad, por tanto se analizarán las vulnerabilidades que conlleva el desarrollo de software en dispositivos móviles, como principal fuente de información se han considerado los estudios de NowSecure (NowSecure, Secure Mobile Development, 2015) y La OWASP (Open Web Application Security Project) (OWASP, Top Ten Mobile Risks, 2014).

Al analizar el conjunto de vulnerabilidades existentes en el desarrollo de software móvil y al no encontrar una estandarización para el mismo, el presente estudio busca emitir una propuesta de mejores prácticas de seguridad para desarrollar aplicaciones móviles, al mismo tiempo permitirá incrementar la disponibilidad de información, para tal efecto el Trabajo de Titulación se encuentra dividido en cuatro capítulos.

El primer capítulo trata de las consideraciones generales de la investigación como las principales vulnerabilidades, amenazas, riesgos, ataques y buenas prácticas de seguridad, el segundo capítulo define los problemas de seguridad en la ESPOCH así como la baja disponibilidad que posee el SGI a través de la aplicación de encuestas, el tercer capítulo recopila los resultados, análisis y discusión, finalmente el cuarto capítulo contempla el desarrollo de la propuesta de mejores prácticas de seguridad para el desarrollo de aplicaciones móviles.

## Antecedentes

Día a día las aplicaciones informáticas van evolucionado, de tal forma que existen en gran tipo, variedad, capacidad, alcance y prestaciones, pero dentro de todas ellas existen un grupo que ha venido creciendo drásticamente y destacándose de manera que están relegando a las demás, las aplicaciones móviles, y dentro de sus sistemas operativos huéspedes más populares son Android y iOS (Pastor, 2014).

Este auge ha permitido que las aplicaciones móviles y sus sistemas operativos sean el blanco perfecto para los atacantes, las vulnerabilidades son explotadas para obtener información sensible como libreta de contactos, cuentas, claves y acceso sin permiso a servicios del dispositivo, los perjuicios generados por los ataques pueden llegar a sumar pérdidas cuantiosas, como por ejemplo las aplicaciones Freedom y iAPPCracker o iAPPFree que permiten usar aplicaciones pagas o realizar compras de forma ilegal en las mismas.

Para los atacantes esta información les provee réditos, ya sea desplegando anuncios en un sistema vulnerado, vendiendo los datos del usuario o sustrayendo el saldo de la víctima, Kaspersky Lab Mobile Secure en el reporte SECURELIST (Garnaeva et al., 2015) ha detectado 103,072 programas maliciosos y 1,527 troyanos sobre aplicaciones bancarias o de pago en el primer cuarto del año 2015, en Telesemana (Telesemana, 2015) se estima que existen 16 millones de dispositivos móviles en todo el mundo que están infectados por malware además enuncia que el sistema operativo Android es afectado en similar proporción que los sistemas operativos Windows, caso contrario en BlackBerry y IOS que son menos atacados.

Docentes investigadores de la Universidad de la Plata (Macia et al., s.f., p:837-841) han determinado que, los nuevos ataques a las plataformas móviles no se enfocan solamente en la obtención de los datos sensibles del usuario, sino en la privacidad de las empresas, a esta nueva tendencia se la denomina Bring Your Own Device (BYOD) (Altirriba, 2015, p:1-12) en la cual los funcionarios pueden conectarse con sus dispositivos en sus oficinas y realizar sus actividades laborales, aunque sin tener en cuenta si su dispositivo ha sido o no infectado por algún código malicioso, esto produce un alto grado de riesgo, puesto que, si el dispositivo ha sido infectado e ingresa a la red de la institución se pueden extraer datos sensibles de la empresa.

La principal vulnerabilidad móvil según varios autores, es el usuario del dispositivo sin embargo existen más debilidades que han sido estudiadas por la OWASP (OWASP, Top Ten Mobile Risks, 2014) y NowSecure (NowSecure, Secure Mobile Development, 2015), donde se evidencian problemas en el almacenamiento de datos sensible, encriptación, inyecciones de código, mal manejo de permisos, privilegios y mala validación SSL, teniendo en cuenta que los principales problemas se dividen en 3 grupos: la red, el servidor y el dispositivo.

Dentro de las vulnerabilidades expuestas en los 3 grupos, el estudio se enfoca en la sección de aplicación principalmente, para lo cual se ha realizado una revisión de buenas prácticas sobre métodos y técnicas para el aseguramiento de aplicaciones y dispositivos móviles de las cuales se destacan: Smartphone Secure Development Guidelines for App Developers (Bansay et al., 2011), NowSecure en Secure Mobile Development y el Top Ten Mobile Risks de la OWASP (OWASP, 2014).

De igual forma se enfocarán vulnerabilidades de red y a nivel de servidor, ya que se emplean APIS de comunicación, pero existe una vulnerabilidad aislada al desarrollo de software, que es la pérdida o robo del dispositivo del usuario, en el Ecuador según la Superintendencia de Telecomunicaciones el 24 de marzo del 2014, al menos 10 de los 17 millones de celulares en el Ecuador son de procedencia ilícita (Barona, 2014), estadística que representa un problema de seguridad, problema ante el cual se deben tomar decisiones al momento de crear la aplicación.

El desconocimiento del usuario es el principal fallo de seguridad, ya que por lo general busca mejorar el rendimiento de su dispositivo móvil al máximo y recurre a técnicas que no son seguras o recomendables, como el rooteo de un teléfono Android o el jailbreak en un dispositivo con iOS (Malenkovich, 2013), acciones con las cuales, se pueden instalar aplicaciones de fuentes no confiables, en Aptoide (un repositorio no oficial Android) y Cydia para iOS la mayoría de aplicaciones solo replica el funcionamiento de una aplicación original y se añaden malware o código malicioso para explotar el dispositivo del usuario.

Según el incremento de las amenazas y vulnerabilidades móviles, se ha determinado que es necesario asegurar la información que estará disponible en la aplicación móvil del SGI, por la importancia en la toma de decisiones y el control riguroso de las evidencias, por lo que se ha determinado que la principal área a asegurar es la aplicación.

## Justificación

### Justificación Teórica

Generar una aplicación móvil para una empresa hoy en día es sinónimo de versatilidad y vanguardia, es una forma de llegar al público juvenil y tecnológico, ya que, usar un dispositivo móvil para gerenciar una empresa agiliza el proceso de toma de decisiones, pero significativamente en el ambiente del desarrollo de software, todo profesional, entusiasta y emprendedor busca incursionar en el desarrollo móvil.

Esta creciente tendencia de desarrollo ha generado una gran brecha entre lo que se debe realizar y lo que se hace, por lo tanto el software generado finalmente no posee la calidad deseada peor aún una seguridad aceptable, y es por esta razón, que al realizar una investigación de seguridad para el desarrollo móvil, aún no se ha encontrado por los autores un estándar formal, sino un conjunto de directrices que permiten incrementar la privacidad de los datos, lo que si se conoce de las aplicaciones móviles son sus vulnerabilidades según OWASP (OWASP, Top Ten Mobile Risks, 2014) y NowSecure (NowSecure, Secure Mobile Development, 2015).

Un ideal de aplicación segura es Telegram, es una aplicación de comunicación a base de mensajes de texto entre sus usuarios, su principal característica es el chat secreto en donde se menciona que posee una seguridad sumamente alta si se poseen entre dos usuarios la misma imagen clave, se basa en un algoritmo de encriptación punto a punto AES 256, que brinda la mejor privacidad a los usuarios ya que no registra datos ni logs en el servidor de Telegram.

En la Facultad de Administración de Empresas no se ha realizado anteriormente un proyecto tecnológico de esta índole, tampoco existen antecedentes que puedan servir como guía, es por esto que, para desarrollar software más seguro, se realiza la propuesta de mejores prácticas de seguridad para el desarrollo de aplicaciones móviles, dejando así un conjunto de directrices para asegurar los datos de mejor manera, tomando en cuenta el genérico de los conceptos de seguridad ningún sistema informático es completamente seguro.

### Justificación Práctica

La FADE para cumplir la evaluación por carreras se ha preparado constantemente en indicadores de acreditación, gestión y planificación estratégica, para tal efecto se han diseñado Mapas de Gestión por Procesos, Balance Score Card y Entorno de Aprendizaje con el modelo de acreditación por carreras, los mismos que permiten saber cómo se encuentra la facultad en tiempo real y con información precisa.

Para facilitar la administración, la FADE se ha visto en la necesidad de automatizar los sistemas de gestión por lo que se ha creado el SGI que abarca los sistemas de Gestión por Procesos (SGP), Balance Score Card (BSC) e Indicadores de Acreditación (SIA), sistemas que en su totalidad se encuentran publicados como aplicaciones web (http://sgc.fade.cimogsys.com).

La información provista por estos sistemas es sumamente importante para las autoridades de la Facultad, ESPOCH y CEAACES por lo que debe estar disponible siempre, según el W3C (Consorcio World Wide Web) (W3C, s.f.), la información publicada en la web debe ser accesible independientemente del lugar, tiempo y el dispositivo.

Para el W3C (W3C, s.f.) los Sistemas Informáticos SGP, BSC y SIA no son completamente accesibles, puesto que no se conoce de la existencia de aplicaciones móviles, de televisión o de automóvil (independencia de dispositivos) que puedan complementar a las aplicaciones web, además estos sistemas informáticos necesitan obligatoriamente una conexión a internet al igual que un ordenador de escritorio.

Con la finalidad de resolver el problema de disponibilidad de información se propone mediante la presente tesis de investigación realizar una aplicación móvil, la misma que permitirá incrementar las funcionalidades del SGI para la Facultad de Administración de Empresas.

## Objetivos

Para resolver los inconvenientes detectados en la FADE, tanto de disponibilidad de información así como seguridad de la misma, los autores se han propuesto objetivos que permitirán el correcto desarrollo de la investigación, estos objetivos abarcarán el estudio de seguridad, el estudio de problemas de seguridad y finalmente el problema de disponibilidad de la información sobre los criterios W3C, para lo cual se han definido los siguientes objetivos general y específicos:

### Objetivo General

Realizar una propuesta de mejores prácticas de seguridad para el desarrollo de la aplicación móvil del Sistema de Gestión de Calidad de la Facultad de Administración de Empresas con la finalidad de ofrecer una mayor disponibilidad y seguridad de la información.

### Objetivos Específicos

• Realizar un estudio de las vulnerabilidades existentes en las aplicaciones móviles.

• Realizar un estudio de las mejores prácticas de seguridad en el desarrollo de aplicaciones móviles.

• Realizar una propuesta de mejores prácticas de seguridad para el desarrollo de aplicaciones móviles.

• Implementar una aplicación móvil que contemple la propuesta de mejores prácticas emitidas por el estudio para asegurar e incrementar la disponibilidad de la información del Sistema de Gestión de Calidad.

# MARCO TEÓRICO

El siguiente capítulo permitirá definir los conceptos necesarios para la realización del estudio investigativo donde se delimitará la relación existente entre la seguridad y disponibilidad de la información por lo tanto se analizará profundamente los requisitos para que la información sea disponible de donde se encuentra la accesibilidad, dentro de la seguridad de una aplicación comprenderá las aplicaciones móviles según el concepto de independencia del W3C, que estándares de seguridad existen para estas aplicaciones y así como sus principales amenazas, vulnerabilidades y ataques, para lograr emitir una propuesta de mejores prácticas de seguridad para el desarrollo de aplicaciones móviles en la ESPOCH.

## Disponibilidad

La parte más importante de los sistemas informáticos es la disponibilidad de información, la misma que resulta de vital importancia para la toma de decisiones y los reportes que se emplean a nivel empresarial, dentro del SGC propuesto por el Centro de Investigación “CIMOGSYS” exportar el estado de los indicadores de la gestión por procesos, planificación estratégica y de planificación permiten visualizar un estado de la Facultad en tres perspectivas distintas.

Para Core One IT (2014) la disponibilidad de la información es “…es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones…” definición que delimita así el entorno donde es disponible la información, la interactividad de sistemas o aplicaciones permiten incrementar la disponibilidad de información por lo que al diseñar una aplicación móvil se ampliaría el contexto de disponibilidad del SGC.

Para Costas (2011, p. 12) la disponibilidad es: “…capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento que se necesite, evitando su pérdida o bloqueo…” a más de ser disponible para cualquier persona o proceso se incrementan los campos de influencia esta definición nos permite añadir criterios de autorización (usuarios) así como también de medidas de seguridad como pérdida del dispositivo en donde las acciones a tomar implicarían inhabilitar el dispositivo para proteger sus datos.

Para TAO de la empresa T-Systems (s.f.) alta disponibilidad es: “… diseñar e implantar las tecnologías y conjunto de medidas y actuaciones necesarias que permitan garantizar el acceso de los usuarios a los servicios las 24 horas del día…”. TAO permite conocer cuál es una de las principales medidas a las que debe adecuarse la disponibilidad de información en base al tiempo con el paradigma genérico 24/7 de la misma manera que proporciona como definición DAMITEL Networks (s.f.) que define alta disponibilidad como: “… asegurar que el servicio funcione 24 horas del día…”

La disponibilidad de la información es la capacidad que posee un usuario autorizado de utilizar y acceder a la información las 24 horas del día en los 7 días de la semana independientemente del lugar, momento o seguridad de la aplicación que la contenga, características que toda aplicación debe poseer.

## Accesibilidad

La accesibilidad es la facilidad que brinda un espacio físico, herramienta o producto para que los usuarios puedan hacer uso de ellos bajo las mismas condiciones, tomando en cuenta que el mundo existe mucha diversidad en cuanto a las personas, sus capacidades y la forma de ver las cosas es indispensable que de alguna u otra forma todo se equipare y brinde igualdad.

Para la Confederación Española de Personas con Discapacidad Física y Orgánica a través del proyecto Observatorio de la Accesibilidad enuncia que la accesibilidad es un factor fundamental para un 10 % de la población, para un 40 % es necesario y para el 100 % es confortable aludiendo así que para todos es necesario cualquier nivel de accesibilidad aún si no es necesaria permite un mayor grado de comodidad y la define accesibilidad como:

*“… aquella condición que deben cumplir los entornos, procesos, bienes, productos y servicios, así como los objetos o instrumentos, herramientas y dispositivos, para ser comprensibles, utilizables y practicables por todas las personas en condiciones de seguridad, comodidad y de la forma más autónoma y natural posible…”* (Observatorio de la Accesibilidad, 2015).

Dentro de las característica esenciales de la accesibilidad se encuentra la seguridad y comodidad, dos puntos que pueden ser interpretados desde una gran amplitud de perspectivas por los que por ejemplo si se habla de infraestructura se referirá a seguridad de muebles e inmuebles de que las edificaciones o estructuras no hagan daño o provoquen lesiones físicas a los usuarios como el proceso de renovación de infraestructura que viene la ESPOCH actualmente incrementando la accesibilidad a las personas que usan silla de ruedas pero otra perspectiva en el ámbito de software es la seguridad de los datos desde el punto de vista que ataques a nuestras aplicaciones o servidor donde si las seguridades fallas será imposible acceder a ellas.

Para la Ley Española 51/2003 artículo 8 inciso b la accesibilidad está definida por principios similares a los del Observatorio de la Accesibilidad pero con un adicional presupone la estrategia de diseño para todo y se entiende sin perjuicio de los ajustes razonables que deban adoptarse, por lo general esto se enmarca mucho en el ámbito del desarrollo web en donde muchos de los efectos así como de las animaciones dependen de los eventos que manejen los agentes principalmente el efecto hover, el mismo que se vuelve excluyente para personas con problemas motrices.

El mayor de los organismos que emiten estándares web es el W3C, el cual emite como política de accesibilidad universal de los dispositivos como el acceso a la información en cualquier momento lugar y dispositivo, su principal estándar es el WCAG 2.0 y el WAI ARIA los mismo s que disminuyen las barreras para las personas con capacidades especiales, estas políticas gobiernan el desarrollo web e incluyen a personas que poseen problemas visuales, mentales, motrices y auditivos.

Es por esta razón que como base fundamental de la accesibilidad de empleará el concepto del Consorcio W3C donde intervienen el tiempo, lugar y dispositivo siendo analizado el tiempo como una disponibilidad de durante los horarios de trabajo y fuera de los mismos, el lugar haciendo referencia a la localización geográfica conexiones a internet y energía, finalmente los dispositivos que incluyen desde televisores hasta automóviles inteligentes; el factor de seguridad se analizará dentro de la creación de la propuesta de mejores prácticas de seguridad completando así el concepto de disponibilidad de información.

## Buenas Prácticas, Normas y Estándares

Pese a que casi la totalidad de las áreas del desarrollo de software se encuentran normadas y reguladas, la seguridad de las aplicaciones móviles no es un tema completamente parametrizado, ya que, por su reciente auge e importancia muchas personas intentan crear aplicaciones para sus empresas o negocios, y aun mayor el número de desarrolladores que incursionan en este nuevo campo, al no existir ninguna normativa realmente aplicable, cada organización desarrolla software móvil bajo sus lineamientos.

Es por ello que se busca constantemente estandarizar el procedimiento para asegurar la información, de modo que el primer paso será analizar las buenas prácticas que emplean las empresas para lograr tal cometido, una buena práctica, mejor práctica o best practice como se le conoce en el idioma inglés es por lo general un término genérico que emplean las instituciones que buscan un alto nivel de calidad en los productos o servicios que ofertan a sus clientes.

El Instituto Moderno de Mejores Prácticas Corporativas define la mejor práctica como: “… Una serie de metodologías, sistemas, herramientas, y técnicas aplicadas y aprobadas con resultados sobresalientes en empresas que han sido reconocidas como de clase mundial…”. (Instituto Moderno De Mejores Prácticas Corporativas, s.f.).

Esta definición se emplea en el ámbito de benchmarking en las entidades que ofertan productos, puesto que consiste en buscar las mejores prácticas para incorporarlas en negocios nacientes y es algo que permite un rápido crecimiento, pero no es muy aplicable a un producto informático, si bien es cierto que se pueden obtener las mejores aplicaciones y ver cómo éstas funcionan, no es muy común verificar como fueron construidas, mucho menos verificar cuáles son sus políticas de seguridad.

De la misma manera la Organización de Naciones Unidas para la Alimentación y Agricultura definen una buena práctica como:

*“ … Una buena práctica no es tan sólo una práctica que se define buena en sí misma, sino que es una práctica que se ha demostrado que funciona bien y produce buenos resultados, y, por lo tanto, se recomienda como modelo. Se trata de una experiencia exitosa, que ha sido probada y validada, en un sentido amplio, que se ha repetido y que merece ser compartida con el fin de ser adoptada por el mayor número posible de personas…”* (FAO, 2015, p: 1).

Una buena práctica, como tal, siempre debe ser compartida como principio filosófico como es el caso del software libre, sin embargo en el campo profesional son los pequeños secretos del desarrollo de software que generan más de dinero, y es que, es un adicional que nuestro software tenga alguna funcionalidad distinta que impacte en el usuario, en el ámbito de seguridad informática compartir nuestra fortaleza es obtener una vulnerabilidad.

Así como los desarrolladores buscan seguridad hay personas que reciben remuneración por encontrar vulnerabilidades, parcialmente es beneficioso ya que podremos mejorar nuestra aplicación, hacerla más confiable, pero cuando se hallan amenazas y sirven para robar nuestros datos ya es perjudicial.

En el documento de Buenas Prácticas Profesionales para el Apoyo a la Parentalidad Positiva se define una buena práctica como: “La referencia a las formas óptimas de ejecutar un proceso que pueden servir de modelo para otras organizaciones” (Rodrigo et al., 2011, p: 1-29). Por lo general estas referencias se encuentran en blogs, foros o comunidades de desarrollo de software como es el caso de Stack Overflow (http://stackoverflow.com/) en el que se ofrece ayuda a los desarrolladores y por lo general las soluciones exitosas son compartidas

Para el presente estudio de manera formal se tomará como fundamento el segundo concepto logrando así la siguiente definición: Buena Práctica es una experiencia validada que funciona bien y produce buenos resultados, ha sido exitosa en un sentido amplio, que se ha repetido y merece ser compartida.

Existen 3 fuentes principales de buenas prácticas que son organizaciones que se han dedicado al desarrollo de software como su principal actividad como por ejemplo la empresa NowSecure que se dedica al testeo de aplicaciones móviles mediante una herramienta online, la Open Web Application Security Project que es una entidad mundial que se dedica a la seguridad web y la empresa europea ENISA, de las cuales nacen las políticas Secure Mobile Development, Top ten Mobile Risks y Smartphone Secure Development Guidelines for App Developers respectivamente.

La principal característica de estas políticas de seguridad es que se enfocan claramente en el desarrollo de aplicaciones móviles en los sistemas operativos Android y iOS, siendo estos los más populares en el mercado por lo tanto no se conocen al momento prácticas que permitan asegurar de forma genérica la creación de este tipo de aplicaciones, los fabricantes Google y Apple también aconsejan seguir sus propias directrices pero en este caso en particular no serán de mucha ayuda ya que no son aplicaciones nativas sino hibridas.

Como ejemplo de buenas prácticas de seguridad móvil tenemos Secure Mobile Development de la Empresa NowSecure que ha venido identificando vulnerabilidades al ofrecer servicios de testeo de aplicaciones móviles y a su vez emitiendo recomendaciones de como repararlas, otro ejemplo es Mobile Security Project – Top Ten Mobile Risks de Open Web Application Security Project (OWASP) que es un proyecto en el cual anualmente se registran las 10 principales vulnerabilidades móviles y de la misma forma como asegurarlas, la OWASP es comunidad mundial que impulsa la visibilidad, evolución en la seguridad y protección de software del mundo.

Una buena práctica como tal, no es más que una experiencia validada y exitosa que merece ser compartida de forma general, pero esta es una opción para quien desee implementarla, y es por este motivo que no se logra una generalización de procesos, a más de ello, el aplicar una buena práctica no es ningún respaldo para la empresa de realizar correctamente sus actividades, caso contrario sucede con los estándares que ya pueden ser formalmente implementadas, reconocidas, y comúnmente son un requisito a cumplir.

El W3C define un estándar como:

*“… Un conjunto de reglas normalizadas que describen los requisitos que deben ser cumplidos por un producto, proceso o servicio, con el objetivo de establecer un mecanismo base para permitir que distintos elementos hardware o software que lo utilicen, sean compatibles entre sí...”* (W3C, Guía Breve sobre Estándares Web, s.f.)

Cuando se genera un estándar se busca que todos los elementos que lo usen independientemente de su funcionamiento, plataforma o diseño puedan comunicarse entre sí o generar compatibilidad, con ello disminuir las limitantes que generalmente se presentan cuando tenemos distintos proveedores de un mismo producto como por ejemplo el desarrollo web en donde se pueden crear aplicaciones en distintos lenguajes de programación, aunque hoy en día todos emiten actualmente información en el estándar de páginas web HTML y frecuentemente en el estándar de estructura de documentos XML.

Evelio Martínez proporciona la siguiente definición de estándar:

*“… Los estándares son acuerdos (normas) documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características. Para asegurar que los materiales productos, procesos y servicios se ajusten a su propósito… ”* (Martínez, s.f.).

Los estándares son definidos de acuerdo a las organizaciones, que por lo general se reúnen y en consenso delimitan sus necesidades y las generalizan, como consecuencia se genera un documento formal que es publicado, estas dos definiciones citadas marcan un contraste significativo pero en abstracción similar uniformidad, en la primera definición se busca la compatibilidad y la segunda busca la armonía de un objeto para cumplir su función.

Frecuentemente es común el confundir la palabra estándar con norma, puesto que las distintas traducciones entre lenguajes varían su connotación, en el Instituto Ecuatoriano de Normalización definen el termino norma como: “… documento, establecido por consenso y aprobado por un organismo reconocido, que proporciona, para uso común y repetido, reglas, instrucciones o características para actividades o sus resultados garantizando un nivel óptimo de orden en un contexto dado…” (INEN, GPE INEN-ISO/IEC 2:2006, 2006).

A vista del presente estudio y analizados los conceptos de estándar y norma, se mantendrá el siguiente concepto de norma: Una norma es una recopilación de estándares publicados como un documento formal que satisface las necesidades de grupos de interés como personas, empresas o naciones que se dedican a una actividad particular con el fin de proporcionar reglas, instrucciones o características para garantizar resultados con un óptimo nivel de calidad.

Estos estándares y normas no buscan otra cosa que no sea mejorar la calidad del producto final, los dos organismos más importantes en el campo de las estandarizaciones son el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y la Organización Internacional de Estandarización (ISO), en el Ecuador para criterios de normalización se ha creado el Servicio Ecuatoriano de Normalización.

Dentro de lo que es la ingeniería de software y respecto al ámbito de seguridades de sistemas informáticos o de sistemas de información el estándar más relevante es el ISO/IEC 27001:2013, norma que “… proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información… ” (ISO, ISO/IEC 27001:2013).

Hasta el momento de la revisión bibliográfica los autores no han podido detectar normas y estándares establecidos para el desarrollo de aplicaciones móviles o sistemas informáticos de forma genérica, sino que, cada organización ha optado por ir cubriendo sus necesidades a medida que surgen problemas, por lo que se emplearán las buenas prácticas mencionadas como una base para emitir una propuesta de seguridades para crear aplicaciones móviles híbridas y como pilar fundamental se empleará la norma ISO/ICE 27001:2013 aceptada y vigente en el Ecuador.

## Dispositivo Móvil

De la misma forma que se ha delimitado cómo y por qué utilizar buenas prácticas, estándares y normas para mejorar la calidad, compatibilidad de productos y servicios, ahora se analizarán los conceptos sobre dispositivo móvil, sistemas operativos móviles, aplicaciones móviles.

Los dispositivos móviles se remontan a la aparición de la telefonía celular, así como los reproductores walkman y mp3 portables, hoy en día hacen referencia al uso de tabletas, PDA, celulares inteligentes, según Alexander García (García, 2011) un dispositivo móvil es “cualquier dispositivo que se pueda utilizar mientras el usuario se encuentra en movimiento”. Así mismo para cumplir este concepto propone las siguientes limitantes a estos dispositivos:

* “… *Capacidad de memoria.*
* *CPU de bajo/medio poder.*
* *Pantallas pequeñas y de baja resolución.*
* *Duración de las baterías.*
* *Mecanismos limitados para la entrada (interfaces) de datos.*
* *Heterogeneidad de plataformas operativas.*
* *Soporte a las herramientas de desarrollo de terceros.*
* *Ancho de banda limitado (hasta la 2.75 G).*
* *Problemas de desconexión temporal a la red…*”

Ya se ha superado por mucho las limitantes mencionadas, si al menos tenemos en cuenta que estamos operando celulares con un ancho de banda de hasta 4G con características potentes como procesadores que poseen varios núcleos lógicos, ancho de banda y conectividad inalámbrica en diversos estándares y frecuencias, cámaras con una resolución de hasta 1080 HD y almacenamiento expandible, a más de un diseño moderno y jovial, son características que poseen hoy en dia muchos de los dispositivos móviles que se comercializan en el mercado, estos aspectos han revolucionado el concepto de dispositivo móvil.

La heterogeneidad de plataformas operativas con las que funcionan los dispositivos y las empresas que cada día buscan estar a la vanguardia, también se han encaminado a la filosofía móvil existiendo así varios sistemas operativos como Android, iOS, Windows Phone, Firefox OS, entre otros, si analizamos esta diversidad habría un sistema operativo móvil por fabricante de dispositivos que de ahí surge la interrogante ¿Cómo construir un software compatible con tal diversidad de entornos?

Para Patricia Delgadillo et al., un dispositivo móvil es:

“… *Un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales…*” (Delgadillo, 2015, p: 7-23).

Los dispositivos pueden variar de tamaño dependiendo de su diseño, fabricante y propósito es cierto que suelen ser de pequeños por su usabilidad, portabilidad y manejo como por ejemplo los celulares y celulares inteligentes (Smartphone) pero hay consumidores más exigentes que también procuran tener una pantalla más amplia he ahí el surgimiento de las tabletas y phablets (híbrido de Tablet y Smartphone) cuyos tamaños varían con pantallas de hasta las 13 pulgadas (Ipad Pro), con lo cual la relación del término pequeño aparato ya no sería aceptable.

Según César Tardáguila (2009) se puede definir a un dispositivo móvil como “… micro-ordenadores que son lo suficientemente ligeros como para ser transportados por una persona, y que disponen de la capacidad de batería suficiente como para poder funcionar de forma autónoma…”.

Generalizando estos tres conceptos se puede actualmente definir a un dispositivo móvil como un dispositivo de pequeña dimensión y peso, que posee gran capacidad de procesamiento y conectividad, que puede ser empleado mientras el usuario se encuentra en movimiento para cumplir funciones generales y específicas.

Algunos ejemplos de tipos de dispositivos móviles son:

* Dispositivos Multimedia
* Teléfonos Móviles
* Teléfonos Inteligentes
* PDA (Personal Device Assistant)
* Tabletas
* Phablets
* Relojes Inteligentes
* Consolas (Video Juegos)
* Lectores de Libros

Estos ejemplos son mencionados por César Tardáguila a excepción de los dispositivos multimedia como mp3, las phablets y los relojes inteligentes, que han surgido en el transcurso de los últimos años.

Las personas en la actualidad ven al dispositivo móvil como una oficina portable ya que se puede editar documentos, realizar video conferencias, cargar y descargar archivos, conectarse a las redes sociales, estar al día en los más importantes acontecimientos y hasta gestionar su propia empresa, existiendo tantos tipos de dispositivos móviles con un uso tan importante es necesario dominar las tendencias de seguridad para poder ofrecer un mejor soporte y confianza en nuestros usuarios.

## Sistema Operativo Móvil

Todo dispositivo móvil para ofertar servicios debe ser operable de forma que debe implementar un sistema operativo apto para dicho dispositivo según sus características, para Abraham Silberschatz (2006, p: 3) un sistema operativo “…es un programa que administra el hardware de una computadora. También proporciona las bases para los programas de aplicación y actúa como un intermediario entre el usuario y el hardware de la computadora…”.

Este concepto se aplica a cualquier dispositivo, ordenador, que use un sistema operativo puesto que es la comunicación esencial entre el hardware, software y el usuario, teniendo en cuenta que ya se ha definido al dispositivo móvil como un ordenador pequeño potente con gran capacidad de procesamiento de información.

Dentro de los dispositivos móviles los usuarios poseen una serie de sistemas operativos a su elección de entre los más populares se encuentran Android de Google, Windows Phone OS de Microsoft y iOS de Apple los mismo que se distribuyen junto a la gran variedad de productos que estas empresas comercializan, por ejemplo iOS se distribuye en iPhone y iPads mientras que Android es distribuido junto con dispositivos Samsung finalmente Windows Phone en Nokia.

Según Mobile Overview Report (ScientiaMobile, 2015, p: 1-32) el sistema operativo más popular en Sudamérica para Smartphones es Android con un porcentaje del 87% seguido de iOS con un 11% datos que han sido recopilados a junio del 2015 por ScientiaMobile, de la misma forma Statista (2015) considera a Android como el más popular en el mercado móvil.

Estos datos pueden estar sujetos a una dependencia social o económica es decir los usuarios se verán más atraídos por los productos y las prestaciones ofertados entre las empresas dependiendo a su necesidad o poder adquisitivo pero sin duda estos dos sistemas operativos son los más buscados y serán en los cuales se centre el estudio de políticas de seguridad.

## Aplicación Móvil

El sistema operativo no es una capa aislada sino que es una plataforma sobre la cual se pueden instalar y configurar un conjunto de herramientas (aplicaciones), hoy en día sobre Android y iOS ha proliferado la venta de aplicaciones, si bien es cierto sobre los sistemas operativos de escritorio ya se realizaba este tipo de actividades (como por ejemplo la venta de antivirus) no es tan común que exista una variedad tal como en los repositorios Google Play y AppStore.

Una aplicación no es más que un conjunto de instrucciones que son compiladas por un sistema operativo y hace uso de este, para realizar tareas generales o específicas que permiten al usuario resolver un problema determinado, existen tres tipos de aplicaciones móviles que son:

* Aplicaciones Nativas.- Aquellas aplicaciones que son desarrolladas para funcionar en un sistema operativo móvil en específico como por ejemplo para iOS desarrollo en Objective-C, Android desarrollo en Java o Windows Phone desarrollo en .NET, adicionalmente la ventaja de estas aplicaciones es que permite usar el hardware del dispositivo con mayor efectividad, son distribuidas al usuario mediante las tiendas formales como AppStore o Google Play (Delia Lisandro et al., 2013, p: 1-11).
* Aplicaciones Web.-Es una aplicación que se puede ejecutar de forma correcta en un dispositivo móvil a través de un navegador, necesariamente debe poseer una conexión a internet para su funcionamiento este tipo de aplicaciones no se distribuyen por una tienda sino que son los propios fabricantes quienes deben distribuirla independientemente, estas aplicaciones no poseen limitantes en cuanto a sistema operativo móvil ni poseen instaladores. Son construidas a base de lenguajes de programaciones web y presentadas mediante maquetación con HTML 5, JavaScript y CSS3.

Es difícil encontrar aplicaciones web que puedan hacer uso del hardware del dispositivo, razón por la cual no son vistas como un producto vendible pero si de gran utilidad en la accesibilidad y usabilidad web, esto es posible hoy en día al cambio del sistema de maquetación de las aplicaciones ya que se ha dejado atrás el diseño perfect pixel o adaptativo y se usa el diseño web responsivo ideal para un browser móvil (Delia Lisandro et al., 2013, p: 1-11).

* Híbridas.- Las aplicaciones móviles hibridas son realizadas mediante lenguajes de maquetación como HTML 5 y CSS3 en conjunto con JavaScript, estas aplicaciones pueden ser compiladas por alguna herramienta como Apache Cordova. Este tipo de aplicaciones posee la ventaja de independencia de plataforma y el uso de recursos hardware del dispositivo, esta mezcla de lenguajes es permitida y funciona gracias a la conjunción del diseño web responsivo y al compilador que traduce en forma nativa para generar instaladores (Delia Lisandro et al., 2013, p: 1-11).

Hoy en día las aplicaciones móviles tienen propósitos tan diversos que categorizarlos sería es un problema, brevemente por ejemplo en Google Play (https://play.google.com/store/apps) se las categoriza de la siguiente manera:

* Bibliotecas
* Comics
* Compras
* Comunicación
* Deportes
* Educación
* Empresa
* Entretenimiento
* Estilo de Vida
* Finanzas
* Fondos Animados
* Fotografía
* Herramientas
* Libros
* Medicina
* Multimedia y video
* Música y audio
* Juegos
* Familia

Esta diversidad ha permitido que se cree el mercado de las aplicaciones móviles, cada aplicación provee al usuario de una solución en específico, este abanico de posibilidades ha generado ingresos cuantiosos a las grandes empresas de desarrollo y de igual forma se han generado un sin número de falsificaciones.

Repositorios no oficiales como Aptoide o Cydia ofrecen a sus usuarios aplicaciones pagas de forma gratuita, Freedom para aplicaciones Android permite hacer compras ilícitas dentro de juegos específicamente. Estos medios son los propicios para trasmitir o generar vulnerabilidades en nuestras aplicaciones o dispositivo y un riesgo para los desarrolladores de software.

Realizar un estudio específico de cada una de las aplicaciones móviles en su sistema operativo huésped, parchar cada una de las vulnerabilidades y amenazas encontradas en el desarrollo y testeo de la misma sería realmente complicado y es por esto que se dejan relegadas las aplicaciones nativas para este estudio y se optan por generalizar los conceptos de seguridad a una sola aplicación hibrida que será distribuida y debe funcionar correctamente en cada dispositivo.

## Vulnerabilidad

Las empresas para seguir este ritmo de avance tecnológico vertiginoso, de oferta y demanda de aplicaciones móviles, busca en menor tiempo estar a la vanguardia en las exigencias de sus usuarios pero esto abre las brechas a contrataciones apuradas e indebidas en incluso por abaratar costos y tiempo se busca soluciones que no son confiables.

De igual forma a esta demanda de tecnología de software existe una oferta a la medida de profesionales, aficionados o conocedores del mundo móvil que suplen estas necesidades, pero si no se está capacitado o no se domina el desarrollo de software se crearán problemas en las soluciones ya sean de usabilidad, escalabilidad, funcionamiento y seguridad que muchas veces es transparente al usuario.

Para detectar un problema de seguridad generalmente se buscan vulnerabilidades en el software ya sea una aplicación (móvil, web o escritorio) o un sistema informático, según Ester Chicano (2014, p:1-316) una vulnerabilidad es “… una característica o capacidad de un activo del sistema de información que lo hace susceptible a amenazas…”, generalmente no se ve a una vulnerabilidad como una característica sino como un problema de seguridad que debe ser solucionado, ocurren por el desconocimiento de las metodologías de desarrollo de software, mal manejo de las tendencias de desarrollo o simplemente no se realiza una etapa de pruebas al software a implementar.

De igual forma para la empresa antivirus NORTON (Cómo atacan: Vulnerabilidades, 2015) las vulnerabilidades son “… imperfecciones del programa informático que crean debilidades en la seguridad general del equipo o la red…”, NORTON maneja un concepto más amplio que solo la aplicación ya que menciona el medio de transporte de los datos en la red de comunicación, generalmente fallos en este medio provocan vulnerabilidades y ataques de tipo “… man in the middle…”, en el mismo que si nuestros datos no viajan de forma segura pueden ser visualizados por cualquier intruso.

Se definirá a una vulnerabilidad como una imperfección de software que se puede generar en tres componentes el servidor, la red de comunicación y la aplicación, imperfección que hace al conjunto de componentes susceptibles a amenazas, que debe ser reparado en un tiempo mínimo desde su detección, por lo tanto el éxito para realizar un sistema informático confiable será reducir a cero todas las vulnerabilidades existentes, hecho que es un ideal ya que no existe sistema informático totalmente seguro.

Para la W3C las vulnerabilidades se encuentran se producen por:

* Controles débiles en el servidor
* Almacenamiento inseguro de datos
* Seguridad débil en la capa de transporte
* Fuga de datos involuntaria
* Pobre Autenticación y Autorización
* Ruptura de criptografía
* Inyección del lado del cliente
* Decisiones de seguridad de datos no fiables
* Mal manejo de sesiones
* Falta de Protección de archivos binarios

En cuanto a una aplicación móvil las vulnerabilidades según NowSecure (NowSecure, Secure Mobile Development, 2015) se producen por:

* Controles pobres del lado del servidor
* Almacenamiento de datos inseguro
* Insuficiente protección en la capa de transporte
* Fuga de datos involuntaria
* Pobre autenticación y validación
* Ruptura de criptografía
* Inyección del lado del cliente
* Decisiones de seguridad sobre entradas no fiables
* Manejo inadecuado de sesiones
* Falta de protección en los archivos binarios.

Al analizar las áreas de impacto sobre las cuales se producen las vulnerabilidades tomamos en cuenta que contempla todo el ámbito de desarrollo de software desde el nivel de aplicación hasta el nivel de servidor por lo que es muy importante generar directrices que permitan asegurar el almacenamiento de la información en el dispositivo, que cifren los datos que viajan a través de la red de comunicación así como verificar bien los procesos de autenticación y autorización por lo que la propuesta de mejores prácticas incluirá controles para evitar estas vulnerabilidades especialmente dos aspectos importantes como los archivos binarios y la pérdida del dispositivo.

## Amenaza

Una amenaza para Ester Chicano (2014, p:1-316) es “… un conjunto de hechos y eventos que pueden ocurrir y que pueden provocar efectos perjudiciales a los activos del sistema de información…”, hechos y eventos que no dependen de una condición determinada por ejemplo una amenaza puede surgir por un problema del proveedor de servicios que suple a la empresa o una falla detectada recientemente en las herramientas que se emplean para el desarrollo de software, no necesariamente debe ser considerado como un error interno de producción es por ello que nuestros activos de información son sumamente sensibles y expuestos a factores ajenos a nuestro conocimiento.

Un activo de información a su vez según la norma ISO 27001 se refiere a “… cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización…”, los activos de información son: datos digitales (bases de datos, copias de seguridad), activos tangibles (correos, fax, libros), activos intangibles (patentes), software, sistemas operativos (ISOTOOLS EXCELLENCE, 2013).

Por lo general cuando se presentan amenazas el equipo a cargo debe analizar cuáles son las prioridades en los activos de información, que debe asegurarse de mejor manera o mantener bajo un celo importante, al hablar de activos de información nos preocuparemos en este momento de aquellos activos que son digitales e intangibles puesto que mediante una aplicación o un ataque de red sería extremadamente difícil extraer un documento impreso de un archivador.

Dentro de los activos digitales nuestra principal preocupación será el manejo de una conexión segura a la base de datos y el debido respaldo de la misma, dentro de los activos intangibles la aplicación a desarrollarse deberá tener la capacidad suficiente para reaccionar ante la eventualidad de una amenaza.

Para el Ministerio de Salud de Buenos Aires (Conceptos Básicos de la Gestión de Riesgos, 2015) una amenaza es considerada como “… cualquier factor externo de riesgo con potencial para provocar daños sociales, ambientales y económicos en una comunidad durante determinado periodo de tiempo, clasificados en amenazas naturales, humanas y mixtas…”, este punto de vista es una análisis más completo debido a que los activos de información no solo están expuestos a amenazas humanas sino a problemas naturales siendo los problemas naturales los más difíciles de predecir y cuantificar.

En el ámbito informático o en el desarrollo de software estas amenazas son mucho más comunes de lo que podrían parecer, las amenazas sociales se producen cuando un sitio de confianza como un portal web de un medio de comunicación es vulnerado y se trasmite información errónea a través del mundo con lo que podría desestabilizar a un sector país o nación, el aspecto económico los sistemas bancarios en su defecto son los blancos de ataque, del cual se puede sustraer dinero mediante las transacciones en línea al atacar a un usuario como por ejemplo a través de Phishing.

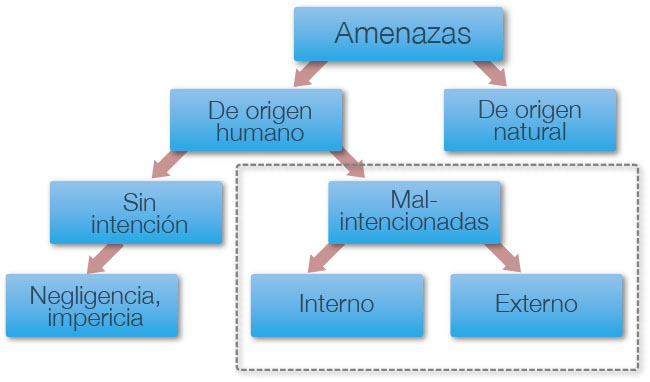


Figura 1‑1 Tipos de Amenazas Informáticas

Fuente: http://www.magazcitum.com.mx/?p=2193#.VfxmLN9\_Oko

Según la clasificación de las amenazas para el Ministerio de Salud de buenos Aires como para la Figura 1-1 de PRANDINI y PALLERO existen dos tipos de amenazas marcadas las humanas causadas probablemente por negligencia o un ataque dirigido y las naturales causadas por desastres, pero no se toma en consideración una amenaza de software si bien es cierto es producida por el hombre no es contemplada en la clasificación de manera formal.

Las amenazas por software generalmente vienen originadas por amenazas humanas externas malintencionadas que infectas a nuestros sistemas informáticos con código malicioso para obtener un objetivo, las principales amenazas de software son por ejemplo los virus, los troyanos, malware, spyware, entre otros los mismos que día a día se producen y fabrican, todo este conjunto de amenazas pueden convertirse en factores de riesgo para la organización.

Las amenazas en el mundo informático son realmente incalculables e impredecibles sin tomar en cuenta que nunca se sabe de donde provienen pero si es claro lo que buscan información por lo que para evitar que puedan convertirse en un problema para la organización se generarán controles que minimicen estos impacto, con respecto la seguridad física y amenazas naturales ya depende de la seguridad del proveedor de hosting que ha sido contratado puesto que es una solución en la nube, sobre las amenazas de software se ha implementado un firewall en el servidor así como controles y rutas, finalmente se deberán considerar las amenazas a nivel de aplicación.

## Gestión del Riesgo

La ISO/Guide 73:2009 define un riesgo como un “… efecto de la incertidumbre sobre los objetivos…”, donde los objetivos son los intereses que se busca obtener estos pueden ser económicos, sociales, e inclusive militares, en el caso de la aplicación móvil del sistema de gestión de calidad sería la exposición del estado de sus indicadores, acciones de mejora y planes de contingencia ya que estos datos son sensible en la toma de decisiones de la Facultad de Administración de Empresas.

Se define además incertidumbre como “… la deficiencia de información relacionada al conocimiento de un evento, consecuencia y probabilidad…” (ISO/Guide 73:2009, Nota 5), esta incertidumbre debe ser cuantificada es ahí donde entra la medición del riego, si bien es cierto en un principio no se conoce muchos datos hacerla de los eventos que pueden suscitarse es lo más recomendable evitar la ocurrencia de los mismos (probabilidad) y su impacto (consecuencias).

Según Marcelo Cartaya (2014, p: 1-94) el riesgo “… es la probabilidad de que una o varias amenazas se convierta en un desastre…”, al hablar de las magnitudes de los eventos un desastre posee un impacto mucho mayor en la organización que el de una amenaza detectada tenido teóricamente una probabilidad mucho menor de ocurrencia, por lo que ya genera motivo de preocupación y alarma.

Para TENSTEP el riesgo se refiere a “… condiciones o circunstancias futuras que existen fuera del control del equipo de proyecto y que tendrán un impacto adverso en el proyecto si se llegan a presentar…” (Metodología TenStep, s.f.). Todas las definiciones citas hacen mención a que un riesgo no posee una predicción futura de impacto y ocurrencia, mucho menos los factores involucrados en el mismo, de forma genérica un riesgo puede ser definido como la incertidumbre que reposa sobre una amenaza, que de materializarse provocará consecuencias negativas sobre los activos de información de la organización.

Para evitar que un riesgo se convierta en un problema incontrolable o tenga efectos devastadores se debe gestionar el mismo, para evitar su ocurrencia o, a su vez, que cause el menor impacto posible sobre los activos de información, según TENSTEP el propósito de la gestión de riesgos es “…identificar los eventos de riesgo dentro de un proyecto y establecer un plan de gestión de riesgo para disminuir la posibilidad de que un evento riesgoso dañe el proyecto…” (Metodología TenStep, s.f.).

TENSTEP lo que busca con su filosofía es disminuir la probabilidad que un riesgo se produzca, identificar los eventos involucrados como causa, efectos, daños colaterales en el proyecto implicado en el desarrollo de software de forma similar se debe identificar que parte del código puede verse afectado, que volumen de información está implicada y cuánto daño puede producir ese efecto sobre el total del aplicativo, al determinar este impacto se juega un efecto dominó que arrastra a la organización al problema.

Para ISOTOOLS Excellence (Las Claves del Éxito para la Gestión de Riesgo, s.f., p: 1-8) gestionar un riesgo significa “… identificar los riesgos que afectan a la organización y establecer medidas de seguridad para reducir estos riesgos…”. Todo plan de gestión de riesgos busca generar medidas, políticas, metodologías de cómo se deben reducir los riesgos pero generalmente estos ciclos comprende procesos organizacionales y no procesos de construcción de herramientas por lo que es necesario particularizar cada punto de las metodologías existentes fin de que se ajuste a las necesidades del producto.

Existen diversas metodologías para la gestión de riesgos como por ejemplo según ISOTOOLS Excellence (Las Claves del Éxito para la Gestión de Riesgo, s.f., p: 1-8) son: MAGERIT, CRAMM, OCTAVE, NIST 800-03, ISO 27005 e ISO 31000, dado a que el Gobierno Ecuatoriano a través del Servicio Ecuatoriano de Normalización hace referencia principal a las normas ISO se tomarán en consideración la norma ISO 27000 por generar sistemas de gestión de información seguros en cambio la ISO 31000 gestiona riesgos a nivel de cualquier empresas sin importar su objetivo, a más de que la propuesta trata sobre mejores prácticas de seguridad sobre una aplicación informática.

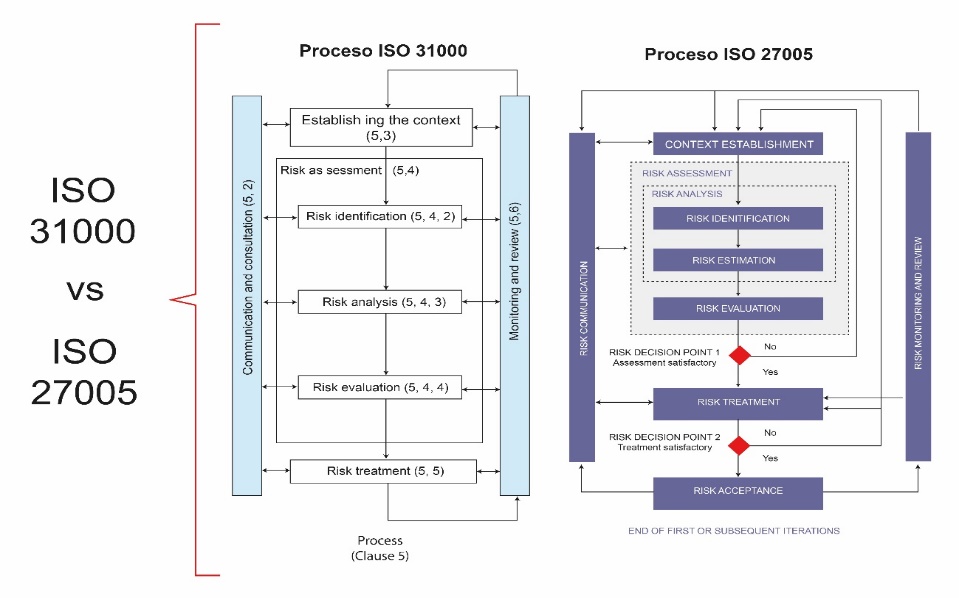


Figura 1‑2 Ciclo de Vida ISO 27005 vs ISO 31000

Fuente: http://es.slideshare.net/besair/gestion-de-riesgos-de-seguridad-de-la-informacion-iso-27005

Pese a realizar la discriminación de las metodologías de gestión de riegos a los sistemas informáticos podemos notar en la Figura 1-2 que los ciclos de vida de las dos normas ISO no son muy distintas entre sí, la diferencia notoria se produce en la estimación del riesgo y como consecuencia el nivel de aceptación del mismo que se maneja en la norma ISO 27000, es decir la empresa puede determinar qué nivel de riesgo puede manejar según sus políticas organizacionales, en la aplicación móvil será de suma importancia determinar este componente, el mismo que se analizará luego de tratar el riesgo si este indicador es demasiado elevado se debe seguir tratando el riesgo.

Los ciclos de vida genéricos de la gestión de riesgos comprenden identificar, evaluar y tratar el riesgo, al identificar el riesgo se verifican las amenazas y vulnerabilidad que los activos de información pueden poseer, para NOWSECURE (Secure Mobile Development, 2014) los principales riesgos para un dispositivo móvil son los siguientes puntos de entrada:

* Navegadores, mail, aplicaciones precargadas.
* Teléfono/SMS.
* Aplicaciones de terceros.
* Sistema Operativo.
* Conectividad por ancho de banda, bluetooth, y canales comm.
* Ataques basados en navegadores.

Como se puede determinar en las 3 categorías de vulnerabilidad no se presenta un patrón único ni una agrupación representativa por lo que es difícil generar una metodología de análisis de riesgos en las aplicaciones móviles, y peor aún sin tomar en consideración su medio ambiente es por ello que se tomará como punto de partida la distribución existente en la Figura 1-1 que generaliza las áreas de impacto en Servidor, Red y Aplicación de entras las cuales en el servidor y la red no se profundizará más allá de los requerimientos necesarios para el funcionamiento de la aplicación.

Se analizará la seguridad de todo el servidor en sí o la red de transmisión pero sí la vulnerabilidad que presentan las APIS en dicho servidor al extraer e ingresar datos, su relación con la base de datos, en la red se identificarán las vulnerabilidades que presenten los datos al ser transmitidos de la aplicación hacia el servidor, esto permitirá enfocar de mejor manera el trabajo de análisis de los riesgos involucrados como fuga o corrupción de los datos.

Al evaluar el riesgo se mide el impacto de dicha vulnerabilidad sobre el activo e información, de esta forma en (Las Claves del Éxito para la Gestión de Riesgo, s.f., p: 1-8) se considera que el cálculo del riesgo se obtiene de la relación de dos variables, la probabilidad de que la vulnerabilidad se materialice por el impacto que origina esta materialización.

Estos valores numéricos son ideales para realizar una escala de riesgos por ejemplo alto, medio, bajo de los mismos que se verificará las acciones a tomar es aquí donde se considera el riesgo aceptable para la organización, por debajo de este indicador no serán considerados y por encima supondrán un peligro latente y deberán ser tratados.

Al tratar el riesgo se proponen estrategias de evasión y minimización para la Comunidad de Madrid (s.f. p: 1-8) las estrategias de evasión impiden que el riesgo ocurra y se cuenta con 4 técnicas: transferencia, reducción, elusión y diversificación; en cuanto a minimización existe la realización de un plan de contingencia ya cuando se materializa el riesgo. Estas técnicas para tratar el riesgo nos indicarán que hacer cuando ya se produce el daño por ejemplo cuando el riesgo no puede ser manejado por el ente que lo identifica se puede transferir a otra empresa o una unidad superior, si el riesgo puede ser manejado se realiza técnicas de reducción del impacto generado, la elusión es no hacer nada cuando el riesgo se produce y diversificar significa distribuir el riesgo en el mayor número de partes posibles con la finalidad de disminuir su impacto y poder tratarlo de manera más eficiente.

Cada riesgo que se produce no es un hecho aislado sino que puede ser producto de una fuente conocida o desconocida, considerando que a más de producir daño en nuestra organización puede ser la puerta abierta para la extracción de información de un intruso mediante un ataque informático.

## Ataques

Un riesgo en sí ya representa un problema para cualquier sistema de información o una organización como tal, pero a su vez estas brechas de seguridad son tomadas como fuentes para que delincuentes informáticos generen sus ataques, con la finalidad de obtener un objetivo valioso en cualquier infiltración, en el mundo informático este objetivo valioso es la información, datos, indicios los mismos que al final del proceso los llevarán a un solo camino el dinero.

Un ataque informático según Jorge Mieres (2009, p: 1-17) consiste en:

*“… Aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización…”.*

La falla más crítica en todo sistema informático en sí son los usuarios, por un simple motivo, la cultura informática que poseamos, no importa cuán robusta sea nuestra aplicación ni lo bien que responda ante cambios, vulnerabilidades o ataques, mucho peor cuantas normativas, estándares existan si el usuario no hace ningún énfasis en ponerlas en práctica, hoy en día los usuarios somos cómodos y buscamos la simplicidad ante lo complejo, lo gratis ante lo pagado (de forma ilícita).

Para la unidad informática Secretaría de Comunicación Social de la Presidencia del Gobierno de Guatemala. (2015, p: 1-29) un ataque informático es: “… un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera)…”

En base a esta definición tomamos en consideración que la seguridad informática no solo depende de nosotros o de la aplicación que generemos como solución, incluso se aísla más allá de nuestras fronteras por lo que es un efecto dominó, muchas veces nuestro software depende de otro y así sucesivamente por ejemplo la aplicación móvil depende del sistema operativo huésped, con lo qué, si este sistema operativo posee vulnerabilidades quizás y de forma casi segura podrán llegar a vulnerar la información que se maneje en el aplicativo por lo que no solo es importante emitir criterios de seguridad caso contrario lo que se debería realizar es un cambio de cultura de seguridad informática de nuestros usuarios y es por esto que el presente estudio no se enfoca solo a ver las vulnerabilidades netas de una aplicación móvil sino que desde su construcción es diseñada de forma genérica con lo que nos lleva a realizar un análisis también de su medio ambiente (definiendo como medio ambiente al sistema operativo, red de transmisión de datos, servidor) .

Según Jorge Mieres (2009, p: 1-17) un ataque informático se constituye de 5 pasos que son: reconocimiento, exploración, obtener acceso, mantener acceso y borrar huellas, esta metodología se la considerará como genérica para analizar un posible ataque o buscar una respuesta a cada nivel al se enfrente nuestro software en el caso preciso del reconocimiento y la exploración la principal medida a tomar sería la teoría de confusión y difusión de Shannon (principios de criptografía) en donde mostraríamos la información de forma oculta y dispersa, al intruso intentar obtener acceso a la aplicación la solución sería la verificación y autenticación del usuario mediante quizás dos métodos usando algún tipo de cifrado asimétrico en lo ideal.

Para el principio de mantener el acceso nuestra aplicación debería responder de forma inmediata, es decir verificar por ejemplo los planes de auditoría que manejen en la organización si existiere algún tipo de acceso no autorizado lo ideal sería finalizar dicha conexión, los logs (bitácoras) son el registro de los servidores para manejar las actividades que se han realizado tanto en el servidor como el rastro en los dispositivos de red por lo que el objetivo para eliminar las huellas del atacante serían estos registros.

El registro de logs sería incluso uno de los principales indicios para verificar la fuente de ataque y su tipo, según Cequeda Jean (2012) existen ataques activos (generación, interrupción, modificación) y pasivos (intercepción), los ataques activos estarían involucrados a los 5 pasos de un ataque debido a que el intruso se encuentra constantemente explorando vulnerabilidades a ser usadas en ese instante o de forma posterior, en este ámbito se ha generado por ejemplo el ataque del día cero. Los ataques pasivos en cambio son los más difíciles de detectar por ejemplo si se produce un ataque de hombre en el medio en el mismo que solo se busca interceptar los datos que viajan a través de la red.

Estos ataques pueden ser originados por diversos tipos de intrusos, Aguilera Purificación (2010, p: 14) enuncia a los principales intrusos como: Hackers, Crackers, Lamers, CopyHacker, Bucanero, Phreakers, Newbie, Piratas Informáticos, Script Kiddie, entre otros, como desarrolladores de software se deberían generar políticas de seguridad informática para evitar la ocurrencia de diversos inconvenientes.

## Tipos de Ataques

Dentro de los principales tipos de ataques se encuentran dirigidos a las aplicaciones o sistemas web así como a los diversos sistemas operativos existentes en el mercado pero principalmente se encuentran dirigidos con principios de ingeniería social es decir que se manipula a los usuarios de tal forma que suministran su información a los atacantes de manera voluntaria, por lo que al revisar la literatura existente para los tipos de ataques a los dispositivos móviles se encuentran como principal amenaza los virus y software malicioso como lo enuncia ESET en su Guía de Seguridad para usuarios de Smartphones, Panda Security en su Informe Especial de Predicciones 2015.

De todos los estudios el más completo es de NowSecure (NowSecure, Secure Mobile Development, 2015) donde los principales tipos de ataques móviles son:

### Basados en el Navegador

Phishing.- Esta es una técnica mediante la cual se substrae información personal del usuario como por ejemplo claves y nombres de usuario, se ha identificado que los usuarios móviles tienen tres veces más posibilidades de incurrir en este tipo de ataque puesto que la navegación en un navegador móvil es muy limitada y la visualización de su contenido muy escaso.

Framing.- El Framing o enmarcado permite realizar una interpretación particularizada de la realidad es por lo que se lo usa como un envoltorio a una página o aplicación web por ejemplo que simule ser la original para ser fuente de otro tipo de ataques como Clickjacking.

Clickjacking.- Este tipo de ataque es basado en la interfaz de la aplicación y se centra en usar el evento clic que realiza el usuario en la interfaz, con la finalidad de tomar posesión de la aplicación mediante la ejecución de código malicioso embebido.

Drive-by Downloading.- Consiste en forzar al usuario a descargarse una aplicación maliciosa al visitar cierto enlace de fuente desconocida con lo que el usuario recibe una notificación para instalar la aplicación maliciosa, esto puede ser explotado por ejemplo por ataques previos como Phishing o Framing engañando al usuario y dándole una sensación de seguridad, este problema se evidencia principalmente en Android.

Man-in-the-Mobile[[1]](#footnote-1).- Hombre en el móvil inicia con una ataque llamado hombre en el navegador donde los usuarios son engañados en un sitio web de escritorio y forzados a descargar una aplicación móvil que es en realidad un malware como Tatanga[[2]](#footnote-2) o Zeus[[3]](#footnote-3) por ejemplo, el modo de operación es usar los códigos de seguridad enviados a los dispositivos móviles como los sistemas de seguridad bancarios y robar su identidad, al tener el malware instalado en el dispositivo el atacante se roba el tráfico de red de su móvil haciendo transacciones no autorizadas.

### Ataques por Teléfono o Mensajes de Texto

Baseband attacks.- Son ataques que emplean las redes de banda base de celular como por ejemplo GSM, comunicaciones que se dan mediante el hardware de las torres repetidoras.

SMiShing.- Ataque mediante mensajes de texto en los cuales se envía al usuario direcciones web de sitios falsificados con la finalidad de obtener información sensible como por ejemplo las credenciales de un usuario.

RF Attacks – Bluejacking.- Ataques de comunicación corta llamados ataques de relay, actúan sobre canales de comunicación NFC o RF para interceptar los datos transmitidos a través de estas redes de corto alcance para tomar posesión de ficheros de claves o información en el dispositivo móvil incluso accionar el bluetooth para tal efecto, se ha popularizado debido a que estos canales se usan como medio para realizar pagos.

### Ataques basados en Aplicación

Almacenamiento de Datos Sensibles.- Según Viaforensics el 83% de las aplicaciones móviles almacenan sus datos de forma insegura como por ejemplo en las tarjetas de memoria externa del dispositivo.

Encriptación pobre o nula.- las aplicaciones móviles transmiten sus mensajes de forma abierta sin protección es decir no emplean un cifrado al enviar datos a través de los canales de comunicación, esto permite a los atacantes verificar el tráfico en la red de comunicación por ejemplo Wi Fi para obtener información.

Validación impropia de SSL.- Problemas existentes en la validación del certificado del protocolo, muchos malware hacen uso de estas brechas de seguridad para obtener información.

Inyección Dinámica en Tiempo de Ejecución.- Son procedimientos que emplean los atacantes para aprovechar las vulnerabilidades de las aplicaciones en tiempos de ejecución, también pueden acceder a los datos que se encontraren almacenados en la memoria del dispositivo.

Permisos Inintencionados, Permisos Escalados y Manipulación de la Configuración.- Son problemas en las validaciones y autenticaciones de los usuarios así como en la configuración del dispositivo por lo que los atacantes pueden acceder a permisos que no han sido asignados al usuarios mediante estos fallos, inclusive a los datos almacenados en archivos de configuración externos.

### Ataques Basados en el Sistema Operativo

No passcode.- Los usuarios incurren mucho en este tipo de ataque o vulnerabilidad se genera principalmente cuando existen aplicaciones que requieren contraseña, al momento de crearla usan combinaciones de datos muy simples o patrones de bloqueo que pueden ser fácilmente precedidos por algún malware.

iOS jailbreaking y Android rooting.- los usuarios de estos sistemas operativos los dos más populares mediante estas técnicas alteran o suprimen las restricciones y seguridades del fabricante lo mismo que ocasiona que las aplicaciones que requieran permisos especiales se ejecuten sin control alguno creando así un fallo de seguridad, al emplear estos métodos también se expone datos sensibles sobre la configuración del dispositivo.

Passwords and data accesible.- Son debilidades existentes en las diversas aplicaciones que se manejan de manera integrada en la nube como por ejemplo el llavero de iOS, estas aplicaciones poseen falencias en sus mecanismos criptográficos y una persona con conocimiento de las mismas puede fácilmente vulnerarlas.

Ataques del Día Cero.- Son ataques planificados, por lo general se encuentran vulnerabilidades en los sistemas operativos, aplicaciones o dispositivos que son ya conocidas por una persona o un grupo y son explotadas en un día específico maximizando así las probabilidades de éxito involucrando a la mayor cantidad de objetivos posibles.

### Ataques Basados en la Red

Wi-Fi.- Cuando los usuarios emplean sus dispositivos móviles en redes inseguras corren el riesgo de sufrir un ataque por lo que se hace necesario usar un protocolo seguro como SSL para prevenir estos ataques, por lo general en redes inseguras se dan ataques de hombre en el medio.

Rogue access points.- Consiste en instalar puntos de acceso no autorizados, o alterados en una red física al mismo tiempo permitir conexiones seguras a los usuarios, con esto se puede fácilmente implementar ataques como Phishing.

Packet sniffing y Man-in-the-Middle.- Son métodos interrelacionados que consisten en la intercepción de paquetes de datos que contienen información valiosa del usuario como contraseñas o tokens de seguridad con los que se extrae información y facilita el espionaje como por ejemplo Session hijacking y SLStrip que es una variante de ataque hombre en el medio que aprovecha vulnerabilidades en el protocolo

DNS poisoning.- El envenenamiento de DNS es empleado como una fuente primaria de un ataque ya que permite direccionar a los usuarios a sitios vulnerados, así también inyectar código malicioso o Falsos Certificados de SSL que confunden a los usuarios y les brindan una falsa sensación de seguridad.

### Ataques Basados en el Servidor

Los ataques basados en el servidor incluyen las vulnerabilidades de la plataforma de desarrollo de software, problemas de mala configuración o falta de la misma, ataques basados en petición y ejecución de archivos externos como por ejemplo XSS o CSRF en donde el atacante filtra un script malicioso a nuestro servidor y lo procesa, otras de las falencias en muchos servidores y dispositivos son los problemas de inicio de sesión por fuerza bruta donde se generan un número considerable de intentos con distintos datos generados por un algoritmo para obtener el acceso a la aplicación o el servidor y por último la escasa validación de los datos de entrada que procesas las aplicaciones donde el usuario sin intención alguna puede provocar un fallo al ingresar datos erróneo.

### Ataques a la Base de Datos

Dentro de los principales ataques de bases de datos se encuentran: la inyección de código SQL, la ejecución de comandos del sistema operativo del servidor que por lo general se lo realiza al vulnerar conexiones en los archivos de la aplicación o mediante conexiones externas y finalmente se encuentran los privilegios escalados.

Con todo este contenido se ha identificado que en la FADE existe un problema de disponibilidad de información según criterios de accesibilidad W3C de momento, lugar y dispositivo, por lo que, se propone la realización de una aplicación móvil, de igual forma se conoce que para el desarrollo de aplicaciones móviles seguras, no rige un estándar predefinido hasta el momento por lo que se propone un modelo de buenas prácticas de seguridad para el desarrollo de este tipos de aplicaciones basados en los estudios de vulnerabilidades, amenazas

# MARCO METODOLÓGICO

Se han definido los conceptos y técnicas que permiten asegurar una aplicación móvil, a continuación se definirá el diseño de la investigación, con la finalidad de dar a conocer la relación existente entre la disponibilidad de información y la seguridad de la aplicación, se delimitará también la población a la que será dirigida la aplicación móvil, la operacionalización de las variables planteadas y las técnicas e instrumentos que facilitarán la recolección de los datos para su posterior análisis, donde se obtendrán los resultados generales de la investigación.

Se empleará un diseño cuasi experimental más una revisión bibliográfica, la aplicación móvil será empleada por el equipo de auditores del Centro CIMOGSYS, así también el Decano, Vicedecano y Directores de Escuela de la Facultad de Administración de Empresas; además se estudiarán las tendencias de desarrollo de aplicaciones informáticas en las distintas facultades de la ESPOCH, DETIC (Departamento de Tecnologías de la Información y Comunicación) e IPEC (Instituto de Posgrado y Educación Continua) para conocer los niveles de seguridad empleados.

Para recopilar la información sobre disponibilidad de información, se toma como población a los auditores de la Facultad de Administración de Empresas, equipo de 5 personas; la seguridad de la aplicación se analizará mediante encuesta a los técnicos responsables del desarrollo, mantenimiento de sistemas informáticos, laboratorios o centros de cómputo en las 7 facultades de la ESPOCH, 7 personas, un miembro del DETIC, un encargado del IPEC dando un total de 9 personas por lo que no amerita realizar un cálculo de la muestra a aplicar y se toma a la población completa.

La investigación se utilizará el método científico diseñado de la siguiente manera:

* La investigación se produce por la necesidad de incrementar la disponibilidad de la información del Sistema de Gestión de Calidad a través de la seguridad de la aplicación móvil en la Facultad de Administración de la ESPOCH.
* Se han definido los objetivos de la investigación con la finalidad de emitir una propuesta de mejores prácticas de seguridad que permita incrementar la disponibilidad de la información.
* En el marco teórico se muestran las razones por las cuales es importante realizar un estudio de seguridades en aplicaciones móviles.
* La hipótesis ha sido planteada como solución al problema de accesibilidad de la información.
* Una vez planteada la hipótesis se realiza la operacionalización de las variables.
* Se define la población a la cual se dirigirá el estudio.
* Se realiza la recolección de datos e indicadores mediante encuestas.
* Se realiza la comprobación de la hipótesis planteada.
* Se propone prácticas de seguridad para el desarrollo de aplicaciones móviles.
* Se emiten conclusiones y recomendaciones.

Este modelo de investigación es un modelo genérico que ha sido aceptado y difundido por la comunidad de científicos a nivel mundial por lo que ha sido diseñado para el presente trabajo de titulación y será aplicada a nivel de Facultad FADE y ESPOCH.

Para la recopilación de la información se empleará como técnica la encuesta, se realizarán preguntas a los técnicos informáticos de facultad y auditores, para analizar los resultados del estudio se procede a plantear la siguiente hipótesis y su respectiva hipótesis nula, así como las variables que interactúan en entre sí:

H0: “Las buenas prácticas de seguridad incrementan la disponibilidad de información del Sistema de Gestión de Calidad”.

H1: “Las buenas prácticas de seguridad no incrementan la disponibilidad de información del Sistema de Gestión de Calidad”.

**Variable Independiente:** Las buenas prácticas de seguridad.

**Variable Dependiente:** La disponibilidad de la información.

Se identifica una relación de dependencia entre variables, donde se determinará cuanta incidencia tiene la seguridad de una aplicación con la disponibilidad de información, para analizar las variables que intervienen en la hipótesis del trabajo de titulación, se procederá a la generalización de conceptos para comprender que implica una buena práctica de seguridad y que es disponibilidad de información.

Tabla 2‑1 Operacionalización Conceptual de las Variables

|  |  |  |
| --- | --- | --- |
| VARIABLE | TIPO | CONCEPTO |
| Buenas Prácticas de Seguridad | Independiente | Buena Práctica de Seguridad es un método empleado que permite asegurar el contenido de una aplicación tanto en su capa de presentación, transporte, reglas del negocio y base de datos. |
| Disponibilidad de Información | Dependiente | La disponibilidad es la característica de la información de encontrarse a disposición del usuario en cualquier momento, lugar y dispositivo. |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

## Operacionalización Metodológica Variable Independiente

Tabla 2‑2 Operación Metodológica Buenas Prácticas de Seguridad

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VARIABLE** | **CONCEPTO** | **DIMENSIÓN** | **INDICADOR** | **ÍNDICE** | **TÉCNICA** | **INSTRUMENTO** |
| Buenas Prácticas de Seguridad | Buena Práctica de Seguridad es un método empleado que permite asegurar el contenido de una aplicación tanto en su capa de presentación, transporte, reglas del negocio, base de datos y servidor. | Capa de Base de Datos | Inyección SQL | Número de ataques de Inyección SQL | Encuesta | Cuestionario  Áreas de Desarrollo de Software / Sistemas de cada Facultad |
| Privilegios | Privilegios asignados a usuarios de base de datos |
| Ejecución de Comandos del SO | Número de ataques de ejecución de comandos de sistema operativo |
| Capa de Reglas del Negocio | Ataques de Fuerza Bruta | Número de ataques de Fuerza Bruta |
| Ataques XSS | Número de ataques XSS |
| Ataques CSRF | Número de ataques CSRF |
| Ataques DOS | Número de ataques DoS |
| Validaciones | Número de problemas de Formularios validados |
| Capa Física de Transporte | Encriptación de datos. | Se cifran los datos antes de ser transmitidos por la red |
| Certificado SSL | Las aplicaciones emplean el protocolo seguro SSL |
| SLStrip | Vulnerabilidades en las firmas SSL |
| Packet Sniffing | Número de ataques de espionaje de paquetes |
| DNS Poisoning | Número de ataques de envenenamiento detectados |
| Session Hijacking | Número de ataques de secuestro de sesión |
| Hombre en el medio. | Número de ataques de hombre en el medio |
| Capa de Presentación | Permisos Inintencionados | Políticas de privilegios para los usuarios de la aplicación |
| Privilegios Escalados. | Número de operaciones no asignadas identificadas |
| Man in the Mobile | Número de ataques identificados |
| Clickjacking | Número de scripts maliciosos detectados |
| Phishing | Número de casos de suplantación de identidad |
| Tipos de aplicaciones. | Qué tipo de aplicaciones se ha desarrollado en su facultad |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

## Operacionalización Metodológica Variable Dependiente

Tabla 2‑3 Operacionalización Metodológica Disponibilidad de Información

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VARIABLE** | **CONCEPTO** | **DIMENSIÓN** | **INDICADOR** | **ÍNDICE** | **TÉCNICA** | **INSTRUMENTO** |
| Disponibilidad de Información. | La disponibilidad es la característica de la información de encontrarse a disposición del usuario en cualquier momento, lugar y dispositivo. | Accesibilidad | Momento | Horario de Oficina | Encuesta | Cuestionario a  Usuarios del Sistema SGC |
| Lugar | ESPOCH |
| Nacional |
| Internacional |
| Dispositivo | Web |
| Móvil |
| Televisión |
| Automóviles |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

# ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Al haber analizado la hipótesis planteada en la investigación se ha identificado que intervienen dos variables, las Buenas Prácticas de Seguridad que en la Tabla 2-2 posee cuatro dimensiones, serán analizadas en las facultades de la ESPOCH así también en el Instituto de Posgrado y Educación y el Departamento de Tecnologías de la Información y Comunicación, la Disponibilidad de Información que en la Tabla 2-3 que posee una sola dimensión, será analizada en el Centro CIMOGSYS, las variables se medirán mediante dos encuestas respectivamente.

## Buenas Prácticas de Seguridad

Para analizar las Buenas Prácticas de Seguridad se ha realizado una encuesta mediante un cuestionario que ha permitido extraer la información necesaria para interpretar como se afronta en las diferentes facultades, el IPEC y el DETIC los principales ataques analizados en el capítulo teórico, se han realizado preguntas a cada unidad para establecer patrones de comportamiento con lo que se ha preguntado si el técnico responsable conoce sobre el tipo de ataque, si se previene el ataque, si existe una metodología para prevenir los ataques y finalmente cuántos ataques de esa variedad ha sufrido la unidad.

### Dimensión Capa de Base de Datos

#### Indicador Inyección SQL

Para analizar el indicador de Inyección SQL se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre este tipo de ataques, verificar si se previenen o no los ataques y si se emplea una metodología específica, finalmente se preguntó sobre la cantidad de ataques identificados para evaluar los mecanismos de protección, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted qué es un ataque de Inyección SQL?
* ¿Se previene en su facultad este tipo de ataques en los sistemas informáticos?
* ¿Emplea en su facultad una metodología para prevenir este tipo de ataques?
* ¿Indique cuántos ataques de inyección SQL se han identificado en su facultad?

De las preguntas realizadas se ha obtenido el siguiente gráfico resumen:

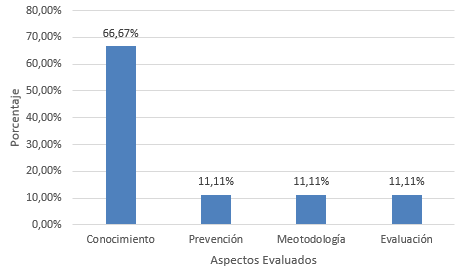


Figura 3‑1 Indicador Inyección SQL

Fuente: Tabulación de encuestas realizadas.

Al analizar las respuestas a las preguntas sobre el indicador en la Figura 3-1 se ha detectado que el 66,67% de las facultades encuestadas conocen el ataque de Inyección SQL lo que permite caracterizar a este tipo de ataques como común o en su defecto posee mucha información, puesto que es conocido por la mayoría de técnicos responsables, pese a ser conocido el 11,11% de las mismas previene el ataque eliminando así una vulnerabilidad de base de datos en los sistemas informáticos, el 11,11% que si previenen el ataque los realizan mediante una metodología que se encuentra especificada en el Manual Técnico de las aplicaciones, por otro punto se ha mencionado que el DETIC provee seguridades contra Inyecciones SQL, con este conocimiento se han identificado 10 ataques de Inyección SQL en la ESPOCH. El no haber detectado esta cantidad incidencias puede interpretarse de dos formas, al no prevenir este tipo de ataques no existe medios de verificar su ocurrencia o no se han realizado procesos de validación de seguridad en las aplicaciones desarrolladas.

#### Indicador Privilegios

Para analizar el indicador de Privilegios se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre los privilegios de los usuarios en una base de datos, verificar si se asignan estos permisos a los usuarios de base de datos, se emplea una metodología específica para asignar permisos y finalmente se preguntó sobre la cantidad de usuarios con permisos distintos a los asignados, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted los privilegios que se asignan a un usuario en una base de datos?
* ¿Se han asignado permisos a los usuarios creados en las bases de datos de su facultad?
* ¿Se emplea una metodología para asignar permisos a los usuarios de base de datos?
* ¿Cuántos casos se han presentado de usuarios con permisos distintos a los asignados?

De las preguntas realizadas se ha obtenido el siguiente gráfico resumen:

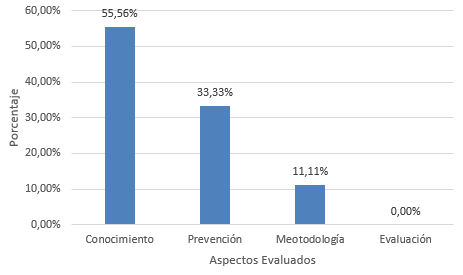


Figura 3‑2 Indicador Privilegios

Fuente: Tabulación de encuestas realizadas.

Al encuestar a los técnicos responsables sobre los permisos que se le pueden asignar a los usuarios de base de datos, como muestra la Figura 3-2, se encontró que el 55,56% conocen sobre los permisos existentes, por lo que se puede identificar que no se emplean base de datos en las facultades restantes o en su defecto el desconocimiento puede darse por que no se conoce el motor de base de datos o se emplea el usuario administrador, por lo que, solo el 33,33% de las facultades asignan permisos a los usuarios de los que el 11,11% emplea una metodología para el efecto, la metodología empleada es una Política de Administración de base de datos, al ser una encuesta genérica no se verifican los permisos específicos de cada motor sino que se busca definir si se asignan o no permisos, esta vulnerabilidad puede traer consecuencias graves para las aplicaciones o sistemas informáticos ya que un atacante puede vulnerar la base de datos en busca de información o borrarla si se usa el usuario administrador, finalmente no se han identificado casos con usuarios de usuarios con permisos distintos a los asignado esto se debe a que no se ha producido ningún ataque o en su defecto no se ha realizado una verificación de esta vulnerabilidad.

#### Indicador Ejecución de Comandos del Sistema Operativo

Para analizar el indicador de Ejecución de Comandos del Sistema Operativo se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre los comandos de base de datos que se pueden ejecutar en un Sistema Operativo, verificar si se previene esta vulnerabilidad, verificar el empleo de una metodología específica y finalmente se preguntó sobre la cantidad de ataques de este tipo han sido identificados, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted qué es un ataque de ejecución de comandos del sistema operativo?
* ¿Se previene en su facultad este tipo de ataques?
* ¿Se emplea una metodología para prevenir la ejecución de comandos del sistema operativo?
* ¿Cuántos ataques a base de ejecución de comandos de sistema operativo se ha identificado?

De las respuestas formuladas se ha obtenido el siguiente gráfico resumen:

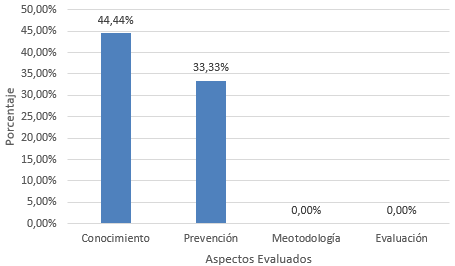


Figura 3‑3 Indicador Ejecución de Comandos de SO

Fuente: Tabulación de encuestas realizadas.

De las encuestas analizadas se ha extraído como muestra la Figura 3-3, que el 44,44% de las facultades conocen en que consiste un ataque de ejecución de comandos del sistema operativo, es decir conocen que a través del sistema operativo huésped del motor se puede administrar una base de datos, el 33,33% previene esta vulnerabilidad dándose así que el porcentaje de prevención es inferior que el de conocimiento, los técnicos conocen el ataque y no saben cómo prevenirlo, el 100% de encuestados no emplea metodología y no se han registrado ataques de este tipo.

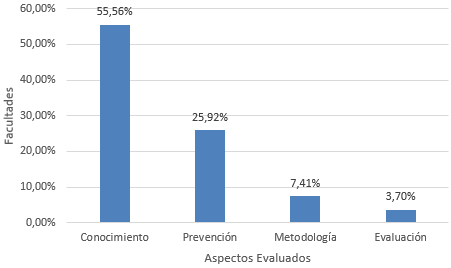


Figura 3‑4 Resumen de la Dimensión Base de Datos

Fuente: Tabulación de encuestas realizadas.

Al analizar los indicadores de la dimensión como muestra la Figura 3-4, de base de datos se puede identificar que la mayoría de los encuestados conoce a que se refiere cada uno de los ataques o vulnerabilidades sin embargo el porcentaje de prevención de los mismos es menor, se identifica además que no existen metodologías para realizar la prevención de ataques y si existe en una metodología única por lo que se concluye que no existe una metodología estándar de seguridad de base de datos así también no se realizan auditorías a las bases de datos existentes en busca de problemas de seguridad, el no registro de ataques se debe a la no existencia de los mismos o falta de interés en verificar si los sistemas han sido o no atacados, probablemente se hayan verificado los ataques y no se tenga registro de los mismos.

### Dimensión Capa de Reglas del Negocio

#### Indicador Ataques de Fuerza Bruta

Para analizar el indicador de Ataques de Fuerza Bruta se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre este tipo de ataques, verificar si se previenen o no y si se emplea una metodología específica, finalmente se preguntó sobre la cantidad de ataques identificados para evaluar los mecanismos de protección, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted qué es un ataque de fuerza bruta?
* ¿Se previene en su facultad los ataques de fuerza bruta?
* ¿Existe alguna metodología para prevenir ataques de fuerza bruta?
* ¿Cuántos ataques de fuerza bruta se han identificado en la facultad?

De los resultados de las preguntas formuladas se ha obtenido el siguiente gráfico resumen:

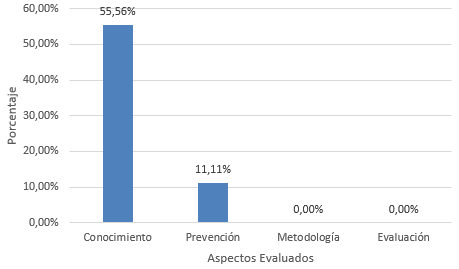


Figura 3‑5 Indicador Ataques de Fuerza Bruta

Fuente: Tabulación de encuestas realizadas.

De los datos analizados en las encuestas como se muestra en la Figura 3-5, se ha podido verificar que el 55,56% de encuestados conoce en que consiste un ataque de fuerza bruta, sin embargo solo el 11,11% previene este tipo de ataques, no existe una metodología para prevenirlos y no se han registrado incidencias de ataques por lo que se puede concluir que no se realizan esfuerzos por asegurar los sistemas informáticos o aplicaciones en la ESPOCH, el personal técnico no realiza verificaciones en busca de fallos de seguridad y no existen registros de haber detectado este tipo de incidencias.

#### Indicador Ataques XSS

Para analizar el indicador de Ataques XSS se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre este tipo de ataques, verificar si se previenen o no y si se emplea una metodología específica, finalmente se preguntó sobre la cantidad de ataques identificados para evaluar los mecanismos de protección, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted qué es un ataque XSS (Cross-Site Scripting)?
* ¿Se previene en su facultad los ataques XSS?
* ¿Existe alguna metodología para prevenir ataques XSS?
* ¿Cuántos ataques XSS se han identificado en la facultad?

De las preguntas realizadas se ha obtenido el siguiente gráfico resumen:

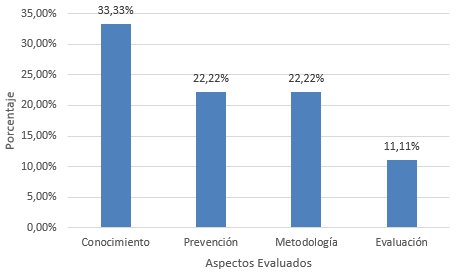


Figura 3‑6 Indicador Ataques XSS

Fuente: Tabulación de encuestas realizadas.

De las facultades encuestadas, como se visualiza en la Figura 3-6, el 33,33% conoce que es un ataque Cross-site Scripting, el 77,78% no previene este tipo de ataques, del 22,22% que si previenen el ataque emplean metodologías registradas una en el manual técnico y otra menciona que se realiza a través del DETIC, el no prevenir este tipo de ataques en las facultades se debe al desconocimiento sin embargo el índice de desconocimiento es inferior al de prevención, finalmente se han registrado en la IPEC 10 incidencias frente a 0 incidencias de las demás unidades, que pueden haber sufrido ataques pero no existen registros.

#### Indicador Ataques DoS

Para analizar el indicador de Ataques DoS se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre este tipo de ataques, verificar si se previenen o no y si se emplea una metodología específica, finalmente se preguntó sobre la cantidad de ataques identificados para evaluar los mecanismos de protección, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted qué es un ataque DoS (Denial of Service)?
* ¿Se previene en su facultad los ataques DoS?
* ¿Existe alguna metodología para prevenir ataques DoS?
* ¿Cuántos ataques DoS se han identificado en la facultad?

De las preguntas realizadas se ha obtenido el siguiente gráfico resumen:

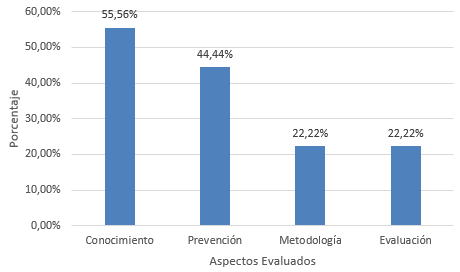


Figura 3‑7 Indicador Ataques DoS

Fuente: Tabulación de encuestas realizadas.

Al analizar las encuestas realizadas a las facultades, como se muestra en la Figura 3-7, se ha determinado que el 55,56% conoce que es un ataque de Negación de Servicios, del porcentaje que conoce el ataque el 44,44% lo previene y solo el 22,22% emplea una metodología que es detallada como políticas de DETIC y un firewall en sistema operativo Linux sin embargo se puede distinguir rápidamente que no son parte de un estándar global, se han identificado 11 ataques de negación de servicios de los cuales 10 se han registrado en el IPEC y 1 en la Facultad de Ciencias, se puede apreciar de esta manera que los sistemas de la ESPOCH se encuentran vulnerables a ataques de negación de servicios.

#### Indicador Validación de Formularios

Para analizar el indicador de Validación de Formulario se ha contemplado como índice la cantidad de problemas en la validación de datos que se ingresan en los sistemas informáticos en cada facultad planteado en las siguientes preguntas:

* ¿Conoce Usted en qué consiste la Validación de Formularios en los sistemas informáticos?
* ¿Se verifican en su facultad los formularios de ingreso de datos en los sistemas informáticos?
* ¿Existe en su facultad alguna metodología para validar formularios?
* ¿Cuántos problemas en la validación de formularios se han presentado?

De las preguntas realizadas se ha podido obtener el siguiente gráfico resumen:

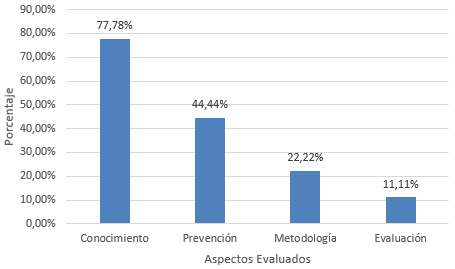


Figura 3‑8 Indicador Validación de Formularios

Fuente: Tabulación de encuestas realizadas.

De las encuestas realizadas a las facultades se ha determinado, como muestra la Figura 3-8, que el 77,78% de los técnicos de facultad conocen en que consiste la validación de datos sin embargo tan solo el 44,44% valida los datos ingresados en los sistemas informáticos, este índice puede ser provocado por el desconocimiento de procesos de validación, no existencia de software desarrollado, el 22,22% de técnicos emplea metodologías para realizar la validación de datos que están registradas en el manual técnico y en procesos de auditoría informática, se han detectado dos problemas de validación de datos en el IPEC, este índice puede ser afectado por sistemas que sean netamente informativos.

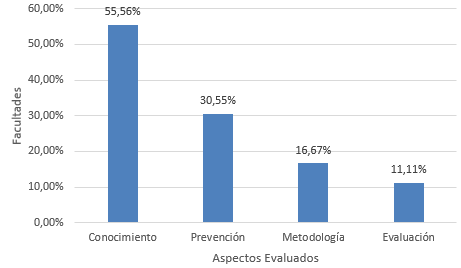


Figura 3‑9 Resumen Dimensión de Reglas de Negocio

Fuente: Tabulación de encuestas realizadas.

En la Dimensión de Capa de Reglas del Negocio, como se muestra en la Figura 3-9, se ha identificado que el conocimiento de las vulnerabilidades supera el 50% en cada uno de los ataques estudiados sin embargo se verifica nuevamente el patrón de prevención de los mismo siendo significativamente menor, se emplean metodologías para sustentar la prevención de ataques siendo las mismas en cada caso distintas, el número de detecciones de incidencias se mantiene bajo, las causas de la baja prevención de ataques puede ser identificada como desconocimiento de técnicas o estándares nacionales o internacionales incluyen también que no se desarrolle software y sea centralizado en el software ESPOCH.

### Dimensión Capa Física de Transporte

#### Indicador Encriptación de datos

Para analizar el indicador de Encriptación de Datos se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre el cifrado de datos, verificar si se envían los datos de forma segura, si se emplea una metodología y un algoritmo de cifrado, finalmente se preguntó sobre la cantidad de problemas en la encriptación de datos, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted en qué consiste la encriptación de datos?
* ¿Se encriptan los datos en los sistemas informáticos de facultad antes de ser transmitidos?
* ¿Existe alguna metodología para realizar la encriptación de datos en la facultad?
* ¿Cuántos problemas en la encriptación de datos se han identificado

De las preguntas realizadas se ha obtenido el siguiente gráfico resumen:

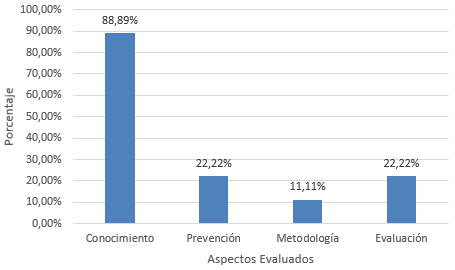


Figura 3‑10 Indicador de Encriptación de datos

Fuente: Tabulación de encuestas realizadas.

Al analizar las respuestas de las encuestas, según la Figura 3-10, El 88,89% de técnicos encuestados ha manifestado conocer en que consiste la encriptación de datos donde el 22,22% ha respondido que los datos de los sistemas informáticos de su facultad se cifran antes de ser enviados en la red y solo el 11,11% emplea una metodología para cifrar datos mediante el algoritmo md5 registrado en el manual técnico, en la Facultad de Informática y Electrónica se ha detectado 2 problemas de encriptación de datos mientras que en DETIC se ha registrado una, pese a que la mayoría de técnicos conoce la vulnerabilidad no se previene este tipo de ataques.

#### Indicador Certificado SSL

Para analizar el indicador de Certificado SSL se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos de unidad sobre el protocolo, verificar si las aplicaciones emplean el protocolo seguro, si son certificados propios o los provee una empresa y finalmente si se han detectado problemas en su uso, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted qué es un Certificado SSL (Secure Sockets Layer)?
* ¿Se emplean certificados SSL en los sistemas informáticos de la facultad?
* ¿Existe alguna empresa que provee certificados SSL a los sistemas informáticos de la facultad?
* ¿Se han detectado problemas en el uso de los certificados SSL?

De las encuestas realizadas se ha obtenido el siguiente gráfico resumen:

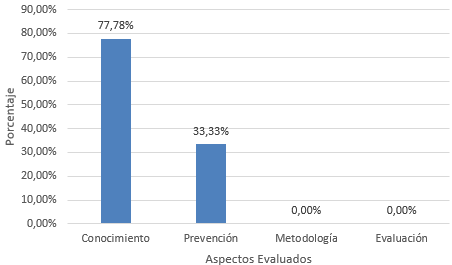


Figura 3‑11 Indicador Certificados SSL

Fuente: Tabulación de encuestas realizadas.

Al analizar los resultados, según la Figura 3-11, de las encuestas el 77,78% de los técnicos de facultad conocen que es un certificado SSL, en 33,33% de las facultades emplean certificados SSL autogenerados ya que no existe ninguna empresa que provea esta seguridad a la ESPOCH lo que significa que puede existir vulnerabilidades en los certificados empleados en los sistemas informáticos.

#### Indicador SLStrip

Para analizar el indicador de SLStrip que explota vulnerabilidades en las firmas SSL/TLS se ha formulado en la encuesta 2 preguntas con la finalidad de identificar las inconsistencias en las firmas del protocolo SSL, las preguntas formuladas fueron las siguientes:

* ¿Se han detectado problemas en el uso de los certificados SSL?
* ¿Se han detectado falsificación del certificado SSL?

De las cuales se han detectado problemas en los certificados según el siguiente gráfico:

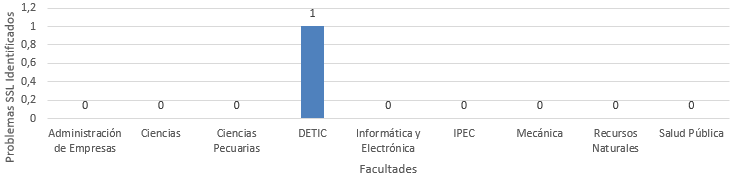


Figura 3‑12 Cantidad de Problemas SSL Identificados

Fuente: Tabulación de encuestas realizadas.

La única unidad como muestra la Figura 3-12, que ha registrado problemas en el uso de certificados SSL el DETIC ya que las demás facultades han manifestado que no se ha detectado falsificación de los certificados, al no registrar problemas las facultades pueden no poseer registros de inconvenientes, pueden no usar certificados o en su defecto los técnicos no tienen conocimiento de estas incidencias.

#### Indicador Packet Sniffing

Para analizar el indicador de Secuestro de Paquetes se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos sobre el rastreo de paquetes en la red de transmisión de datos, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted en que consiste el espionaje de paquetes?
* ¿Se previene en su facultad este tipo de ataques?
* ¿Existe alguna metodología para prevenir el espionaje de paquetes en la facultad?
* ¿Cuántos ataques de espionaje de paquetes se ha detectado?

De las encuestas se han obtenido los siguientes resultados:

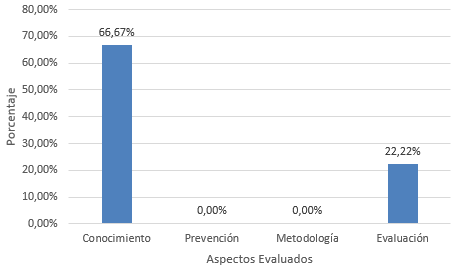


Figura 3‑13 Indicador Espionajes de Paquetes Identificados

Fuente: Tabulación de encuestas realizadas.

De los técnicos encuestados, como muestra la Figura 3-13, el 66,67% conoce en que consiste el espionaje de paquetes ninguna facultad previene este tipo de ataques, esto puede darse debido a que desconocen mecanismos de protección ante esta vulnerabilidad, de igual forma no se ha identificado ninguna metodología de prevención sin embargo se han detectado 3 casos de espionaje de paquetes 2 en la IPEC y uno en DETIC, datos que evidencian un registro de ataques en estas unidades.

#### Indicador DNS Poisoning

Para analizar el indicador de Envenenamiento DNS se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos sobre el ataque de envenenamiento, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted en que consiste el envenenamiento de DNS?
* ¿Se previene en su facultad el envenenamiento de DNS?
* ¿Existe alguna metodología para prevenir el envenenamiento DNS en la facultad?
* ¿Cuántos ataques de envenenamiento de cache se han identificado?

¿Cuántos ataques de envenenamiento DNS se han identificado?

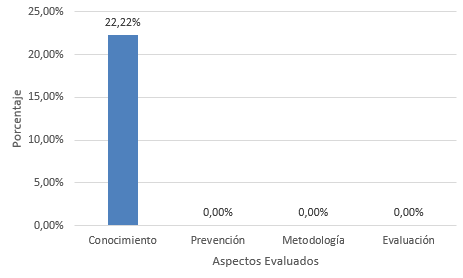


Figura 3‑14 Cantidad de Ataques de Envenenamiento DNS

Fuente: Tabulación de encuestas realizadas.

De las preguntas realizadas, según los resultados de la Figura 3-14, en la encuesta se ha identificado que el 22,22% de los encuestados ha respondido que conoce en que consiste el envenenamiento DNS, el 77,78% no conoce en que consiste el ataque y ha manifestado que no se previene este tipo de ataque en la facultad o unidad encuestada, no existen metodologías de prevención y no se han identificado ataques, dada la falta de conocimiento del ataque es normal que no se identifique el mismo así como la inexistencia de registros ante estas incidencias, este ataque de realiza a nivel de servidor por lo que las aplicaciones o sistemas informáticos están vulnerables adicionalmente a ataques de suplantación de identidad.

#### Indicador Session Hijacking

Para analizar el indicador de Secuestro de Sesiones se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos sobre este tipo de ataques, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted en qué consiste el secuestro de sesiones?
* ¿Se previene en los sistemas informáticos de su facultad el secuestro de sesiones?
* ¿Existe alguna metodología para el manejo de sesiones en los sistemas informáticos en la facultad?
* ¿Cuántos ataques de este secuestro de sesiones se han identificado?

De las encuestas realizadas se ha obtenido el siguiente gráfico resumen:

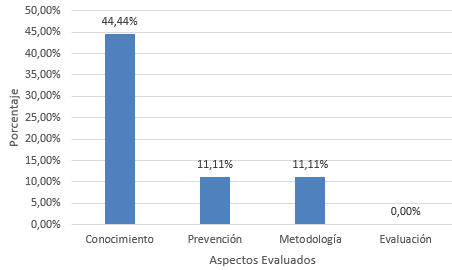


Figura 3‑15 Indicador Secuestro de Sesiones

Fuente: Tabulación de encuestas realizadas.

De los técnicos encuestados, según la Figura 3-15, se ha determinado que el 44,44% conoce en que consiste el secuestro de sesiones pese a esto solo el 11,11% de facultades previene estos ataques y emplean una metodología para el efecto que se encuentra detallada en el manual de técnico de las aplicaciones o sistemas informáticos pero no se han detectado incidencias de secuestro de sesiones en las facultades, esto se debe a que no se han realizado evaluaciones de seguridad a las aplicación, pueden haber existido incidencias pero no poseen registro de las mismas o la metodología no permite la detección de los mismos.

#### Indicador Hombre en el medio

Para analizar el indicador de Hombre en el Medio se ha formulado en la encuesta 4 preguntas con la finalidad de identificar cuanto conocen los técnicos sobre este tipo de ataques en la red de transmisión de datos, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted en qué consiste el ataque de hombre en el medio?
* ¿Se previene en la facultad los ataques de hombre en el medio?
* ¿Existe una metodología en la facultad para prevenir ataques de hombre en el medio?
* ¿Cuántos ataques de hombre en el medio se han identificado?

De las respuestas se ha obtenido el siguiente gráfico resumen:

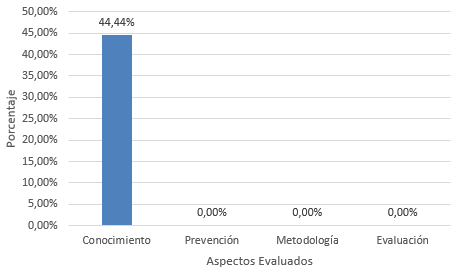


Figura 3‑16 Indicador Hombre en el Medio

Fuente: Tabulación de encuestas realizadas.

Sobre ataques de hombre en el medio, como muestra la Figura 3-16, se identificó que el 44,44% de técnicos de facultades conoce en que consiste este tipo de ataques, sin *embargo* pese a conocer en que consiste el ataque coinciden que no se previene en la facultad el ataque, por ende no se emplean metodologías ni existen incidencias registradas o identificadas, al analizar estos datos verificamos que pese al conocimiento no se realizan procesos de evaluación de los sistemas informáticos a este tipo de ataques y los sistema están vulnerables a intercepción de datos.

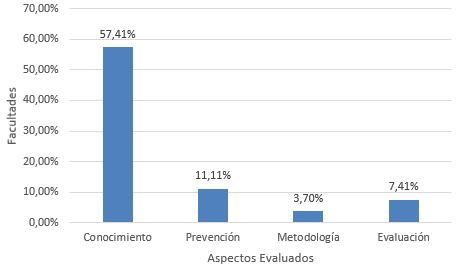


Figura 3‑17 Resumen Dimensión Capa de Transporte

Fuente: Tabulación de encuestas realizadas.

Para la dimensión de Capa Física de Transporte, como se evidencia en la Figura 3-17, se ha identificado que los técnicos de facultad conocen poco sobre ataques de hombre en el medio y secuestro de sesiones por lo que la red de transmisión de datos de la ESPOCH y de las Facultades pueden ser vulnerables a este tipos de ataques ya que también se ha identificado en un bajo porcentaje o nulo que se emplean mecanismos de prevención sin embargo se mantiene el criterio que no se emplean metodologías estandarizadas de prevención sino que se emplean técnicas aisladas de cada aplicación o sistema informático.

### Dimensión Capa de Presentación

#### Indicador Permisos Inintencionados

Para analizar el indicador de permisos inintencionados se ha formulado en la encuesta 4 preguntas con la finalidad de identificar si se asignan permisos a los usuarios, la metodología empleada y la evaluación de permisos, las preguntas formuladas fueron las siguientes:

* ¿Conoce Usted que son los permisos no intencionados?
* ¿Se verifica en los sistemas informáticos los permisos asignados a los usuarios?
* ¿Existe alguna metodología para asignar permisos a los usuarios de los sistemas informáticos?
* ¿Cuántos problemas se han identificado de usuarios con permisos incorrectos?

De las preguntas realizadas se ha obtenido el siguiente gráfico resumen:

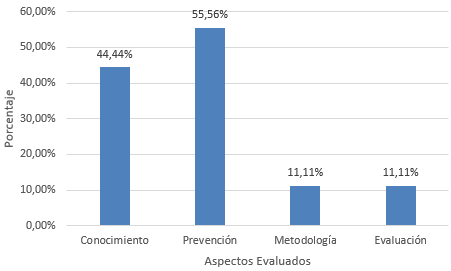


Figura 3‑18 Indicador de Permisos Inintencionados

Fuente: Tabulación de encuestas realizadas.

Para determinar que los permisos asignados a los usuarios sean los correctos se verifican en cada aplicación los mismos puesto que si algún usuario ingresa con permisos distintos existe un problema de permisos no intencionados, para lo cual al encuestar a los técnicos de facultad, como muestra la Figura 3-18, se ha evidenciado que el 44,44% conoce en que consiste este tipo de ataques no obstante el 55,56% valida los permisos a los usuario en las aplicaciones, esto evidencia que intuitivamente los técnicos sin poseer conocimientos del ataque realizan procesos de prevención el 11,11% emplea una metodología de checklist para asignar permisos y se ha detectado solo un caso de usuarios con permisos incorrectos en la Facultad de Ciencias, este hecho evidencia que no existe una metodología genérica para asignar permiso de usuarios de aplicaciones en las facultades o unidades encuestadas así mismo no se ha implementado o registrado incidencias de ataques.

#### Indicador Privilegios Escalados

Para analizar el indicador de permisos escalados se ha formulado en la encuesta 2 preguntas con la finalidad de identificar si se verifican los permisos a los usuarios y si se han detectado problemas en los permisos asignados, las preguntas formuladas fueron las siguientes:

* ¿Se validan los permisos de los usuarios en los sistemas informáticos de la facultad al momento de realizar operaciones?
* ¿Se han identificado operaciones de un usuario que no han sido asignadas?

De las preguntas asignadas se han detectado los siguientes problemas de permisos no asignados:

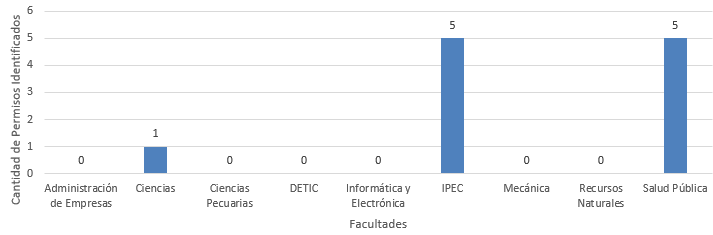


Figura 3‑19 Cantidad de operaciones no asignadas identificadas

Fuente: Tabulación de encuestas realizadas.

El indicador de privilegios asignados permite analizar a más de procesos de inicio de sesión verificar los permisos de usuario en cada operación realizada, como se muestra en la Figura 3-19, se ha identificado que el 55,56% de facultades conoce en que consiste este proceso de validación y en el 33,33% de facultades se han identificados operaciones realizadas de usuarios que no debería realizarlas en la Facultad de Ciencias se ha detectado 1 incidencia, en IPEC y Salud Pública 5 incidencias, lo que evidencia que existen usuarios que con intención o no realizan operaciones que no deberían esto evidencia una vulnerabilidad grave en los sistemas informáticos, si estos permisos escalan a privilegios de administrado cualquier usuario o atacante podría tener control total del sistema.

#### Indicador Man in the Mobile

Para analizar el indicador de Hombre en el Móvil se ha formulado en la encuesta 4 preguntas con la finalidad de identificar si se conoce en las facultades este tipo de ataque, si se previene, la metodología empleada y la evaluación de ataques identificados, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted en qué consiste el ataque de hombre en el móvil?
* ¿Se previene en la facultad los ataques de hombre en el móvil?
* ¿Existe una metodología en la facultad para prevenir ataques de hombre en el móvil?
* ¿Cuántos ataques de hombre en el móvil se han identificado?

De las preguntas analizadas se ha obtenido el siguiente gráfico resumen:

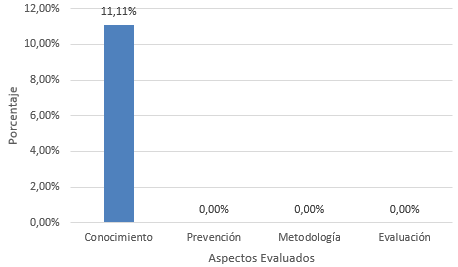


Figura 3‑20 Indicador Hombre en el Móvil

Fuente: Tabulación de encuestas realizadas.

Al total de técnicos de facultades encuestados se ha identificado como muestra la Figura 3-20 el 11,11% conoce en qué consiste este tipo de ataques por lo cual el 100% de facultades no lo previene ni usa alguna metodología específica así como no se han identificado incidencias, se puede evidenciar que no existe mecanismos de protección ante esta vulnerabilidad por desconocimiento y quien conoce la vulnerabilidad no ha encontrado o conoce formas de prevenirla.

#### Indicador Clickjacking

Para analizar el indicador de Secuestro del Clic se ha formulado en la encuesta 4 preguntas con la finalidad de identificar si se conoce en las facultades este tipo de ataque, si se previene, la metodología empleada y la evaluación de ataques identificados, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted en qué consiste el ataque Clickjacking?
* ¿Se previene en la facultad los ataques de Clickjacking?
* ¿Existe una metodología en la facultad para prevenir ataques Clickjacking?
* ¿Cuántos ataques Clickjacking se han identificado?

De las preguntas encuestadas se ha obtenido el siguiente gráfico resumen:

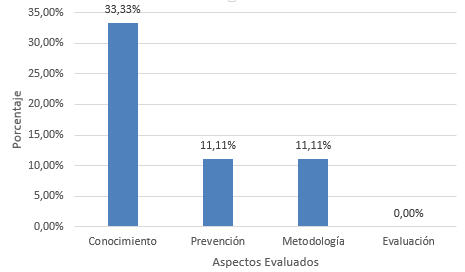


Figura 3‑21 Indicador Ataque Clickjacking

Fuente: Tabulación de encuestas realizadas.

De la cantidad de facultades encuestadas se ha identificado en la Figura 3-21 que el 33,33% conoce en que consiste este tipo de ataques, además el 11,11% ha manifestado prevenir esta vulnerabilidad empleando una metodología la cual no posee mucho fundamento documental se menciona el uso de una norma ISO pero no se identifica cuál, no se han registrado incidencias en las facultades por lo que se concluye que los sistemas informáticos en la ESPOCH se encuentran vulnerables a este tipo de ataques a más de ellos los técnicos no poseen herramientas para prevenirlos por desconocimiento.

#### Indicador Phishing

Para analizar el indicador de Suplantación de Identidad se ha formulado en la encuesta 4 preguntas con la finalidad de identificar si se conoce en las facultades este tipo de ataque, si se previene, la metodología empleada y la evaluación de ataques identificados, las preguntas formuladas fueron las siguientes:

* ¿Conoce usted en qué consiste de suplantación de identidad?
* ¿Se previene en la facultad los ataques de suplantación de identidad?
* ¿Existe una metodología en la facultad para prevenir ataques de suplantación de identidad?
* ¿Cuántos ataques de suplantación de identidad se han identificado?

De las preguntas encuestadas se ha obtenido el siguiente gráfico resumen:

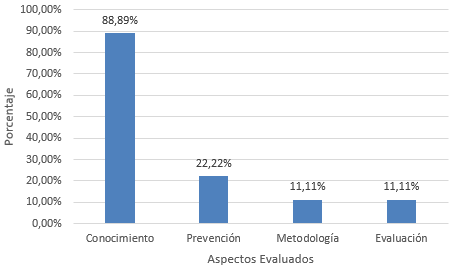


Figura 3‑22 Cantidad de Ataques de Suplantación de Identidad

Fuente: Tabulación de encuestas realizadas.

De los técnicos encuestados como muestra la Figura 3-22, se ha determinado que el 88,89% conocen en que consiste un ataque de suplantación de identidad, el 22,22% encuestados manifiesta que se previene este tipo de ataques en su facultad y el 11,11% emplea una metodología de prevención que radica en bloquear el sistema sin embargo el ataque de suplantación se emplea para obtener datos del usuario en sistemas informáticos que no pertenecen a la facultad de modo que el bloqueo del sistema no tendría ninguna intervención, la metodología empleada no es estandarizada, en IPEC se han detectado 10 casos de suplantación de identidad.

#### Indicador Tipos de aplicaciones

Para analizar el indicador de tipos de aplicaciones se ha realizado preguntas para identificar los tipos de aplicaciones de auto, televisión, web, escritorio y móvil resumido en el siguiente gráfico.

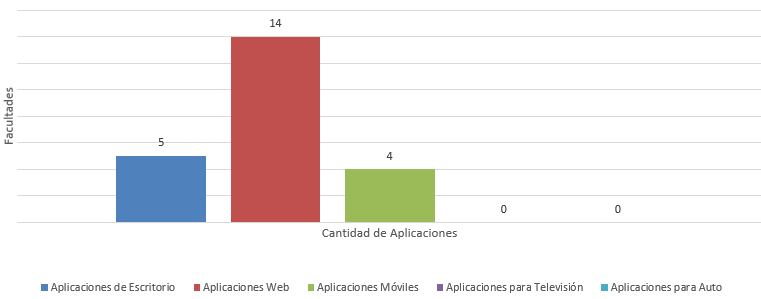


Figura 3‑23 Cantidad de Aplicaciones creadas en las Facultades

Fuente: Tabulación de encuestas realizadas.

En base a la Figura 3-23 se ha identificado la existencia de 14 aplicaciones web y de 4 aplicaciones móviles donde el 66,67% de facultades posee al menos una aplicación web y el 44,44% posee una aplicación móvil, aplicaciones que pueden estar vulnerables a los ataques identificados para el estudio, estas aplicaciones deberían poseer una metodología de prevención de ataques.

En la dimensión de Capa de Transporte se han identificado desconocimiento de las facultades en los ataques estudiados en donde existe una metodología o carecen de las mismas y no se realizan prevención de ataques de forma general las aplicaciones identificadas en el ámbito móvil y web se encuentran vulnerables.

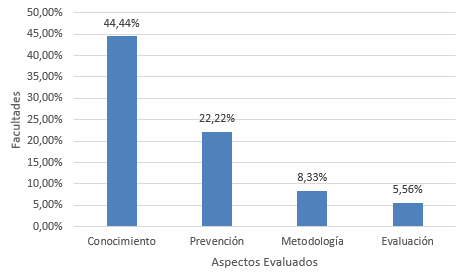


Figura 3‑24 Resumen Dimensión Capa de Presentación

Fuente: Tabulación de encuestas realizadas.

Como muestra la Figura 3-24 del análisis de la variable independiente se puede identificar que los usuarios desconocen los tipos de ataques y si los conocen en la mayoría de casos no los previenen, al prevenir los ataques no se emplean metodologías estandarizadas sino que son metodologías propias, al ser vulnerabilidades o ataques nuevos los técnicos no conocen como prevenirlos por lo que se evidencia la necesidad de estandarizar las metodologías de prevención de vulnerabilidades.

## Disponibilidad de Información

Para verificar la necesidad de incrementar la accesibilidad el Sistema de Gestión de Calidad de la Facultad de Informática y Electrónica se ha planteado la variable dependiente la misma que permite identificar los problemas de accesibilidad existentes.

### Dimensión Accesibilidad

#### Indicador Momento

Para analizar el indicador de momento se ha encuestado a los auditores del Centro CIMOGSYS si pueden emplear el SGC fuera de sus horarios de oficina en la siguiente pregunta:

¿Puede usted emplear el SGC fuera de su horario de oficina?

De la pregunta se ha obtenido el siguiente gráfico resumen:

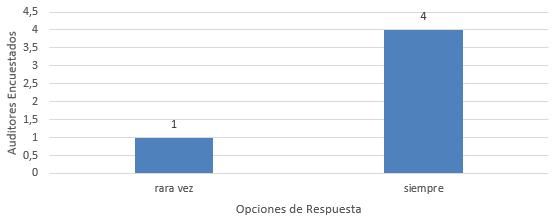


Figura 3‑25 Uso del SGC fuera de horario de oficina

Fuente: Tabulación de encuestas realizadas.

Sobre el uso del SGC de calidad como muestra la Figura 3-25, se han planteado 5 opciones sobre las cuales el 20% de los encuestados ha respondido que rara vez emplean el sistema fuera de horario de oficina mientras que el 80% restante menciona que siempre emplean el SGC fuera del horario de oficina lo que permite evidenciar que el SGC se encuentra disponible en cualquier momento.

#### Indicador Lugar

Para analizar el indicador de lugar se ha preguntado a los usuarios auditores si se ha podido emplear el SGC en la ESPOCH, fuera de la ciudad y fuera del país, además se ha encuestado a los auditores sobre la existencia de dificultades al emplear el sistema en los lugares mencionados.

¿Puede usar el SGC en los auditorios o laboratorios de la ESPOCH?

De la pregunta se obtiene el siguiente gráfico resumen:

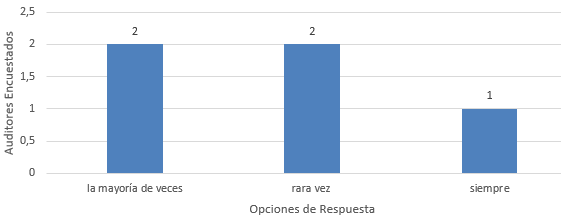


Figura 3‑26 Uso del SGC en la ESPOCH

Fuente: Tabulación de encuestas realizadas.

De los datos obtenidos como muestra la Figura 3-26, el 20% de auditores encuestados ha manifestado que siempre pueden usar el SGC en los laboratorios de la ESPOCH, el 20% menciona que la mayoría de veces se puede emplear el sistema y el 20% restante menciona que rara vez pueden emplear el sistema, el 80% de los usuarios que tienen dificultades para usar el sistema en los laboratorios ha mencionado que se debe a problemas de conectividad a internet mientras que el 20% ha tenido inconvenientes por fala de equipos, para solventar el problema de conectividad a internet se plantea como opción la creación de una aplicación móvil que permita visualizar los indicadores necesarios de forma oportuna ya sea en una red wifi o en su defecto mediante el empleo de paquetes de datos.

¿Ha salido Usted de la Ciudad de Riobamba y ha podido usar el Sistema de Gestión de Calidad?

De la pregunta se obtiene el siguiente gráfico resumen:

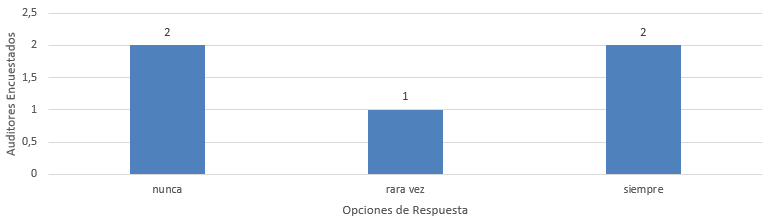


Figura 3‑27 Uso del SGC fuera de la ciudad de Riobamba

Fuente: Tabulación de encuestas realizadas.

Los auditores de CIMOGSYS encuestados según la Figura 3-27, han manifestado que el 20% siempre puede emplear el SGC fuera de la ciudad de Riobamba, el 20% rara vez puede usar el sistema y el 20% nunca ha podido emplear el sistema fuera de la ciudad a lo que el 60% de encuestados indica que se debe a la falta de un computador y el 20% por problemas de conectividad a internet, se identifica que el sistema puede ser empleado fuera de la ciudad de Riobamba con inconvenientes de hardware.

¿Ha salido Usted del País y ha podido usar el Sistema de Gestión de Calidad?

De la pregunta se ha obtenido el siguiente gráfico resumen:

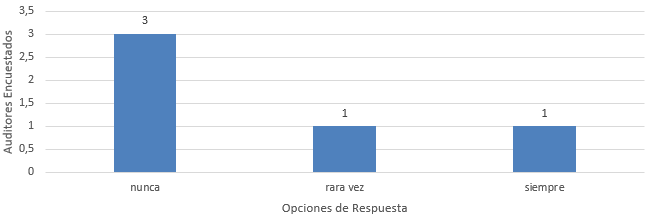


Figura 3‑28 Uso de SGC fuera del País

Fuente: Tabulación de encuestas realizadas.

De las encuestas realizadas como muestra la Figura 3-28, se evidencia que el 60% de los auditores nunca ha podido emplear el SGC fuera del país, el 20% rara vez puede emplearlo y 20% siempre ha podido emplearlo, de las posibles causas de estos problemas de uso el 100% menciona que el no poseer un ordenador disponible es la limitante de uso del sistema.

Al evaluar el indicador de lugar se verifica que el sistema puede ser empleado en cualquier lugar sin embargo se esto tiene sus limitantes que son problemas de conectividad a internet y ordenadores disponibles puesto que el sistema se encuentra en su versión web, el problema de conectividad a internet se ha analizado en el indicador de momento, para disminuir el requisito de hardware se propone el empleo de una aplicación móvil que reemplace al uso del ordenador en caso de ser necesario.

#### Indicador Dispositivo

Para analizar el indicador de dispositivo se ha preguntado a los usuarios auditores si se ha podido emplear el SGC en la web, en dispositivos móviles, en televisores y autos, además se ha encuestado a los auditores sobre la experiencia de uso en los dispositivos mencionados anteriormente.

¿Ha utilizado Usted el Sistema de Gestión de Calidad en un navegador web?

De la pregunta se ha obtenido el siguiente gráfico resumen:

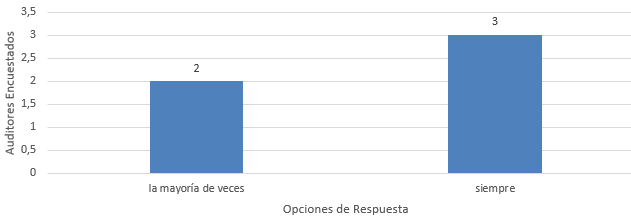


Figura 3‑29 Uso del SGC en la Web

Fuente: Tabulación de encuestas realizadas.

Sobre el SGC se han manifestado, como muestra la Figura 3-29, que el 60% de los usuarios siempre pueden emplear el sistema de gestión de calidad en un navegador web y el 40% puede emplearlo la mayoría de veces no obstante sobre su experiencia de uso se ha identificado que el 20% puede emplear el SGC en un navegador web con dificultades, el 60% lo puede usar normalmente y el 20% restante lo puede emplear sin ningún inconveniente, estos resultados evidencian que los usuarios encuentran accesible el contenido del sistema en un navegador web aunque su uso experiencia de uso de no evidencia de igual manera esto puede darse por problemas en el diseño de la interfaz, navegación confusa o falta de capacitación sobre el sistema.

¿Ha utilizado Usted el Sistema de Gestión de Calidad en un dispositivo móvil?

De la pregunta se ha obtenido el siguiente gráfico resumen:

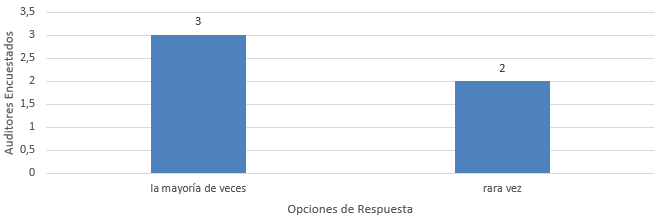


Figura 3‑30 Uso del SGC en el Móvil

Fuente: Tabulación de encuestas realizadas.

Sobre el uso del SGC en un dispositivo móvil, como muestra la Figura 3-30, los usuarios encuestados han manifestado que el 60% puede usar el sistema la mayoría de veces mientras que el 40% puede usarlo rara vez, sobre la experiencia de uso los usuarios solo el 20% puede usar el sistema fácilmente mientras que el 20% lo puede usar con dificultades y el 60% no puede usar el SGC, para mejorar la accesibilidad en los dispositivos móvil se sugiere la creación de una aplicación móvil con lo que se reducirá los problemas de accesibilidad.

¿Puede usar el SGC en un televisor?

De la pregunta se ha obtenido el siguiente gráfico resumen:

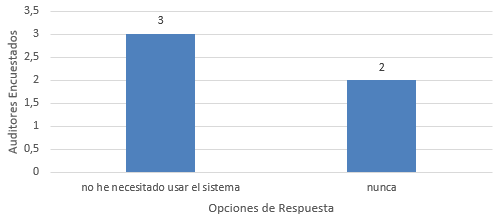


Figura 3‑31 Uso del SGC en la Televisión

Fuente: Tabulación de encuestas realizadas.

Los auditores mediante las encuestas, como muestra la Figura 3-31, el 60% ha manifestado que no le hecho falta emplear el SGC en un televisor mientras que el 40% nunca ha podido usarlo, no se mencionan causas por las que no se ha podido usar el SGC, el empleo de estos dispositivos en la actualidad no es muy común por lo que es normal que los usuarios no se encuentren familiarizados sin embargo el 40% ha intentado emplear su uso sin éxito.

¿Puede usar el SGC en un automóvil?

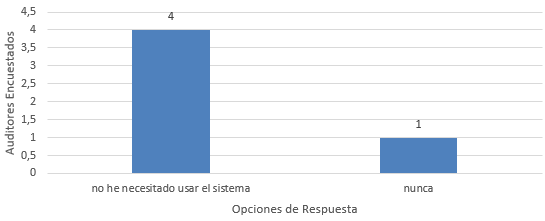


Figura 3‑32 Uso del SGC en autos

Fuente: Tabulación de encuestas realizadas.

Del total de encuestas receptadas, como muestra la Figura 3-32, se ha obtenido un total de 80% de usuarios que no han necesitado emplear el sistema en automóviles mientras que el 20% nunca ha podido utilizarlo esto puede darse a que no posee un vehículo con las características necesarias para visualizar el sistema o lo ha intento usar sin éxito.

Del indicador de dispositivo se puede verificar que el SGC se emplea mayoritariamente en dispositivos que puedan visualizar contenido web como computadores, tabletas y teléfonos inteligentes sin embargo la experiencia de uso de los usuarios no es excelente por lo que se plantea como posibles soluciones, la mejora de la interfaz web para que se adapte a dispositivos móviles si fuera el caso o en su defecto crear una aplicación específica para los dispositivos móviles con lo que se cumpliría el segundo índice del indicador.

La dimensión de accesibilidad según las políticas W3C permite que un usuario pueda hacer uso de la información en cualquier momento, lugar y dispositivo a los cual en el análisis de indicadores se ha verificado que en el Sistema de Gestión de Calidad el usuario puede acceder a la información en cualquier momento definidos como en horario de oficina y fuera de él, con respecto a cualquier lugar se identificó que los usuarios pese a los problemas de conectividad de internet y falta de ordenadores puede emplear el SGC en la ESPOCH, fuera de la Ciudad y Fuera del País para cumplir con este indicador se propone la creación de una aplicación móvil con lo que se suprimiría la dependencia de equipos como computadores e incluso de conexión a internet mediante el análisis realizado en la investigación sobre el indicador de dispositivos web, móvil, televisión y auto se propone resolver el segundo indicador mediante la aplicación móvil.

# PROPUESTA DE MEJORES PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES MÓVILES

Mediante la propuesta de mejores prácticas se pretende disminuir el problema de seguridad informática identificado en la Escuela Superior Politécnica de Chimborazo específicamente en el desarrollo de aplicaciones móviles a cargo del Centro de Investigación en Modelos de Gestión y Sistemas Informáticos, para implementar la propuesta se ha generado una aplicación móvil para el Sistema de Gestión de Información que será aplicado en la Facultad de Administración de Empresas, si bien es cierto es un modelo para un determinado grupo de proyectos de software el mismo puede ser implementado en diversos proyectos aplicando la metodología propuesta.

## Estado Inicial de la Facultad de Administración de Empresas

La Facultad de Administración de Empresas apuesta a la innovación y el desarrollo tecnológico de manera conjunta con la transferencia de conocimiento con las demás facultades en la ESPOCH, en la actualidad la facultad se encuentra implementado modelos de gestión informatizados, el proyecto inició en el año 2011 mediante la Comisión de Sistemas de Gestión de Calidad, para el año 2012 la facultad contaba ya con la estructura documental de los modelos, no obstante, hasta el año 2013 fueron aprobadas las políticas del Sistema de Gestión de Calidad SGC con enfoque de procesos.

Al año 2014 la facultad inicia la implementación del ciclo de mejora continua dentro del SGC por lo que se genera la necesitad de automatizar los sistemas, se creó el primer Sistema de Gestión de Información que comprende el portal web de la Facultad, el Sistema de Gestión de Procesos, Balance Score Card y Sistema de Gestión de Indicadores de Acreditación, sistemas que en la actualidad se encuentran funcionando y permiten realizar las auditorías a los procesos internos.

En la actualidad se estudia dar mayor accesibilidad a los sistemas informáticos por tanto al haber estudiado los niveles de seguridad en las facultades de la ESPOCH y en especial al haber analizado ataques y sus mecanismos de prevención, se ha verificado en la FADE, el desconocimiento en gran parte de la lista de ataques encuestados así que para continuar con el ciclo de la mejora continua e implementación de sistemas informáticos es necesario aplicar seguridad al software en la facultad.

## Estado Inicial del Centro de Investigación en Modelos de Gestión y Sistemas Informáticos

El centro de investigación fue creado en el año 2015 el mes de agosto entre dos grupos de Investigación de las facultades de Informática y Electrónica y Administración de Empresas, el centro ha asumido las competencias de innovación de desarrollo de la Comisión de Gestión de Sistemas de Calidad, por lo que en la actualidad asume la creación y desarrollo de los productos de gestión y aplicaciones de software.

La propuesta de innovación que maneja el centro continuamente ha permitido identificar el requerimiento de la creación de una aplicación móvil con la finalidad de eliminar limitaciones que presentan las aplicaciones web existentes, debido al desconocimientos de los ataques existentes en la ESPOCH y a la cantidad de software que se genera para su implementación es necesario generar políticas de seguridad de la información sensible que se genera en el Sistema de Gestión de Información, vital para la toma de decisiones.

## Mejores Prácticas de Seguridad Para el Desarrollo de Aplicaciones Móviles

Las prácticas de seguridad se proponen por la existencia de vulnerabilidades en la Escuela Superior Politécnica d Chimborazo, estas vulnerabilidades han sido recopiladas por el estudio de seguridades efectuado a manera de encuestas a los responsables de los laboratorios, centro de cómputo, informáticos de cada Facultad así como al Instituto de Posgrado y Educación Continua y el Departamento de Tecnologías de la Información y Comunicación.

Se definirá que una buena práctica es un conjuntos de procedimientos que funcionan bien y que generan buenos resultados, que han sido replicados, validados y merece ser compartida, este concepto se ha fundamentado como en la definición de la Organización de Naciones Unidas para la Alimentación y Agricultura, de este concepto genérico se obtiene que una buena práctica de seguridad es un conjunto de parámetros, lineamientos y directrices que permiten disminuir las vulnerabilidades que se producen mediante el desarrollo de software, que han sido probadas, funcionan bien y merecen ser adoptadas por la comunidad de desarrollo de software.

Hasta el momento el estudio realizado no ha podido identificar ningún estándar que generalice este proceso de desarrollo no obstante se han identificado 3 propuestas de prácticas de seguridad para el desarrollo de aplicaciones móviles que son:

* Secure Mobile Development (NowSecure)
* Mobile Security Premier (NowSecure)
* Mobile Security Project – Top Ten Mobile Risks (OWASP)

De los 3 estudios se han identificado las principales características que influyen en el desarrollo de software móvil y se han ido anexando a la propuesta actual, con la finalidad de cubrir aspectos faltantes, las propuestas han sido organizadas en 4 grupos que hacen referencia al modelo principal de interacción de una aplicación o sistema informático de la siguiente manera:

Tabla 4‑1 Buenas Prácticas de Seguridad para el Desarrollo de Aplicaciones

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N°** | **Buena Práctica** | **CAD** | **CLN** | **CT** | **CP** |
| 1 | Analizar el Almacenamiento de Datos en HTML 5 |  | A |  | A |
| 2 | Analizar la Red de Transmisión de Datos |  |  | A |  |
| 3 | Analizar las Vulnerabilidades del Almacenamiento de Datos | A | B |  | M |
| 4 | Analizar las Vulnerabilidades del Framework de Desarrollo |  | A |  | A |
| 5 | Analizar las Vulnerabilidades del Sistema Operativo Huésped | B | M |  | A |
| 6 | Analizar los Datos de Buffer y Cache | B | B | B | B |
| 7 | Emitir Alertas al Usuario Cuando no se Emplee un Canal de Transmisión de Datos Seguro |  | M |  | M |
| 8 | Emplear un Canal de Transmisión de Datos Seguro SSL/TLS |  | B | A |  |
| 9 | Evitar el Uso de Canales de Transmisión de Datos Alternativo (SMS, MMS) |  |  |  | A |
| 10 | Evitar el Uso de Certificados de Compañías no Reconocidas |  | M | A |  |
| 11 | Evitar el Uso del Método Get para Enviar Datos |  | A |  | A |
| 12 | Implementar una Metodología de Codificación | B | A |  | M |
| 13 | Implementar una Metodología para el Manejo de Datos Geográficos |  | B |  | A |
| 14 | Implementar Complejidad y Ofuscación en el Código | B | A |  | A |
| 15 | Implementar una Metodología de Respuestas a Fuentes de Datos no Seguras |  | A | M |  |
| 16 | Implementar una Metodología de Validación de Formularios |  | A |  | M |
| 17 | Implementar una Metodología para Asignación de Permisos y Privilegios | A | M |  |  |
| 18 | Implementar una Metodología para el Cifrado de Datos | M | A | A | B |
| 19 | Implementar una Metodología para el Manejo de Archivos | M | A |  | A |
| 20 | Implementar una Metodología para el Manejo de Archivos de Manifiesto/Configuración |  | M |  | A |
| 21 | Implementar una Metodología para el Manejo de Archivos XML | B | M |  | A |
| 22 | Implementar una Metodología para el Manejo de Cookies |  | A |  | A |
| 23 | Implementar una Metodología para el Manejo de Logs | A | A | A | B |
| 24 | Implementar una Metodología para el Manejo de Servicios Web | M | A |  | A |
| 25 | Implementar una Metodología para el Manejo de Sesiones | B | A | B | A |
| 26 | Implementar una Metodología para el Uso de Autenticación de Doble Factor |  | A |  | B |
| 27 | Implementar una Metodología para el Uso de Claves Seguras | A | A |  | M |
| 28 | Realizar procesos de Verificación de Permisos y Privilegios | A | A |  | M |
| 29 | Realizar procesos de Autenticación y Autorización | A | A | B | M |
| 30 | Implementar una Política para el Manejo de URL |  | A | M | A |
| 31 | Ocultar el Uso de Números de Cuenta y Tokens de Formularios |  | A |  | A |
| 32 | Prevenir Ataques CSRF |  | A |  | B |
| 33 | Prevenir Ataques de Descarga de Drive |  | M |  | A |
| 34 | Prevenir Ataques de Día Cero | B | B | B | B |
| 35 | Prevenir Ataques de Envenenamiento DNS |  | M | A |  |
| 36 | Prevenir Ataques de Fuerza Bruta |  | A | M |  |
| 37 | Prevenir Ataques de Hombre en el Medio |  | M | A |  |
| 38 | Prevenir Ataques de Hombre en el Móvil |  | B |  | A |
| 39 | Prevenir Ataques de Secuestro de Clic |  |  |  | A |
| 40 | Prevenir Ataques de Secuestro de Paquetes |  |  | A |  |
| 41 | Prevenir Ataques de Secuestro de Sesiones |  | M | A | B |
| 42 | Prevenir Ataques de Suplantación de Identidad |  |  | M | A |
| 43 | Prevenir Ataques RF |  |  |  | A |
| 44 | Prevenir Ataques SlStrip |  |  | A | B |
| 45 | Prevenir Ataques SMiShing |  |  |  | A |
| 46 | Prevenir Ataques XSS |  | A |  | B |
| 47 | Prevenir el Uso de Software Fabricado por Terceros | B | A | B | A |
| 48 | Prevenir Inyecciones SQL | A | A |  | B |
| 49 | Prevenir la Inclusión de Archivos en la Aplicación |  |  |  | A |
| 50 | Prevenir la Modificación de Archivos Fuentes |  |  |  | A |
| 51 | Verificar los Canales de Distribución de la Aplicación |  |  |  | A |
| 52 | Prevenir ataques BYOD |  |  |  |  |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

En la Tabla 4-1 se han ordenado las prácticas de seguridad para el desarrollo de aplicaciones, las prácticas han sido priorizadas según su importancia (Alta = A, Media = M, Baja = B) y aplicación en las capas, las capas han sido codificadas como “CAD” Capa de Almacenamiento de Datos, “CLN” Capa de Lógica del Negocio, “CT” Capa de Transporte y “CP” Capa de Presentación, se identificaron 52 políticas de seguridad, las mismas que pueden ser aplicadas en conjunto o por cada capa.

No obstante al realizar un análisis de las prácticas sugeridas a los resultados de las encuestas aplicadas en la ESPOCH se puede identificar claramente que existen vulnerabilidades que pueden ser fácilmente corregidas, en el caso de la capa de almacenamiento de datos, se evidencia que no se aplican políticas para la asignación de usuarios, sus permisos y privilegios, esto junto al desconocimiento de los mismos por parte de los encargados que fueron encuestados y en el caso de conocerlos no aplican una metodología para su asignación así como no se registran Logs de acciones, estas vulnerabilidades pueden ser corregidas mediante la práctica 17 de la tabla 4-1, de igual forma no se conocen los comandos de ejecución del sistema operativo, no se conoce que no hace falta vulnerar el motor de datos en sí, si no, basta apoderarse del sistema operativo huésped teniendo así la capacidad de ejecutar comandos de bases de datos sin acceder a la misma, esta vulnerabilidad la previene la práctica 5.

En cuanto a la capa de transporte los usuarios han manifestado que no se emplean mecanismos de cifrado de datos, es decir los datos pasan de forma clara a través de la red de comunicación esto permite a un atacante ver información sensible sin necesidad de vulnerar un algoritmo criptográfico, la práctica 18 enuncia que se debe implementar una metodología de cifrado de datos que para la misma se recomienda la utilización de algoritmos de cifrado como AES 256 dado que mecanismos de hasheado como md5 ya no son seguros, otra vulnerabilidad que complementa al cifrado de datos es el uso de firmas SSL no validadas por una empresa, si bien es cierto quizás una firma auténtica podría prevenir un ataque, ningún proceso nos garantiza que el certificado autónomo sea seguro, sería mejor confiar en una empresa de seguridad, esta recomendación la contempla las políticas 8 y 44 que tratan de canales de conexión segura sobre SSL/TLS, finalmente no existen medios ni mecanismos de prevención ante ataques de hombre en el medio, por lo que la red de la ESPOCH podría estar vulnerable a ataques de hombre en el medio, para prevenir este ataque se recomienda el cifrado de datos como medida disuasiva y como prevención implementar mecanismos de acceso a la red como claves, firewalls que bloqueen puertos de software de rastreo.

En cuanto al servidor o capa de lógica del negocio se identifican problemas en el uso de metodologías para la validación de formularios, prevención de ataques DoS, XSS y de fuerza bruta, estas vulnerabilidades son contrarrestadas haciendo uso de las prácticas 16, 35 y 46 respectivamente, lo básico para aplicar las buenas prácticas es buscar una metodología de prevención como por ejemplo cantidad de inicio de sesión, o la validación de los campos de datos en base al diccionario de datos de nuestro motor, sin embrago lo preocupante es que los encargados conocen de las vulnerabilidades pero no buscan prevenirlas, sin embargo ningún sistema informático está exento de un ataque de día cero, por lo que es mejor mantener el mayor número de vulnerabilidades conocidas mitigadas.

Para identificar cuáles son las mejores prácticas imprescindibles en cada capada de la arquitectura de un sistema informático se han generado las siguientes listas en orden de prioridad:

### Capa de Almacenamiento de Datos

Todos los sistemas o aplicaciones necesitan manejar datos, no siempre empleando un motor de base de datos sino que pueden usarse archivos, la memoria del sistema operativo o el hardware sobre el cual se ha implementado, en esta capa es de vital importancia aplicar políticas de seguridad ya que se considera un punto sensible en toda arquitectura de un sistema informático, para asegurar esta capa se proponen las siguientes consideraciones:

Tabla 4‑2 Buenas Prácticas de Seguridad para la Capa de Almacenamiento de Datos

|  |  |
| --- | --- |
| **Buena Práctica** | **CAD** |
| Analizar las Vulnerabilidades del Almacenamiento de Datos | A |
| Implementar una Metodología para Asignación de Permisos y Privilegios | A |
| Implementar una Metodología para el Manejo de Logs | A |
| Implementar una Metodología para el Uso de Claves Seguras | A |
| Realizar procesos de Verificación de Permisos y Privilegios | A |
| Realizar procesos de Autenticación y Autorización | A |
| Prevenir Inyecciones SQL | A |
| Implementar una Metodología para el Cifrado de Datos | M |
| Implementar una Metodología para el Manejo de Archivos | M |
| Implementar una Metodología para el Manejo de Servicios Web | M |
| Analizar las Vulnerabilidades del Sistema Operativo Huésped | B |
| Analizar los Datos de Buffer y Cache | B |
| Implementar una Metodología de Codificación | B |
| Implementar Complejidad y Ofuscación en el Código | B |
| Implementar una Metodología para el Manejo de Archivos XML | B |
| Implementar una Metodología para el Manejo de Sesiones | B |
| Prevenir Ataques de Día Cero | B |
| Prevenir el Uso de Software Fabricado por Terceros | B |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos

En la Tabla 4-2 se han sugerido políticas de seguridad para prevenir ataques a nivel de almacenamiento de datos, son 18 políticas para su implementación de las cuales han sido calificadas como prioridad Alta son aquellas prácticas que deben ser aplicadas obligatoriamente y de manera inmediata, en cuanto a las priorizadas como Bajas son opcionales.

### Capa de Lógica del Negocio

Todos los sistemas o aplicaciones necesita implementar la lógica de funcionamiento esto por lo general se realiza mediante un servidor, generalmente web hoy en día, esta capa involucra al servidor, sus configuraciones y protecciones debidas, además implica la seguridad de todas las transacciones que se generen, para asegurar de mejor manera esta capa se proponen las siguientes prácticas:

Tabla 4‑3 Buenas Prácticas de Seguridad para la Capa de Lógica del Negocio

|  |  |
| --- | --- |
| **Buena Práctica** | **CLN** |
| Analizar el Almacenamiento de Datos en HTML 5 | A |
| Analizar las Vulnerabilidades del Framework de Desarrollo | A |
| Evitar el Uso del Método Get para Enviar Datos | A |
| Implementar una Metodología de Codificación | A |
| Implementar Complejidad y Ofuscación en el Código | A |
| Implementar una Metodología de Respuestas a Fuentes de Datos no Seguras | A |
| Implementar una Metodología de Validación de Formularios | A |
| Implementar una Metodología para el Cifrado de Datos | A |
| Implementar una Metodología para el Manejo de Archivos | A |
| Implementar una Metodología para el Manejo de Cookies | A |
| Implementar una Metodología para el Manejo de Logs | A |
| Implementar una Metodología para el Manejo de Servicios Web | A |
| Implementar una Metodología para el Manejo de Sesiones | A |
| Implementar una Metodología para el Uso de Autenticación de Doble Factor | A |
| Implementar una Metodología para el Uso de Claves Seguras | A |
| Realizar procesos de Verificación de Permisos y Privilegios | A |
| Realizar procesos de Autenticación y Autorización | A |
| Implementar una Política para el Manejo de URL | A |
| Ocultar el Uso de Números de Cuenta y Tokens de Formularios | A |
| Prevenir Ataques CSRF | A |
| Prevenir Ataques de Fuerza Bruta | A |
| Prevenir Ataques XSS | A |
| Prevenir el Uso de Software Fabricado por Terceros | A |
| Prevenir Inyecciones SQL | A |
| Analizar las Vulnerabilidades del Sistema Operativo Huésped | M |
| Emitir Alertas al Usuario Cuando no se Emplee un Canal de Transmisión de Datos Seguro | M |
| Evitar el Uso de Certificados de Compañías no Reconocidas | M |
| Implementar una Metodología para Asignación de Permisos y Privilegios | M |
| Implementar una Metodología para el Manejo de Archivos de Manifiesto/Configuración | M |
| Implementar una Metodología para el Manejo de Archivos XML | M |
| Prevenir Ataques de Descarga de Drive | M |
| Prevenir Ataques de Envenenamiento DNS | M |
| Prevenir Ataques de Hombre en el Medio | M |
| Prevenir Ataques de Secuestro de Sesiones | M |
| Analizar las Vulnerabilidades del Almacenamiento de Datos | B |
| Analizar los Datos de Buffer y Cache | B |
| Emplear un Canal de Transmisión de Datos Seguro SSL/TLS | B |
| Implementar una Metodología para el Manejo de Datos Geográficos | B |
| Prevenir Ataques de Día Cero | B |
| Prevenir Ataques de Hombre en el Móvil | B |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

En la Tabla 4-3 se han sugerido políticas de seguridad para prevenir ataques a nivel de la capa de lógica del negocio o consideraciones para el servidor, son 40 políticas para su implementación de las cuales han sido calificadas como prioridad Alta son aquellas prácticas que deben ser aplicadas obligatoriamente y de manera inmediata, en cuanto a las priorizadas como Bajas son opcionales.

### Capa de Transporte

Esta capa hace referencia al medio físico por el cual se transportan los datos en la aplicación por lo general aquí se producen los ataques de espionaje, para disminuir las vulnerabilidades se proponen las siguientes recomendaciones:

Tabla 4‑4 Buenas Prácticas de Seguridad para la Capa de Transporte

|  |  |
| --- | --- |
| **Buena Práctica** | **CT** |
| Analizar la Red de Transmisión de Datos | A |
| Emplear un Canal de Transmisión de Datos Seguro SSL/TLS | A |
| Evitar el Uso de Certificados de Compañías no Reconocidas | A |
| Implementar una Metodología para el Cifrado de Datos | A |
| Implementar una Metodología para el Manejo de Logs | A |
| Prevenir Ataques de Envenenamiento DNS | A |
| Prevenir Ataques de Hombre en el Medio | A |
| Prevenir Ataques de Secuestro de Paquetes | A |
| Prevenir Ataques de Secuestro de Sesiones | A |
| Prevenir Ataques SlStrip | A |
| Implementar una Metodología de Respuestas a Fuentes de Datos no Seguras | M |
| Implementar una Política para el Manejo de URL | M |
| Prevenir Ataques de Fuerza Bruta | M |
| Prevenir Ataques de Suplantación de Identidad | M |
| Analizar los Datos de Buffer y Cache | B |
| Implementar una Metodología para el Manejo de Sesiones | B |
| Implementar una Metodología para Procesos de Autenticación y Autorización | B |
| Prevenir Ataques de Día Cero | B |
| Prevenir el Uso de Software Fabricado por Terceros | B |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

En la Tabla 4-4 se han sugerido políticas de seguridad para prevenir ataques a nivel de la capa de transporte, son 19 políticas para su implementación de las cuales han sido calificadas como prioridad Alta son aquellas prácticas que deben ser aplicadas obligatoriamente y de manera inmediata, en cuanto a las priorizadas como Bajas son opcionales.

### Capa de Presentación

Es la capa que permite la comunicación del usuario con la aplicación son las interfaces que permiten que sea usable la aplicación en la capa de presentación se recomienda tener en cuenta lo siguiente:

Tabla 4‑5 Buenas Prácticas de Seguridad para la Capa de Presentación

|  |  |
| --- | --- |
| **Buena Práctica** | **CP** |
| Analizar el Almacenamiento de Datos en HTML 5 | A |
| Analizar las Vulnerabilidades del Framework de Desarrollo | A |
| Analizar las Vulnerabilidades del Sistema Operativo Huésped | A |
| Evitar el Uso de Canales de Transmisión de Datos Alternativo (SMS, MMS) | A |
| Evitar el Uso del Método Get para Enviar Datos | A |
| Implementar una Metodología para el Manejo de Datos Geográficos | A |
| Implementar Complejidad y Ofuscación en el Código | A |
| Implementar una Metodología para el Manejo de Archivos | A |
| Implementar una Metodología para el Manejo de Archivos de Manifiesto/Configuración | A |
| Implementar una Metodología para el Manejo de Archivos XML | A |
| Implementar una Metodología para el Manejo de Cookies | A |
| Implementar una Metodología para el Manejo de Servicios Web | A |
| Implementar una Metodología para el Manejo de Sesiones | A |
| Implementar una Política para el Manejo de URL | A |
| Ocultar el Uso de Números de Cuenta y Tokens de Formularios | A |
| Prevenir Ataques de Descarga de Drive | A |
| Prevenir Ataques de Hombre en el Móvil | A |
| Prevenir Ataques de Secuestro de Clic | A |
| Prevenir Ataques de Suplantación de Identidad | A |
| Prevenir Ataques RF | A |
| Prevenir Ataques SMiShing | A |
| Prevenir el Uso de Software Fabricado por Terceros | A |
| Prevenir la Inclusión de Archivos en la Aplicación | A |
| Prevenir la Modificación de Archivos Fuentes | A |
| Verificar los Canales de Distribución de la Aplicación | A |
| Analizar las Vulnerabilidades del Almacenamiento de Datos | M |
| Emitir Alertas al Usuario Cuando no se Emplee un Canal de Transmisión de Datos Seguro | M |
| Implementar una Metodología de Codificación | M |
| Validar Formularios | M |
| Implementar una Metodología para el Uso de Claves Seguras | M |
| Realizar procesos de verificación de Permisos y Privilegios | M |
| Realizar procesos de Autenticación y Autorización | M |
| Analizar los Datos de Buffer y Cache | B |
| Implementar una Metodología para el Cifrado de Datos | B |
| Implementar una Metodología para el Manejo de Logs | B |
| Implementar una Metodología para el Uso de Autenticación de Doble Factor | B |
| Prevenir Ataques CSRF | B |
| Prevenir Ataques de Día Cero | B |
| Prevenir Ataques de Secuestro de Sesiones | B |
| Prevenir Ataques SlStrip | B |
| Prevenir Ataques XSS | B |
| Prevenir Inyecciones SQL | B |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

En la Tabla 4-5 se han sugerido políticas de seguridad para prevenir ataques a nivel de la capa de presentación, son 42 políticas para su implementación de las cuales han sido calificadas como prioridad Alta son aquellas prácticas que deben ser aplicadas obligatoriamente y de manera inmediata, en cuanto a las priorizadas como Bajas son opcionales.

Se han determinado las prácticas de seguridad que deben aplicarse en cada capa de forma obligatoria por el impacto de la vulnerabilidad en la misma, no obstante se han propuesto medidas de seguridad genéricas que pueden ser aplicadas en cualquier tipo de aplicación, sin embargo se propone su uso de forma organizada de la siguiente manera:

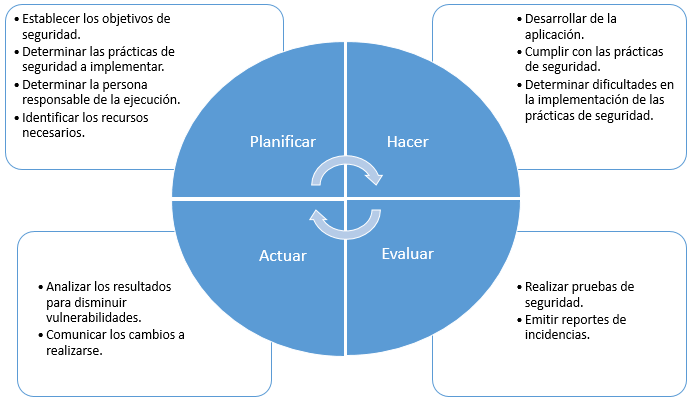


Figura 4‑1 Forma de Aplicar las Propuestas de Seguridad

Fuente: Fausto Cevallos, Javier Sigüenza.

La Figura 4-1 visualiza la forma de aplicar las prácticas de seguridad identificadas, se contempla 4 etapas en las cuales se realizará el proceso de asegurar la aplicación, la planificación permite al equipo de desarrollo definir la persona que será responsable de la seguridad, en conjunto se definirán los objetivos de seguridad que representan a las capas a emplearse, de igual forma escogerán de la propuesta las consideraciones que se pueden emplear, si hubiere la necesidad de emplear recursos externos o extras podrá ser definido con oportunidad, la etapa de hacer contempla en neto desarrollo de la aplicación, su programación e interfaces, aquí se deben aplicar las políticas de seguridad planificadas y registrar si hubiere los problemas para su implementación.

En la fase de evaluar se realizarán las pruebas que como resultado mostrarán que las vulnerabilidades han sido aseguradas, se deben definir también el mecanismo de realización de las pruebas y las condiciones de las mismas, se mantendrá un registro de incidencias si hubiere el caso, finalmente la etapa de actuar estará dirigida por el responsable de seguridad, esta persona interpretará los resultados de las pruebas de seguridad y anunciará los cambios a realizarse si fueren necesarios.

Estas etapas han sido propuestas para complementar el uso de las prácticas de seguridad, es de responsabilidad del equipo implementarlas en conjunto con la metodología de desarrollo de software, es importante su aplicación ya que dadas razones como “el bajo presupuesto para la seguridad en el desarrollo de aplicaciones, el fácil acceso a frameworks de desarrollo que no priorizan la seguridad y el desconocimiento de los lenguajes de programación modernos” (OWASP, 2015) hacen que hoy en día se mantengan priorizadas las prisas y el desconocimiento, es por eso que se debe impulsar la inversión en seguridad informática.

## Desarrollo de la aplicación móvil del Sistema de Gestión de Información, haciendo uso de buenas prácticas de seguridad, implementada en la Facultad de Administración de Empresas.

El Centro de Investigación en Modelos de Gestión y Sistemas Informáticos CIMOGSYS de la Escuela Superior Politécnica de Chimborazo ESPOCH, ejecuta proyectos que permiten el aseguramiento de la calidad de las facultades y áreas de gestión de la ESPOCH enfocados en parámetros gubernamentales, del Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior CEAACES así como la Ley Orgánica de Educación Superior (LOES, Título IV, Capítulo 1, articulo 93-94, 2010) con la finalidad de lograr la acreditación por carreras y universitaria.

Las facultades de la Escuela Superior Politécnica de Chimborazo se encuentran inmersas en procesos de acreditación y evaluación continua, por este motivo se ha visto la necesidad en cada una de ellas de crear y aplicar distintas metodologías, herramientas y conceptos que lleven a incrementar su nivel de calidad ofertada a los educandos, en la Facultad de Administración de Empresas se han creado sistemas informáticos guiados por el centro CIMOGSYS que permiten la evaluación y seguimiento de todos los indicadores de acreditación necesarios.

Los sistemas informáticos creados en la Facultad de Administración de Empresas son parte de un Sistema de Gestión de Información SGI que permite a sus usuarios conocer el estado de tres perspectivas de la facultad que se enmarcan en los modelos de acreditación, el Sistema de Gestión de Procesos SGP[[4]](#footnote-4) permite llevar el control de la calidad de los procesos de la facultad enmarcados en el Sistema de Gestión de Calidad, El sistema Balance Score Card[[5]](#footnote-5) permite medir el cumplimiento de la planificación estratégica y el Sistema de Gestión de Indicadores de Acreditación[[6]](#footnote-6) basados en los criterios del modelo CEAACES.

Estos sistemas se encuentran publicados en una plataforma en la nube como aplicaciones web creadas en el lenguaje PHP con el framework Laravel en su versión 4.2 con un motor de base de datos MySql, para incrementar la accesibilidad de los sistemas se propone la creación de una aplicación móvil mediante el uso de Apache Córdova que permite la creación de aplicaciones móviles a base de aplicaciones web, la aplicación se encuentra direccionada a los sistemas operativos móviles más populares Android y iOS, esto permitirá eliminar las limitaciones que presentan las aplicaciones netamente web.

No obstante la aplicación debe incrementar la disponibilidad de información del Sistema de Gestión de Información SGI por lo que se ha realizado una propuesta de mejores prácticas de seguridad para el desarrollo de aplicaciones móviles y será aplicada en este proyecto, por lo que al incrementar la seguridad de la aplicación se incrementa la disponibilidad de la misma, se pretende emplear las técnicas de prevención que involucren netamente al desarrollo de software, se recomienda su aplicación de manera integral ya que capas como base de datos, reglas del negocio y transporte pueden seguir siendo vulnerables, para el desarrollo de esta aplicación se ha empleado la metodología ágil de SCRUM que permite tener una alta participación de los involucrados en el proyecto.

### Beneficios Tangibles e Intangibles

Al implementar un sistema informático el principal resultado es el beneficio que adquiere el usuario, para el usuario estos beneficios pueden ser de dos tipos tangibles e intangibles, el usuario no es el único beneficiado del producto sino también las partes interesadas en el caso de la aplicación móvil no solo el usuario tendrá beneficios sino también la Escuela Superior Politécnica de Chimborazo y la Facultad en sí, como principales beneficios de la aplicación móvil tenemos los siguientes:

#### Beneficios tangibles

La Facultad de Administración de Empresas se beneficiará de diversas formas en cuanto a la auditoría de procesos, cumplimiento y acreditación, puesto que se brindará mayor productividad al permitir que los usuarios solo realicen las actividades necesarias, de modo que se incrementará el volumen de auditorías realizadas, ya que la aplicación móvil permite que el usuario se desplace dinámica y fácilmente entre las opciones, además un dispositivo móvil es mucho más atrayente para ser usado en el trabajo como la tendencia Bring Your Own Device BYOD.

#### Beneficios Intangibles

Las autoridades de la Facultas verán la mejoría en la toma de decisiones puesto que si requieren información de forma rápida y oportuna no se necesitará el ingresar a los sistemas web, ya que se elimina la necesidad de usan computador y el consumo de datos móviles es significativamente pequeño.

Los auditores verán de mejor manera su ambiente de trabajo, ya que dispondrán de un sistema no solo las 24 horas del día sino que, tendrán información actualizada, realizaran sus auditorías in situ de forma efectiva, podrán subir evidencia de forma digitalizada, lo que elimina el escaneado de la información luego del levantamiento de datos al tomar una fotografía del documento.

En base a los parámetros de la World Wide Web Consortium, la aplicación permite incrementar la accesibilidad de los dispositivos, puesto que no solo se abarca sistemas de escritorio sino que se ve beneficiado el indicador de la aplicación móvil, quizás más adelante se pueda incrementar sistemas de gestión en televisiones y automóviles, no obstante son tecnologías poco usadas en el país.

Al realizar una aplicación móvil con indicadores de seguridad aplicados, se permite incrementar la disponibilidad de la información desde el punto de vista de seguridad y confianza de los datos, de que sirve para la alta dirección la toma de decisiones si se tiene datos que no son confiables, el sistema perdería su credibilidad, en la aplicación móvil, se guarda una estricta cultura de seguridad informática.

Los beneficios de la aplicación móvil por ser un aplicativo del estudio investigativo tendrá su justificación en beneficios intangibles ya que se pretende aplicar seguridad a la información, por lo general la seguridad es incremental pero no posee una medición exacta del incremento sino se menciona que la aplicación es más segura, aunque por la simplicidad del manejo de la aplicación se puede decir que reduce los tiempos de realización de las auditorías de los sistemas, además la aplicación incrementa los criterios de accesibilidad y disponibilidad de la información, dadas las características y beneficios de la aplicación se recomienda su desarrollo e implementación.

### Especificación de Requerimientos

Un requerimiento para (Gómez, 2001) es “lo que debe hacer el sistema (sus funciones) y sus propiedades esenciales y deseables”, es decir que identifica todas las funciones que se deben realizar en el sistema para que su ejecución sea considerada como exitosa, estos requerimientos son definidos por los usuarios quienes detallan sus necesidades, esta especificación permite eliminar los malos entendidos en la etapa de desarrollo de software por lo que deben ser documentados.

Para definir los requerimientos de la aplicación móvil se han realizado 2 reuniones con los involucrados con la finalidad de cubrir las necesidades expuestas, los requerimientos pueden ser según (Sommerville, 2015) funcionales o no funcionales, los mismos que han sido identificados de la siguiente manera:

#### Requerimientos Funcionales

Los requerimientos funcionales especifican que debe realizar la aplicación al momento de ser implementada, estos se han identificado en las 2 reuniones con el usuario y se han detallado los requerimientos de los usuarios, del sistema de gestión de procesos que son características que han sido proporcionadas por el cliente, del mismo modo se han generado requerimientos del Balance Score Card y el Sistema de Gestión de Indicadores de Acreditación.

Para la realización de la aplicación se han identificado 29 requerimientos funcionales organizados en 5 categorías y han sido aprobados por los usuarios, los mismos permiten incorporar el uso de 3 sistemas informáticos en una sola aplicación, este detalle se encuentra como resultado en el Product Backlog en la Tabla 4 – 14.

#### Requerimientos No Funcionales

Los requerimientos no funcionales para Sommerville especifican las propiedades del software y se dividen en 3 categorías Requerimientos del Producto, Organizacionales y Externos, de estas 2 categorías la aplicación cumplirá los siguientes requerimientos:

* Requerimientos del Producto.- Los requerimientos que se especifican en esta categoría permiten cualificar la el comportamiento de la aplicación por lo tanto se definen requerimientos de fiabilidad y portabilidad por lo que la aplicación debe mantener la confidencialidad de la información sensible así como cumplir el criterio de la W3C de universalidad de dispositivos en el criterio de lugar.
* Requerimientos Organizacionales.- Estos requerimientos permiten alinear el producto en torno a las políticas que maneja la empresa solicitante, por lo tanto la aplicación móvil ha sido diseñada para cumplir las normativas de las aplicaciones dentro del Sistema de Gestión de Información.

Se ha identificado 2 requerimientos no funcionales para el desarrollo de la aplicación, de los cuales se han detallado características en base al producto y a la organización en este caso CIMOGSYS, lo cual permite realizar los procesos de auditoría a más de brindar al usuario confianza y seguridad.

Este conjunto de requerimientos, permitirá a la aplicación, satisfacer de mejor manera al usuario, evitará conflictos al momento de desarrollar el proyecto, con ello los mal entendido serán minimizados, se han registrado un total de 33 requerimientos divididos en 29 funcionales y 2 no funcionales, una vez finalizada la especificación de requerimientos el equipo tiene la base documental para iniciar el proceso de estimaciones.

### Estimación

La estimación del proyecto es una de las fases más importantes del desarrollo de software ya que permite identificar de manera inicial la cantidad de tiempo y recursos necesarios para la ejecución del proyecto, así también es un primer filtro de viabilidad, ya que si no se cuenta con el tiempo necesario el proyecto se declara no viable en lugar de ir hacia el fracaso.

De otra forma la estimación también nos permite buscar alternativas y soluciones para continuar con el desarrollo en caso de presentarse inconvenientes, para el proyecto de la aplicación móvil, se empleara una estimación a base de puntos de fusión, la misma que será calculada mediante el software USC-COCOMO II.2000.4.

Para realizar la estimación en base a puntos de fusión se necesita clasificar los requerimientos, identificarlos por su dificultad en una escala de alta, media y baja, para determinar el tiempo que se empleará en cada uno de ellos, los tipos de requerimientos existentes, son 29 requerimientos de entrada, salida y consulta.

De los 29 requerimientos, se han obtenido 4 entradas, 20 salidas, 5 consultas de las cuales existen 3 entradas con dificultad media y 1 baja, 16 salidas bajas y 4 medias, 3 consultas bajas, 1 media y 1 alta, la dificultad asignada a cada requerimientos ha sido identificada por el equipo de desarrollo en base a la experiencia en trabajos de desarrollo de software anteriores.

Los puntos de función junto al lenguaje de programación que se empleará permite obtener un estimado de líneas de código que es el factor que permite a COCOMO realizar su modelo matemático para estimar esfuerzo, costo y personal, se ingresan los valores de las entradas, salidas y consultas identificadas en el software teniendo la siguiente figura:

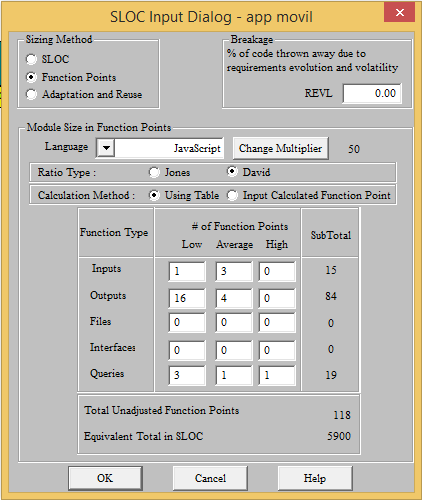


Figura 4‑2 Puntos de Función

Fuente: Realizado por Fausto C., Ángel S.

La Figura 4-2 muestra la configuración de los requerimientos de entrada, salida y de consultas con sus respectivas estimaciones de complejidad, se ha empleado un lenguaje JavaScript que permite procesar los datos, con un total 4 requerimientos de entrada, 20 salidas y 5 consultas haciendo un total de 118 puntos de función con un total de 5900 líneas de código, se ha empleado el método de la tabla de requerimientos así como Ratio Type David que permite el uso del lenguaje JavaScript para la estimación.

Así también por ser el primer proyecto móvil a realizar por el equipo de desarrollo, se han ajustados los factores de esfuerzo de COCOMO como se muestra en la siguiente tabla:

Tabla 4‑6 Factores de Esfuerzo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Categoría | Factor de Esfuerzo | Siglas | Base | Justificación |
| Atributos del producto de software | Fiabilidad Requerida de Software | RELY | HI | Puede producir perdidas económicas |
| Medida del volumen de Datos | DATA | VHI | 437000000/5900 = 74067,80 |
| Complejidad del Producto | CPLX | NOM | Normal |
| Reutilización Requerida | RUSE | VHI | A través de la línea de productos |
| Documentación Asociada a las Necesidades del Ciclo de Vida | DOCU | NOM | Normal |
| Atributos relacionados con la plataforma de desarrollo | Restricción del Tiempo de Ejecución | TIME | HI | 70 |
| Restricción del Almacenamiento Principal | STOR | NOM | Normal |
| Volatilidad de la Plataforma | PVOL | NOM | 6 meses |
| Atributos del personal involucrado en el proyecto | Habilidad del Analista | ACAP | NOM | Normal |
| Experiencia en Aplicaciones Similares | AEXP | VLO | Menos de 2 meses |
| Habilidad del Programador | PCAP | HI | Alta comunicación y cooperación |
| Experiencia en la Plataforma | PEXP | LO | Menos de 2 meses en apache cordova |
| Experiencia en la Herramienta y en el Lenguaje | LTEX | HI | 3 años en html 5, css3, javascript y netbeans |
| Continuidad del Personal | PCON | NOM | Personal continuo por año |
| Atributos propios del proyecto | Uso de Herramientas de Software | TOOL | NOM | Normal |
| Desarrollo Multilugar | SITE | NOM | Normal |
| Cronograma de Desarrollo Requerido | SCED | NOM |  |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

Los factores de esfuerzo de COCOMO vienen configuración con una valoración nominal, pero dadas las características del proyecto se han sido modificadas como muestra la Tabla 4-6, se han colocados valores en alto en cuanto a la Fiabilidad Requerida de Software, al Volumen de Datos y a la Complejidad del Producto por la investigación que se ha realizado y por la asistencia a la toma de decisiones que brinda la aplicación, dentro de los atributos del personal del proyecto de han puesto valores muy bajos y bajo a la experiencia del equipo en aplicaciones similares y a la experiencia de uso de la plataforma respectivamente, esto por ser el primer proyecto móvil a realizarse por el equipo de trabajo no obstante se ha colocado valores altos en la habilidad del programador así como en la experiencia en el manejo del lenguaje en este caso HTML 5, CSS 3 y JavaScript.

La modificación de los factores de esfuerzo permiten realizar un cambio en el modelo de estimación de COCOMO, puesto que a cada valoración de alta, normal y baja internamente posee un valor que modifica el Factor de Esfuerzo como se muestra en la siguiente tabla:

Tabla 4‑7 Valor de Factores de Esfuerzo

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Atributo | Abreviatura | Muy Bajo | Bajo | Normal | Alto | Muy Alto | Extra Alto |
| Producto | RELY | 0.82 | 0.92 | 1.00 | 1.10 | 1.26 | N/A |
| DATA | N/A | 0.9 | 1.00 | 1.14 | 1.28 | N/A |
| DOCU | 0.81 | 0.91 | 1.00 | 1.11 | 1.23 | N/A |
| CPLX | 0.73 | 0.87 | 1.00 | 1.17 | 1.33 | N/A |
| RUSE | N/A | 0.95 | 1.00 | 1.07 | 1.15 | 1.24 |
| Plataforma | TIME | N/A | N/A | 1.00 | 1.11 | 1.29 | 1.63 |
| STOR | N/A | N/A | 1.00 | 1.05 | 1.17 | 1.46 |
| PVOL | N/A | 0.87 | 1.00 | 1.15 | 1.30 | N/A |
| Personal | ACAP | 1.42 | 1.19 | 1.00 | 0.85 | 0.71 | N/A |
| APEX | 1.22 | 1.10 | 1.00 | 0.88 | 0.81 | N/A |
| PCAP | 1.34 | 1.15 | 1.00 | 0.88 | 0.76 | N/A |
| PLEX | 1.19 | 1.09 | 1.00 | 0.91 | 0.85 | N/A |
| LTEX | 1.20 | 1.09 | 1.00 | 0.91 | 0.84 | N/A |
| PCON | 1.29 | 1.12 | 1.00 | 0.90 | 0.81 | N/A |
| Proyecto | TOOL | 1.17 | 1.09 | 1.00 | 0.90 | 0.78 | N/A |
| SCED | 1.43 | 1.14 | 1.00 | 1.00 | 1.00 | N/A |
| STIE | 1.22 | 1.09 | 1.00 | 0.93 | 0.86 | 0.80 |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

Como muestra la Tabla 4-7, la modificación de cada atributo ya sea de Producto o de Proyecto implica una variación en el cálculo del Factor de Esfuerzo, así mismo se puede identificar que en una valoración Normal o Nominal todos los factores tienen la valoración de 1.00 mientras que sus valores tanto a la izquierda como la derecha son cambiantes, en los factores de Producto y Plataforma sus valores a la izquierda representan una disminución de su valor normal mientras que los valores a la derecha presentan un incremento.

Caso contrario sucede con los factores de Personal y Proyecto, un software estimado mediante COCOMO con todos sus atributos valorados en Normal el Factor de Esfuerzo no interfiere en el cálculo del modelo mientras que si se cambia su valoración, este valor afecta considerablemente el resultado, no obstante, es recomendable configurar estos parámetros puesto que los equipos que son implicados así como los productos a desarrollar no poseen las mismas características, como resultado de esta parametrización se obtiene el siguiente gráfico:

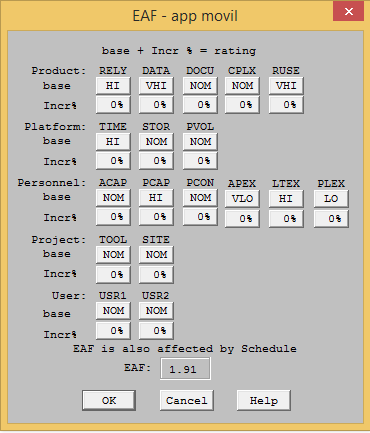


Figura 4‑3 Factor de Esfuerzo

Fuente: Realizado por Fausto C., Ángel S.

Como se puede observar en la Figura 4-3, se ha configurado en el modelo los atributos dando una valoración en base a la Tabla 1, la valoración de cada factor se ha estimado en base al manual de ayuda del Modelo de USC-COCOMO II.2000.4[[7]](#footnote-7), en el Atributo Producto se ha configurado 2 bases con valoración Normal, 2 muy alta y 1 alta, en Plataforma se obtienen 2 bases normales, 1 alta, en Personal son 1 base muy baja, 1 baja, 2 normales y 2 altas, finalmente en Proyecto son dos bases normales, no se ha configurado el Atributo Usuario, esta parametrización ha permitido obtener un Factor de Esfuerzo “EAF” de 1.91, el mismo que se empleará en el modelo de COCOMO.

Para finalizar la configuración del software COCOMO se han configurado los Factores de Escala en el Diseño Post Architecture, este diseño permite la mejor configuración del modelo ya que usa los 17 factores de esfuerzo anteriormente configurados, este modelo permite configurar los parámetros en base al conocimiento existente en cuando al equipo, al mantenimiento y al ciclo de vida del desarrollo de software, para configurar los Factores de Escala se ha empleado la siguiente parametrización:

Tabla 4‑8 Factores de Escala

|  |  |  |  |
| --- | --- | --- | --- |
| FACTORES DE ESCALA | ABREVIATURA | VALOR | JUSTIFICACIÓN |
| Precedentes | PREC | LO | Poca experiencia con el cliente y en la herramienta. |
| Flexibilidad en Desarrollo | FLEX | LO | Existe premura en el desarrollo de la aplicación. |
| Arquitectura / Riesgo | RESL | NOM | Valor de riesgo predefinido. |
| Cohesión del Equipo | TREAM | LO | El equipo de desarrollo no tiene la misma perspectiva del producto, y es difícil acoplar todos los objetivos de los involucrados. |
| Madurez de los Procesos | PMAT | NOM | Madurez de los procesos normal. |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

Como se puede evidenciar en la Tabla 4-8 se han configurado los factores de escala en la estimación lo que nos permite identificar el ambiente en el proyecto, los precedentes son bajos, ya que es la segunda vez en la que el equipo de desarrollo trabaja con el cliente, así como la primera vez en el uso del framework Apache Cordova, la Flexibilidad del desarrollo es baja puesto que primero se tiene premura en que el producto sea terminado, integra 3 aplicaciones web y finalmente los requerimientos han sido obtenidos del uso de los 3 sistemas, de procesos, balance score Card y acreditación, se mantiene el valor de nominal y madurez de procesos, finalmente la cohesión del equipo es baja, puesto que existen desarrolladores, diseñadores y administradores como interesados, esto se debe a que es complicado para el equipo acoplar todos los objetivos de los miembros, se ha estimado estos valores en base a la dirección del manual técnico de COCOMO y al configurar en el software se ha obtenido el siguiente gráfico:

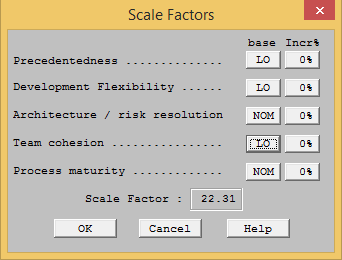


Figura 4‑4 Factores de Escala

Fuente: Realizado por Fausto C., Ángel S.

Como se puede observar en la Figura 4-4, se han configurado en los Factores de Esfuerzo 3 bases con valoración baja, y dos con configuración normal que nos permite obtener un Factor de Escala general de 22.31, con esta configuración se ha finalizado la parametrización del modelo en COCOMO.

Una vez asignados los valores para estimar las líneas de código a base de puntos de función, se han modificado los factores de esfuerzo y se han configurado los factores de escala, se obtiene la siguiente figura que resume y genera la estimación del software COCOMO como se puede apreciar en el Manual Técnico p13 Figura 4 ,los valores del resultado de la estimación del software COCOMO, se ha estimado un total de 5900 líneas de código, un salario de 354 dólares americanos a los integrantes del equipo, un factor de esfuerzo de 1.91 y un riesgo calculado por el modelo de 3.6, COCOMO permite observar 3 tipos de estimación que son: Optimista, Realista y Pesimista.

Para Bednar y Robertson[[8]](#footnote-8) la estimación optimista es el mejor escenario para el proyecto, el realista es el escenario más confiable para el proyecto mientras que el pesimista es el peor escenario, en cuanto a tiempo, dinero y personal, para este proyecto se empleará el modelo de estimación realista del cual se puede obtiene los siguientes valores, esfuerzo 42.0 personas por mes, duración de 12.4 meses, productividad de 140 líneas de código por persona mes, costo de 14884.59 dólares americanos y un equipo de 3.4 personas, sin embargo el equipo es de 2 personas por lo que se recomienda replantear la estimación.

En COCOMO la fórmula para estimar las personas necesarias en el equipo es:

Donde, al despejar el tiempo de desarrollo, conociendo las personas reales en el equipo, tenemos:

Donde el esfuerzo es constante y las personas que integran el equipo son 2, por lo tanto:

Finalmente la estimación más próxima a la real tiene los siguientes datos: esfuerzo de 42.0 personas/mes, tiempo de desarrollo de 21 meses, productividad de 140,3 líneas de código por mes con un equipo de dos personas y un costo de 14884.59 dólares, con este resultado se sugiere que se continúe con los estudios de factibilidad.

De lo planificado a lo realizado en realidad se ha identificado que existe una variación considerable en cuanto a tiempo de desarrollo de software, la estimación realizada por el equipo cuenta con 21 meses de tiempo estimado no obstante la aplicación ha sido realizada en 3 meses, plazo que es mucho menor por lo que existe un problema en la estimación del producto, pese a ser los factores de esfuerzo ajustados de la mejor manera no se ha acercado a la realidad, se han estimado además 5900 líneas de código, mientras que el proyecto real se han realizado 15 526 líneas de código reales, esto se puede dar por la arquitectura de la aplicación móvil que conlleva 3 lenguajes sin embargo se ha estimado en uno solo que es JavaScript, del mismo que han sido solo 4200 líneas de código.

Estos errores de estimación de tiempo, se deben a que básicamente el desarrollo de software en la Escuela Superior Politécnica de Chimborazo, no se realizan los procesos adecuados de desarrollo, se omiten procedimientos como pruebas de desarrollo, pruebas de ejecución así como de mantenimiento que producen información de fallos del software, a más de ello las prisas por la entrega del producto impide que los desarrolladores realicen procesos de refactorización de código que es sumamente importante, pero aún más sensible no se realiza la verificación de las políticas de seguridad como pruebas de usabilidad y accesibilidad parametrizada, no se siguen de manera formal los estándares y los requerimientos son muy cambiantes por lo que se recomienda de manera especial que se haga un estudio del modelo COCOMO para que pueda ser aplicado en las estimaciones de software de la Escuela Superior Politécnica de Chimborazo.

### Estudio de Factibilidad

El estudio de Factibilidad permite a CIMOGSYS medir los recursos necesarios para la realización de la aplicación móvil, estos recursos pueden existir como no, permite determinar el personal necesario y estimar el monto de la inversión, para el centro este estudio permitirá definir la viabilidad del proyecto por lo que se han realizado los estudios de factibilidad operativa, técnica y económica.

#### Factibilidad Técnica

El estudio técnico permite analizar si el centro CIMOGSYS posee el hardware (servidores, computadores), software (herramientas de desarrollo, licencias de software) y personal necesario para la realización del proyecto, para desarrollar la aplicación móvil se han definido los siguientes recursos:

Tabla 4‑9 Hardware Requerido

|  |  |  |
| --- | --- | --- |
| CANTIDAD | DESCRIPCIÓN | OBSERVACIONES |
| 1 | Servidor Web | Servidor que alojará los servicios web de la aplicación móvil del SGI. |
| 2 | Computadores | Equipos empleados para el desarrollo de la aplicación. |
| 2 | Dispositivo Móvil | Dispositivos Android y iOS para realización de pruebas. |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

El hardware requerido en la Tabla 4-9 es un descriptivo del equipo mínimo que se necesita para el desarrollo e implementación de la aplicación móvil, donde es imprescindible un servidor web donde se alojarán los datos de la aplicación y los servicios web que consumirá la aplicación, dos computadores para el desarrollo de la aplicación, ventajosamente CIMOGSYS cuenta con un servidor web propio, los computadores para el desarrollo del software se sustituirán por los computadores del equipo de desarrollo son necesarias dos unidades para que se pueda compilar el código fuente generado en los sistemas operativos Windows para Android y OS X para iOS de igual forma son necesarios dos dispositivos móviles de pruebas en los sistemas operativos móviles mencionados.

Al realizar la revisión del hardware se determina que es factible el desarrollo del proyecto ya que se cuenta con los equipos necesarios y si no existieren son reemplazados por computadores o dispositivos del equipo de desarrollo.

Tabla 4‑10 Software Requerido

|  |  |  |
| --- | --- | --- |
| NOMBRE | DESCRIPCIÓN | LICENCIA |
| Netbeans IDE | IDE de desarrollo con soporte HTML 5, CSS 3, Javascript y PHP | GPLv2 |
| Apache Cordova | Marco de desarrollo para aplicaciones móviles híbridas multiplataforma. | GNU |
| FileZilla | Cliente FTP | GNU |
| Firefox | Navegador web para pruebas de aplicaciones web responsivas. | Creative Commons |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

El software requerido en la Tabla 4-10 son herramientas que permitirán el desarrollo de la aplicación, Netbeans permite desarrollar los servicios web de conexión sobre Laravel, así también permite crear las interfaces móviles con HTML5, CSS3 y JavaScript que son los lenguajes de maquetación y programación, FileZilla es un cliente FTP con el que se cargarán en el servidor web los archivos de servicios ya en funcionamiento para pruebas y producción, Firefox permite realizar pruebas de visualización de interfaces antes de compilar el proyecto; todas las herramientas poseen licencias libres con lo que se encuentran disponibles para los desarrolladores permitiendo así la factibilidad de software.

Tabla 4‑11 Personal Técnico Requerido

|  |  |  |
| --- | --- | --- |
| FORMACIÓN | FUNCIÓN | EXPERIENCIA |
| Ingeniero en Sistemas Informáticos | Scrum Master | Conocimiento y manejo de metodologías de desarrollo de software, facilidad para trabajar con grupos de personas, experiencia en dirección de proyectos de software. |
| Ingeniero en Sistemas Informáticos | Desarrollador | Desarrollo de aplicaciones web, aplicaciones híbridas, manejo del software Apache Córdova, conocimiento del lenguaje PHP para desarrollo de servicios web, conocimiento de seguridades móviles. |
| Ingeniero en Diseño Gráfico | Diseñador | Desarrollo y maquetación de interfaces según la metodología primero móvil. |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

En el personal requerido en la Tabla 4-11 para el proyecto son necesarios 1 Scrum Master que dirija la realización del proyecto y su metodología, 1 diseñador gráfico que genere las interfaces que usará la aplicación enmarcada en los lineamientos de imagen del centro y la facultad, 2 desarrolladores para la realización de interfaces y servicios clientes así como las pruebas de seguridad necesarias para incrementar la disponibilidad de la información. En el centro no existen profesionales formados como Ingenieros en Sistemas Informáticos es por esto que el equipo de desarrollo conformado por los estudiantes Fausto Cevallos y Javier Sigüenza (tesistas) de la Facultad de Informática y Electrónica han sido designados para la creación de la aplicación móvil además cumplen con los requisitos de experiencia detallados.

Al analizar el personal requerido se ha identificado que existen las personas con la formación requerida como Scrum Master el Ing. Jorge Menéndez, como diseñadora gráfica la Srta. Erika Razo practicante de diseño gráfico del centro y como desarrolladores Fausto Cevallos y Javier Sigüenza tesistas, por lo que existe la factibilidad de personal requerido.

Una vez realizado el análisis del software, hardware y personal técnico requerido se contempla que todos los requerimientos ya existen o pueden ser adquiridos sin ninguna dificultad por lo que se declara factible técnicamente la realización del proyecto.

#### Factibilidad Económica

En una empresa el costo de un proyecto de software es fundamental, el estudio económico permite conocer la cantidad de inversión necesaria para el desarrollo y mantenimiento del software por lo que al realizar una análisis CIMOGSYS emitirá si puede asumir o no los costos de creación de la aplicación y declarar la viabilidad económica, para el estudio económico se abarcan áreas como personal, software, hardware y recurso operativo.

Tabla 4‑12 Factibilidad Económica

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Descripción | Tipo de Costo | Cantidad | Costo Unitario | Tiempo  (meses) | Costo Total |
| Scrum Master | Costos de Desarrollo | 1 | 1200 | 2 | 2400 |
| Diseñador Gráfico | 1 | 500 | 2 | 500 |
| Servicio de Internet | 1 | 27,90 | 21 | 585.9 |
| Aplicación Móvil | 1 | 14884.59 |  | 14884.59 |
| Total |  | | | | 18370.49 |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

Se han determinado los costos necesarios según el detalle de la Tabla 4-12 para el desarrollo de la aplicación que consisten en costos de personal y de servicio de internet, costos que suman 18370.49 dólares americanos, el Scrum Master es contratado ocasionalmente durante un periodo total de dos mes, los desarrolladores son contratados durante todo el proyecto gastas incluidos en el costo de aplicación móvil estimado por COCOMO, la diseñadora gráfica es contratada en la fase inicial del proyecto durante dos mes, los costos son asumidos por cada miembro del equipo por lo que se declara factible económicamente el proyecto.

#### Factibilidad Operativa

El estudio operativo permite definir las personas que estarán a cargo de la aplicación móvil quienes administrarán contenidos, emitirán reportes, y verificarán el funcionamiento correcto del proyecto; para todas estas funciones se ha designado al personal técnico existente en la Facultad de Administración de Empresas donde se implementará el proyecto, al mismo que se le brindará una capacitación sobre la aplicación, con este análisis la facultad cuenta con el personal operativo para el funcionamiento del proyecto por lo que se declara una factibilidad operativa.

Una vez analizada la factibilidad técnica, económica y operativa se ha determinado que en cada una de ellas el proyecto es factible y puede realizarse ya que se posee o se pueden gestionar las herramientas, infraestructura, software y equipos, el costo del personal es asumido por el equipo de desarrollo y existe el personal operativo para administrar la aplicación por lo que se declara que el proyecto se puede realizar y se procede al desarrollo del software mediante la metodología SCRUM.

### Personas y Roles

Se ha tomado en cuenta los equipos interdisciplinarios que se han reunido para la realización del proyecto quedando el equipo de trabajo conformado de la siguiente manera:

Tabla 4‑13 Integrantes y Roles del Proyecto

|  |  |  |
| --- | --- | --- |
| Integrantes | Rol | Contacto |
| Jorge Menéndez | Scrum Master | Email: [jmenendez@espoch.edu.ec](mailto:jmenendez@espoch.edu.ec) |
| ESPOCH | Product Owner | Teléfono: (03) 2 998-200 |
| Erika Razo | Diseñadora Gráfica | Teléfono: 0995632054 |
| Javier Sigüenza | Desarrollador | Email: [javier.siguenza@live.com](mailto:javier.siguenza@live.com),  Teléfono: 0987115420 |
| Fausto Cevallos | Desarrollador | Email: [fausto\_cevallos@cimogsys.com](mailto:fausto_cevallos@cimogsys.com),  Teléfono: 0979076215 |
| Giovanny Alarcón | Cliente | Email: [giovanny\_alarcon@cimogsys.com](mailto:giovanny_alarcon@cimogsys.com),  Teléfono: 0999046921 |

Fuente: Trabajo de Investigación

Realizado por: Fausto Cevallos, Javier Sigüenza

Los integrantes y roles del proyecto detallados en la Tabla 4-13, han sido identificados en base a la metodología SCRUM siendo un total de 6 personas, Product Owner es quien aporta con el financiamiento del producto en este caso se ve representado en el del Rector de la ESPOCH, el cliente emitirá los requerimientos que debe cumplir la aplicación móvil, la diseñadora gráfica para la creación de las interfaces, puesto que en el centro de investigación se maneja un criterio de identidad corporativa, los desarrolladores quienes realizarán la aplicación y el Scrum Master quien asegura el cumplimiento de la metodología, se encarga de la realización de las reuniones de trabajo y solucionar los problemas que se presentaren en el transcurso del proyecto.

### Planificación

La planificación de las actividades a realizar es una de las etapas más importantes en un proyecto informático, según la metodología SCRUM se deben definir dos productos de la planificación el Product Backlog y el Sprint Backlog, el primero es un listado de historias de usuario a realizar priorizadas en nivel de importancia para el usuario y el Sprint Backlog es la planificación de cuantas historias de usuario serán realizadas por iteración, para realizar estos productos se necesita emplear un método de estimación que para el proyecto se empleará el método de las tallas de la camiseta.

Las tallas de la camiseta ejemplifican la vida real por lo que su medición será basada en las letras: S, M, L, XL cada talla significará una duración en el tamaño del sprint o una fracción de este, para estimar la duración de un sprint se empleará la talla L que son 20 puntos estimados de trabajo realizados en una semana, cada punto estimado se medirá en 2 horas de trabajo, de tal manera que la talla M significarán 10 puntos estimados, la talla S significarán 5 puntos estimados y la talla XL significará 40 puntos estimados, de esta manera será mucho más fácil realizar la estimación de duración del proyecto.

Con la finalidad de incorporar las buenas prácticas de seguridad en el desarrollo de la aplicación móvil se recomienda en esta etapa definir la persona que será responsable de la seguridad de la aplicación, la misma que definirá los objetivos de seguridad junto a las prácticas que se implementarán de igual forma definirá cuales son los recursos necesarios para las pruebas, por lo que se propone la creación de una historia técnica que contenga estas necesidades y se adjunte al Product Backlog.

Para definir el Product Backlog se empleará la especificación de requerimientos realizada, estos requerimientos serán transformados a historias de usuario, serán priorizados y se realizará una estimación de su duración, no obstante la aplicación no solo consta de las historias de usuario sino que también posee historias técnicas del sistema como el estándar de codificación, el diseño de la arquitectura de la aplicación entre otras todas estas historias de usuario e historias técnicas han sido organizadas y priorizadas de la siguiente manera:

Tabla 4‑14 Product Backlog

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Historia de Usuario | Prioridad | Estimación |
| HT1 | Como desarrollador, necesito establecer la arquitectura del sistema, con la finalidad de iniciar el desarrollo de la aplicación. | Alta | 5 |
| HT2 | Como desarrollador, necesito establecer el estándar de codificación a emplearse, con la finalidad de obtener un código uniforme a través de un documento guía. | Alta | 5 |
| HT3 | Como desarrollador, necesito que se especifique el estándar de interfaces junto a la diseñadora, con la finalidad de cumplir con el estándar gráfico de CIMOGSYS. | Alta | 10 |
| HT4 | Como responsable de seguridad, necesito que se especifiquen los objetivos de seguridad, con la finalidad de asegurar la aplicación desde su desarrollo | Alta | 20 |
| HU1 | Como usuario, necesito que se despliegue el Mapa de Procesos de la Facultad, con la finalidad de visualizar los Macroprocesos, Procesos existentes y su semaforización. | Alta | 40 |
| HU2 | Como usuario, necesito que se despliegue el Mapa Estratégico de la Facultad, con la finalidad de visualizar las perspectivas, objetivos, proyectos existentes y su semaforización. | Alta | 40 |
| HU3 | Como usuario, necesito que se despliegue el Mapa de Entorno de Aprendizaje de la Facultad, con la finalidad de visualizar los criterios, subcriterios, indicadores y variables de la Facultad y su semaforización | Alta | 40 |
| HU4 | Como auditor, necesito evaluar los procesos de la Facultad, con la finalidad de realizar la auditoría de procesos. | Alta | 10 |
| HU5 | Como auditor, necesito evaluar los procesos de la Escuela de Contabilidad y Auditoría, con la finalidad de realizar la auditoría de procesos. | Alta | 10 |
| HU6 | Como auditor, necesito evaluar los procesos de la Escuela de Empresas, con la finalidad de realizar la auditoría de procesos. | Alta | 10 |
| HU7 | Como usuario, necesito evaluar los procesos de la Escuela de Gestión de Transporte, con la finalidad de realizar la Auditoría de procesos. | Alta | 10 |
| HU8 | Como auditor, necesito evaluar los procesos de la Escuela de Marketing, con la finalidad de realizar la auditoría de procesos. | Alta | 10 |
| HU9 | Como auditor, necesito evaluar los procesos de la Escuela de Finanzas, con la finalidad de realizar la auditoría de procesos. | Alta | 10 |
| HU10 | Como auditor, necesito evaluar los procesos de la Escuela de Comercio Exterior, con la finalidad de realizar la auditoría de procesos. | Alta | 10 |
| HU11 | Como auditor, necesito evaluar los procesos de la Escuela de Ingeniería Comercial, con la Finalidad de Realizar la auditoría de procesos. | Alta | 10 |
| HU12 | Como auditor, necesito evaluar las perspectivas de la Facultad, con la finalidad de realizar la auditoría de cumplimiento. | Alta | 10 |
| HU13 | Como auditor, necesito evaluar las perspectivas de la Escuela de Contabilidad y Auditoría, con la finalidad de realizar la auditoría de cumplimiento. | Alta | 10 |
| HU14 | Como auditor, necesito evaluar las perspectivas de la Escuela de Empresas, con la finalidad de realizar la auditoría de planificación. | Alta | 10 |
| HU15 | Como auditor, necesito evaluar las perspectivas de la Escuela de Gestión de Transporte, con la finalidad de realizar la auditoría de planificación. | Alta | 10 |
| HU16 | Como auditor, necesito evaluar las perspectivas de la Escuela de Marketing, con la finalidad de realizar la auditoría de planificación. | Alta | 10 |
| HU17 | Como auditor, necesito evaluar las perspectivas de la Escuela de Finanzas, con la finalidad de realizar la auditoría de planificación, | Alta | 10 |
| HU18 | Como auditor, necesito evaluar las perspectivas de la Escuela de Comercio Exterior, con la finalidad de realizar la auditoría de planificación. | Alta | 10 |
| HU19 | Como auditor, necesito evaluar las perspectivas de la Escuela de Ingeniería Comercial, con la Finalidad de Realizar la auditoría de planificación. | Alta | 10 |
| HU20 | Como auditor, necesito evaluar los criterios de la Escuela de Contabilidad y Auditoría, con la finalidad de realizar la auditoría de acreditación. | Alta | 10 |
| HU21 | Como auditor, necesito evaluar los criterios de la Escuela de Empresas, con la finalidad de realizar la auditoría de acreditación. | Alta | 10 |
| HU22 | Como auditor, necesito evaluar los criterios de la Escuela de Gestión de Transporte, con la finalidad de realizar la auditoría de acreditación. | Alta | 10 |
| HU23 | Como auditor, necesito evaluar los criterios de la Escuela de Marketing, con la finalidad de realizar la auditoría de acreditación. | Alta | 10 |
| HU24 | Como auditor, necesito evaluar los criterios de la Escuela de Finanzas, con la finalidad de realizar la auditoría de acreditación, | Alta | 10 |
| HU25 | Como auditor, necesito evaluar los criterios de la Escuela de Comercio Exterior, con la finalidad de realizar la auditoría de acreditación. | Alta | 10 |
| HU26 | Como auditor, necesito evaluar los criterios de la Escuela de Ingeniería Comercial, con la Finalidad de Realizar la auditoría de acreditación. | Alta | 10 |
| HU27 | Como usuario, necesito visualizar los contenidos de la página de Misión y Visión, con la finalidad de informar a los usuarios | Baja | 5 |
| HU28 | Como usuario, necesito visualizar los contenidos de la página de Objetivos de Calidad, con la finalidad de informar a los usuarios | Baja | 5 |
| HU29 | Como usuario, necesito visualizar los contenidos de la página de Compromisos, con la finalidad de informar a los usuarios | Baja | 5 |
| HU30 | Como usuario, necesito visualizar los contenidos de la página de Mensaje de la Comisión, con la finalidad de informar a los usuarios | Baja | 5 |
| HU31 | Como usuario, necesito visualizar los contenidos de la página de Contactos de Redes Sociales, con la finalidad de informar a los usuarios | Baja | 5 |
| HU32 | Como usuario, necesito visualizar los contenidos de la página de Descargas, con la finalidad de informar a los usuarios | Baja | 10 |
| HU33 | Como docente, necesito visualizar los contenidos de la página de Gestión Docente, con la finalidad de informar a los usuarios | Baja | 10 |
| HU34 | Como usuario, necesito visualizar los contenidos de la página de Inicio, con la finalidad de informar a los usuarios. | Baja | 5 |
| HT5 | Como desarrollador, necesito que se realice el manual técnico, con la finalidad de registrar como está realizada la aplicación. | Baja | 20 |
| HT6 | Como usuario, necesito que se realice el manual de usuario, con la finalidad de conocer cómo funciona la aplicación. | Baja | 20 |

Fuente: Especificación de Requerimientos de Software

Realizado por: Fausto Cevallos, Javier Sigüenza

Como se puede apreciar en la Tabla 4-14 las Historias de Usuario así como las historias técnicas del sistema se han organizado por su nivel de prioridad así como se les ha asignado una estimación en base al método de la talla de la camiseta, se han organizado 34 Historias de Usuario las cuales están identificadas por un código que consiste de la letra “H” más un número de la siguiente manera H1, también se han organizado 6 Historias Técnicas y su codificación se rige a las letras “HT” más un número por ejemplo HT1, en total se tienen 4 historias técnicas con prioridad alta y 2 con prioridad baja asignadas por los desarrolladores, se tienen 8 historias de usuario de prioridad baja y 26 historias de prioridad alta, prioridad que ha sido asignada por el cliente.

Estas historias de usuario que nos permiten administrar los requerimientos del usuario deben ser planificadas en las distintas iteraciones como fruto de esta planificación realizada se obtiene el siguiente Sprint Backlog:

Tabla 4‑15 Sprint Backlog

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ACTIVIDADES DEL PROYECTO | Esfuerzo | INICIO | FIN | RESPONSABLE |
| Aplicación Móvil SGI | **480** | **01/10/15** | **23/12/15** |  |
| Sprint 1 | **20** | **01/10/15** | **07/10/15** |  |
| HT1 Diseño de la Arquitectura del Sistema | 5 | 01/10/15 | 01/10/15 | Javier Sigüenza |
| HT2 Diseño del Estándar de Codificación | 5 | 02/10/15 | 02/10/15 | Javier Sigüenza |
| HT3 Diseño del Estándar de Interfaces | 10 | 05/10/15 | 07/10/15 | Javier Sigüenza |
| HT4 Especificación de Objetivos de Seguridad | 20 | 01/10/15 | 07/10/15 | Fausto Cevallos |
| Sprint 2 | **20** | **08/10/15** | **14/10/15** |  |
| HU1.1 Despliegue de Mapas de Procesos Facultad | 20 | 08/10/15 | 14/10/15 | Javier Sigüenza |
| HU1.2 Despliegue de Mapas Estratégicos Facultad | 20 | 08/10/15 | 14/10/15 | Fausto Cevallos |
| Sprint 3 | **20** | **15/10/15** | **21/10/15** |  |
| HU2.1 Despliegue de Mapas de Procesos Escuelas | 20 | 15/10/15 | 21/10/15 | Javier Sigüenza |
| HU2.2 Despliegue del Mapa Estratégicos Escuelas | 20 | 15/10/15 | 21/10/15 | Fausto Cevallos |
| Sprint 4 | **20** | **22/10/15** | **28/10/15** |  |
| HU3.1 Despliegue de Mapas de Entorno de Aprendizaje Facultad | 20 | 22/10/15 | 28/10/15 | Javier Sigüenza |
| HU4 Auditoría de Procesos de la Facultad | 10 | 22/10/15 | 26/10/15 | Fausto Cevallos |
| HU5 Auditoría de Procesos de la Escuela de Contabilidad y Auditoría | 10 | 27/10/15 | 28/10/15 | Fausto Cevallos |
| Sprint 5 | **20** | **29/10/15** | **04/11/15** |  |
| HU3.2 Despliegue de Mapas de Entorno de Aprendizaje Escuelas | 20 | 29/10/15 | 04/11/15 | Javier Sigüenza |
| HU6 Auditoría de Procesos de la Escuela de Empresas | 10 | 29/10/15 | 02/11/15 | Fausto Cevallos |
| HU7 Auditoría de Procesos de la Escuela de Gestión de Transporte | 10 | 03/11/15 | 04/11/15 | Fausto Cevallos |
| Sprint 6 | **20** | **05/11/15** | **11/11/15** |  |
| HU8 Auditoría de Procesos de la Escuela de Marketing | 10 | 05/11/15 | 09/11/15 | Javier Sigüenza |
| HU9 Auditoría de Procesos de la Escuela de Finanzas | 10 | 10/11/15 | 11/11/15 | Javier Sigüenza |
| HU10 Auditoría de Procesos de la Escuela de Comercio Exterior | 10 | 05/11/15 | 09/11/15 | Fausto Cevallos |
| HU11 Auditoría de Procesos de la Escuela de Ingeniería Comercial | 10 | 10/11/15 | 11/11/15 | Fausto Cevallos |
| Sprint 7 | **20** | **12/11/15** | **18/11/15** |  |
| HU12 Auditoría de Planificación de la Facultad | 10 | 12/11/15 | 16/11/15 | Javier Sigüenza |
| HU13 Auditoría de Planificación de la Escuela de Contabilidad y Auditoría | 10 | 17/11/15 | 18/11/15 | Javier Sigüenza |
| HU14 Auditoría de Planificación de la Escuela de Empresas | 10 | 12/11/15 | 16/11/15 | Fausto Cevallos |
| HU15 Auditoría de Planificación de la Escuela de Gestión de Transporte | 10 | 17/11/15 | 18/11/15 | Fausto Cevallos |
| Sprint 8 | **20** | **19/11/15** | **25/11/15** |  |
| HU16 Auditoría de Planificación de la Escuela de Marketing | 10 | 19/11/15 | 23/11/15 | Javier Sigüenza |
| HU17 Auditoría de Planificación de la Escuela de Finanzas | 10 | 24/11/15 | 25/11/15 | Javier Sigüenza |
| HU18 Auditoría de Planificación de la Escuela de Comercio Exterior | 10 | 19/11/15 | 20/11/15 | Fausto Cevallos |
| HU19 Auditoría de Planificación de la Escuela de Ingeniería Comercial | 10 | 23/11/15 | 25/11/15 | Fausto Cevallos |
| Sprint 9 | **20** | **26/11/15** | **02/12/15** |  |
| HU20 Auditoría de Acreditación de la Escuela de Contabilidad y Auditoría | 10 | 26/11/15 | 30/11/15 | Javier Sigüenza |
| HU21 Auditoría de Acreditación de la Escuela de Empresas | 10 | 01/12/15 | 02/12/15 | Javier Sigüenza |
| HU22 Auditoría de Acreditación de la Escuela de Gestión de Transporte | 10 | 26/11/15 | 30/11/15 | Fausto Cevallos |
| HU23 Auditoría de Acreditación de la Escuela de Marketing | 10 | 01/12/15 | 02/12/15 | Fausto Cevallos |
| Sprint 10 | **20** | **03/12/15** | **09/12/15** |  |
| HU24 Auditoría de Acreditación de la Escuela de Finanzas | 10 | 03/12/15 | 07/12/15 | Javier Sigüenza |
| HU25 Auditoría de Acreditación de la Escuela de Comercio Exterior | 10 | 08/12/15 | 09/12/15 | Javier Sigüenza |
| HU26 Auditoría de Acreditación de la Escuela de Ingeniería Comercial | 10 | 03/12/15 | 07/12/15 | Fausto Cevallos |
| HU27 Desarrollar Página de Misión y Visión | 5 | 08/12/15 | 08/12/15 | Fausto Cevallos |
| HU28 Desarrollar Página de Objetivos de Calidad | 5 | 09/12/15 | 09/12/15 | Fausto Cevallos |
| Sprint 11 | **20** | **10/12/15** | **16/12/15** |  |
| HU29 Desarrollar Página de Compromisos | 5 | 10/12/15 | 10/12/15 | Javier Sigüenza |
| HU30 Desarrollar Página de Mensaje de la Comisión | 5 | 11/12/15 | 11/12/15 | Javier Sigüenza |
| HU31 Desarrollar Página de Descargas | 10 | 14/12/15 | 16/12/15 | Javier Sigüenza |
| HU32 Desarrollar Página de Inicio | 5 | 10/12/15 | 10/12/15 | Fausto Cevallos |
| HU33 Desarrollar Página de Contactos | 5 | 11/12/15 | 11/12/15 | Fausto Cevallos |
| HU34 Desarrollar Página de Gestión Docente | 10 | 14/12/15 | 16/12/15 | Fausto Cevallos |
| Sprint 12 | **20** | **17/12/15** | **23/12/15** |  |
| HT5 Realización de Manual Técnico | 20 | 17/12/15 | 23/12/15 | Javier Sigüenza |
| HT6 Realización de Manual de Usuario | 20 | 17/12/15 | 23/12/15 | Fausto Cevallos |

Fuente: Especificación de Requerimientos de Software

Realizado por: Fausto Cevallos, Javier Sigüenza

En la Tabla 4-15 se puede apreciar cómo han sido organizadas las historias en 12 Sprints los mismos que tienen una duración de 5 días o el equivalente a la Talla L de la camiseta con una estimación de 20 puntos, a cada historia de usuario se le ha asignado un nombre (Consta en cada actividad a realizarse), una fecha de inicio y una fecha de culminación de la Historia así como un responsable de su realización, el equipo de desarrollo está conformado de dos personas, una vez planificadas las historias se procede al desarrollo de la aplicación móvil.

### Desarrollo de la aplicación

El desarrollo de la planificación o del proyecto no es más que la ejecución de la metodología SCRUM, es decir, la implementación de todas y cada una de las historias de usuario priorizadas en el Product Backlog y organizadas por Sprints, cada historia se usuario termina su ejecución con las pruebas de aceptación donde valida el software o la terea realizada.

#### Sprint 1

Para la ejecución del primer sprint se ha realizado una reunión de inicio con los miembros del proyecto donde se han organizado las historias técnicas, si bien es cierto no representan en sí una funcionalidad, son sumamente necesarias para su implementación, las historias técnicas seleccionadas han sido: diseño de la arquitectura del sistema, diseño del estándar de codificación, diseño del estándar de interfaces, especificación de los objetivos de seguridad que son la parte fundamental para la aplicación de buenas prácticas de seguridad, a continuación se detalla la realización de cada una de las historias técnicas:

##### Diseño de la Arquitectura del Sistema

Tabla 4‑16 Historia Técnica

|  |  |
| --- | --- |
| HISTORIA TÉCNICA | |
| Número: HT1 | **Nombre de la Historia Técnica:** Diseño de la Arquitectura del Sistema. |
| Usuario: Desarrollador | **Sprint Asignado:** 1 |
| Puntos Estimados: 5 | **Puntos Reales:** 5 |
| Descripción: Como desarrollador, necesito establecer la arquitectura del sistema, con la finalidad de iniciar el desarrollo de la aplicación. | |
| Pruebas de Aceptación:   * Verificar que los componentes de la arquitectura permitan el correcto desarrollo de las funcionalidades de la aplicación. | |

Elaboración: Fausto Cevallos, Javier Sigüenza

Como muestra la Tabla 4-16, todas las historias técnicas han sido realizadas en base a este formato de tarjeta, donde se involucra el nombre de la tarjeta, su identificación con número y nombre, así también se designa el usuario que la ha solicitado y el sprint asignado, que es el orden en que se realizará su resolución, se genera la documentación de puntos estimados y los reales empleados, se realiza una breve descripción de la tarjeta y se suman las pruebas de aceptación, las que permitirán identificar si se ha realizado de forma exitosa o no.

Tabla 4‑17 Tarea de Ingeniería

|  |  |
| --- | --- |
| TAREA DE INGENIERÍA | |
| Sprint: 1 | **Número de Tarea:** TI\_HT1\_1 |
| Nombre de la Historia: Diseño de la Arquitectura del Sistema | |
| Nombre de la Tarea: Determinar el diseño que adoptará el sistema para la aplicación móvil | |
| Responsable: Javier Sigüenza | **Tipo de Tarea:** Desarrollo |
| Fecha Inicio: 1/10/2015 | **Fecha Fin:** 1/10/2015 |
| Descripción: Se debe realizar la distribución de los componentes que tendrá el sistema los mismos que deben ser representados mediante UML, haciendo uso del diagrama de despliegue. | |
| Pruebas de Aceptación: Analizar los componentes identificados. | |

Elaboración: Fausto Cevallos, Javier Sigüenza

Para realizar las historias técnicas, se han identificado en la reunión inicial del sprint las tareas de ingeniería necesarias las cuales a su vez se documentan en base a la Tabla 4-17, donde se escribe el nombre de la tarjeta, su sprint asignado y su identificación, el nombre de la historia a la que pertenece, el nombre de la tarea que será sometida a evaluación, el responsable de la prueba y el tipo de la tarea de ingeniería, la fecha de inicio y fin de la evaluación, así como su descripción y las pruebas a realizarse.

Tabla 4‑18 Prueba de Aceptación

|  |  |
| --- | --- |
| PRUEBA DE ACEPTACIÓN | |
| Código: PA\_HT1\_2 | **Nombre de la Historia:** Diseño de la Arquitectura del Sistema |
| Nombre de la Prueba: Analizar los componentes identificados. | |
| Responsable: Javier Sigüenza | **Fecha:** 1/10/2015 |
| Descripción: Cada componentes debe proveer al sistema una funcionalidad distinta y complemente toda la arquitectura. | |
| Condiciones de Ejecución: Se empleará una arquitectura de n capas, mínimo deben encontrarse las capas de interfaz de usuario, lógica del negocio, acceso a datos y almacenamiento de datos. | |
| Pasos de Ejecución:   * Analizar las capas que se han identificado en base al diagrama UML. * Determinar si se debe agregar o eliminar capas. | |
| Resultado Esperado: La arquitectura permite el correcto funcionamiento del sistema. | |
| Evaluación de la Prueba: Exitosa. | |

Elaboración: Fausto Cevallos, Javier Sigüenza

Para las pruebas de aceptación, se las realizarán de acuerdo al pedido de la historia a la que pertenece o su tarea de ingeniería, se documentan en base a la Tabla 4-18, donde se ha identificado a la prueba con un código, el nombre de la historia a la que pertenece, el nombre de la prueba que ha sido asignada en la tarea de ingeniería, el responsable, la fecha en la que se realiza la prueba, su descripción, las condiciones de ejecución de la prueba, es decir el medio ambiente en el que se realizará, los pasos de ejecución de las pruebas, el resultado esperado y su evaluación correspondiente, de aquí en adelante todas las historias se comentaran como la Tabal 4-16, las Tareas de Ingeniería como la Tabla 4-17 y las pruebas de aceptación como la Tabal 4-18.

Para la arquitectura del sistema se ha definido una aplicación en n-capas que permitirá incrementar la escalabilidad del sistema, de igual forma permitirá agregar de forma oportuna y eficaz nuevas funcionalidades sin tener que realizar modificaciones importantes en la arquitectura, se han definido 4 capas básicas que el sistema implementará o hará uso de las mismas, estas capas se han identificado en las siguiente figura:

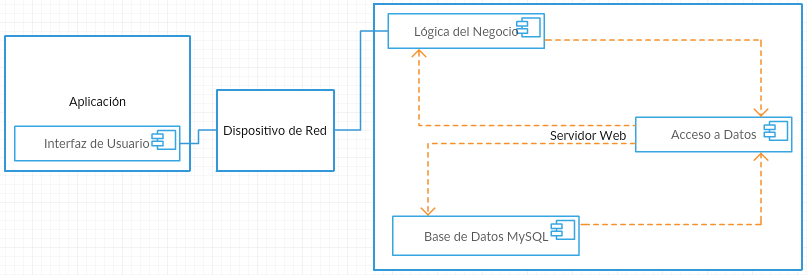


Figura 4‑5 Diagrama de Despliegue

Fuente: Realizado por Fausto C., Ángel S.

La Figura 4-5 representa el diagrama de despliegue del sistema informático, del que consta de un servidor web que aloja a las capas de lógica del negocio, acceso a datos y base de datos, esta configuración se debe a que la aplicación móvil (interfaz) consume servicios web del servidor de CIMOGSYS a través de un dispositivo de red, cada capa cumple una función específica que en conjunto forma el sistema informático de la aplicación móvil.

##### Diseño del Estándar de Codificación

El estándar de codificación permite normar el desarrollo de software con la finalidad de mejorar la legibilidad del código y su mantenimiento, permitiendo así que cualquier persona que tenga acceso al código pueda dar continuidad al proyecto en el caso de que un riesgo se presentare, existen diversos estándares de codificación por lo que sería poco favorable diseñar un estándar adicional por lo que se sugiere la implementación de uno existente, por su facilidad de memorización y aplicación se ha escogido es estándar Upper Camel Case empleado inicialmente en los años 50 en el Proyecto CinemaScope.

Upper Camel Case tiene recomendaciones[[9]](#footnote-9) básicas para su implementación de las cuales se pueden mencionar las siguientes:

* La primera letra siempre será mayúscula.
* Una o más letras en la palabra pueden ser mayúsculas.
* La palabra no puede terminar en una letra mayúscula.
* No pueden existir dos letras mayúsculas seguidas.
* No puede existir un número en ningún lugar de la palabra.
* No se pueden emplear puntos (“.”), guiones bajos (“\_”), guiones medios (“-”), solo palabras.
* No se admiten letras o caracteres especiales.

Dadas las principales características del estándar se verifica que puede ser implementado en el proyecto dado su uso genérico en cualquier nombre de archivo, función, procedimiento o variables por lo que el equipo de desarrollo ha considerado su aplicación.

##### Diseño del Estándar de Interfaces

Todas las interfaces de la aplicación móvil se basan en un patrón gráfico que representa a los sistemas informáticos creados actualmente y con anterioridad en el Centro de Investigación, como la aplicación será implementada en la Facultad de Administración de Empresas se ha adecuado la interfaz para la facultad, generando de la siguiente las pantallas de la aplicación móvil:

Inicio de Sesión

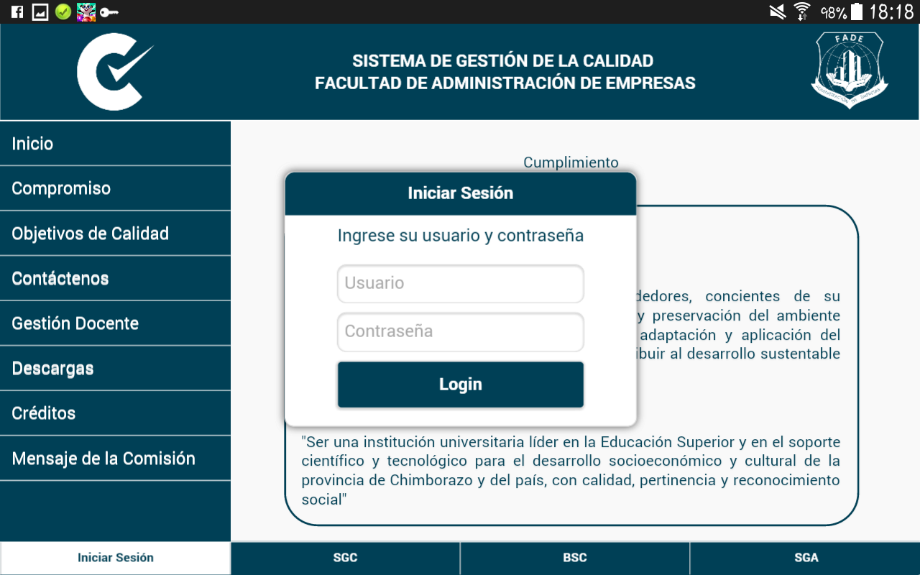


Figura 4‑6 Interfaz de Inicio de Sesión

Fuente: Estándar de Interfaces

Para la interfaz de inicio de sesión se ha creado un pop up en donde el usuario ingresará su usuario y contraseña, esta pantalla se mostrará cuando el usuario solicite autenticarse o en su defecto cuando una acción requiera un usuarios con privilegios distintos a los usuarios visitantes.

Pantallas de Inicio e Informativas

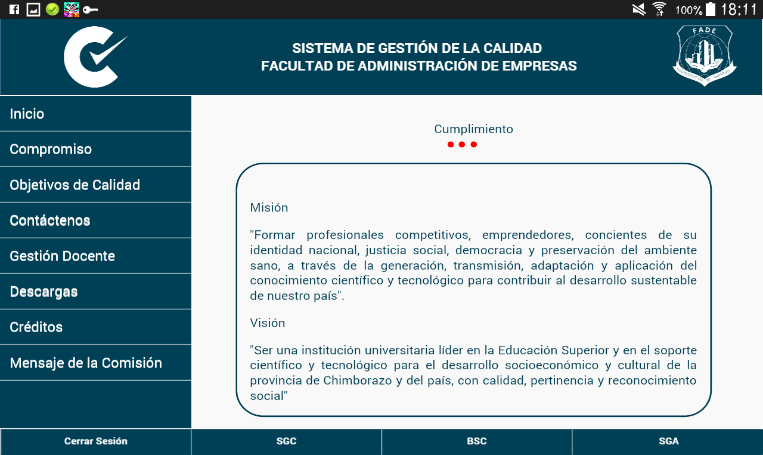
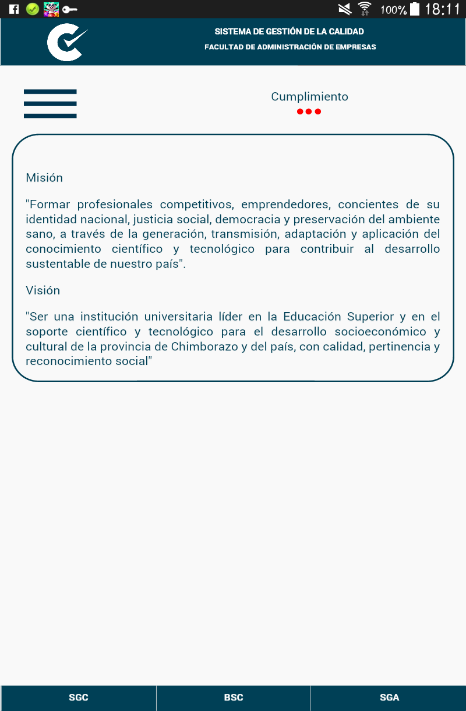


Figura 4‑7 Página de Inicio

Fuente: Estándar de Interfaces

Como se pueden apreciar en la Figura 4-7 se han representado como se visualizarán las interfaces de la aplicación móvil en pantallas de teléfonos inteligentes (izquierda) y tabletas (derecha) respectivamente, los diseños pueden ser fácilmente identificados en la interfaz de teléfono inteligente se pueden apreciar 3 secciones representativas, el encabezado que mantiene un logo y dos títulos, el primero identificativo de la aplicación y el segundo de la organización donde se implementa, en el encabezado predomina en contraste de colores azul y blanco, en la sección media se han posicionado los contenidos principales como el menú con efecto off canvas así como el semáforo que indica el nivel de cumplimiento, en esta sección predomina el gris con letras azules, finalmente en la parte inferior se diferencia un menú que conduce a los mapas de los 3 sistemas operativos que integra la aplicación.

En la interfaz para tabletas el diseño se mantiene aunque varían sus contenidos, como principal característica se puede apreciar el logo de la facultad en el encabezado, en la sección media el menú pierde el efecto off canvas y se torna de color azul, en la sección gris se mantienen las disposiciones de contenidos así como en el pie de página, este diseño mantiene concordancia con la línea gráfica de CIMOGSYS, las interfaces que manejan este criterio son las páginas de misión y visión, mensaje de la comisión, créditos, contactos, mensaje de la comisión, compromisos y objetivos de calidad.

Menú de los Sistemas de Gestión



Figura 4‑8 Menú de los Sistemas de Gestión

Fuente: Estándar de Interfaces.

Al ingresar el usuario en cualquier de los sistemas que se encuentran en el menú inferior y sean de Procesos, Balance Score Card o Acreditación se encontrarán con el menú de la Figura 4-8, el menú permite la navegación interna de cada sistema, la misma que consiste en la visualización de la facultad y sus escuelas con los semáforos que indican el cumplimiento que se ha generado en los respectivos sistemas informáticos, permanece el estándar de secciones encabezado, cuerpo y pie de página de la pantalla inicial, desde cada uno de los enlaces publicados se puede visualizar los procesos, perspectivas y criterios existentes, de igual forma un usuario autenticado puede acceder desde esta interfaz para realizar las auditorías.

Interfaces de Mapas

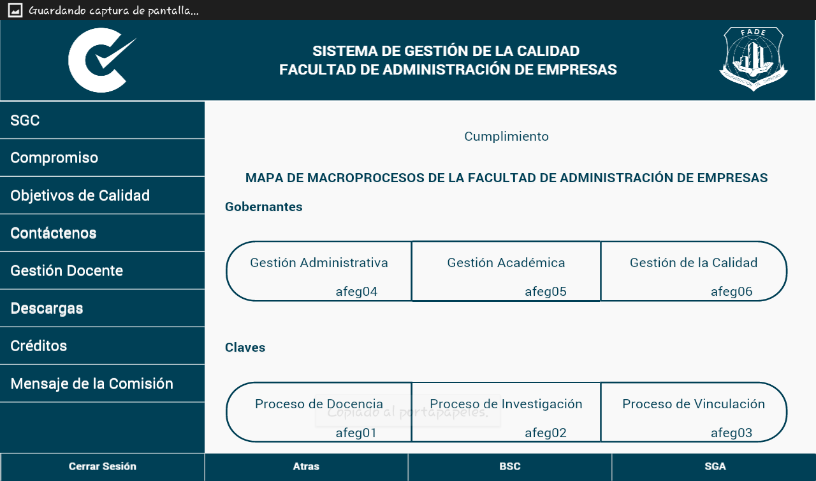
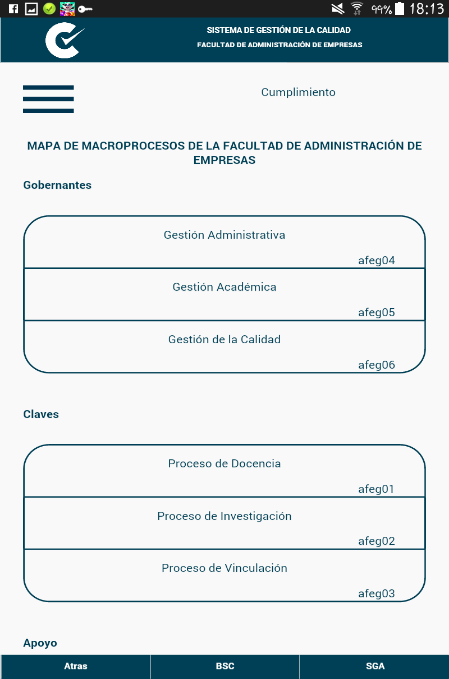


Figura 4‑9 Mapas de Procesos

Fuente: Estándar de Interfaces.

Los mapas de procesos se visualizarán como se muestra en la Figura 4-9, se mantiene la estructuras de las páginas de la aplicación con sus 3 secciones sin embargo se ha realizado una ligera modificación en el despliegue de los mapas de procesos que su diseño en la interfaz web, esto se debe a que no existe el espacio suficiente para la visualización de contenidos, se mantiene los 3 grupos de macro procesos y de identifica cada uno de ellos mediante un código asignado, en la interfaz móvil (izquierda) los macroprocesos se asignan de forma vertical y en el diseño tableta (derecha) se organizan de manera horizontal, esta tendencia se mantiene en los mapas estratégicos y de entorno de aprendizaje.

Interfaces de auditorías

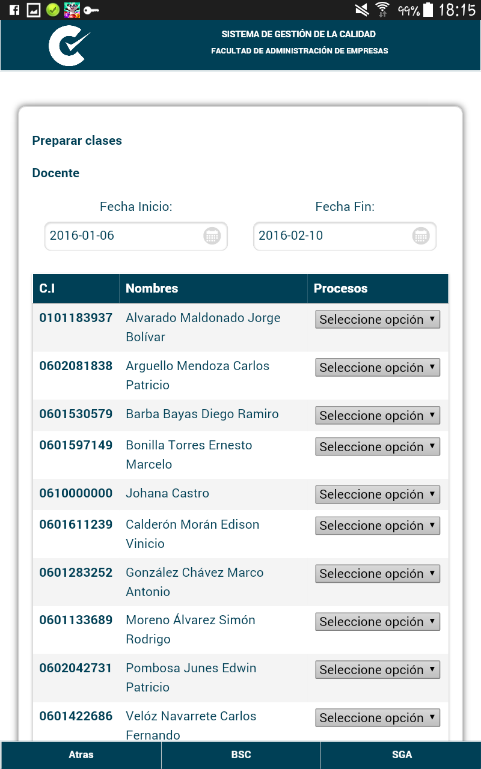


Figura 4‑10 Interfaces de Auditoría de Procesos

Fuente: estándar de Interfaces.

En la Figura 4-10 se puede apreciar las interfaces para realizar la auditoría de un proceso, tanto en la interfaz de dispositivo móvil como de tableta muestran dos campos para ingresar la fecha de inicio de auditoría así como la fecha final, a los cual se mostrará la lista de los responsables del proceso, los mismos que serán evaluados en base a su cumplimiento, se identifica que las interfaces mantienen la disposición de 3 secciones, esta disposición de mantiene en la auditoría de cumplimiento a las perspectivas del mapa estratégico.

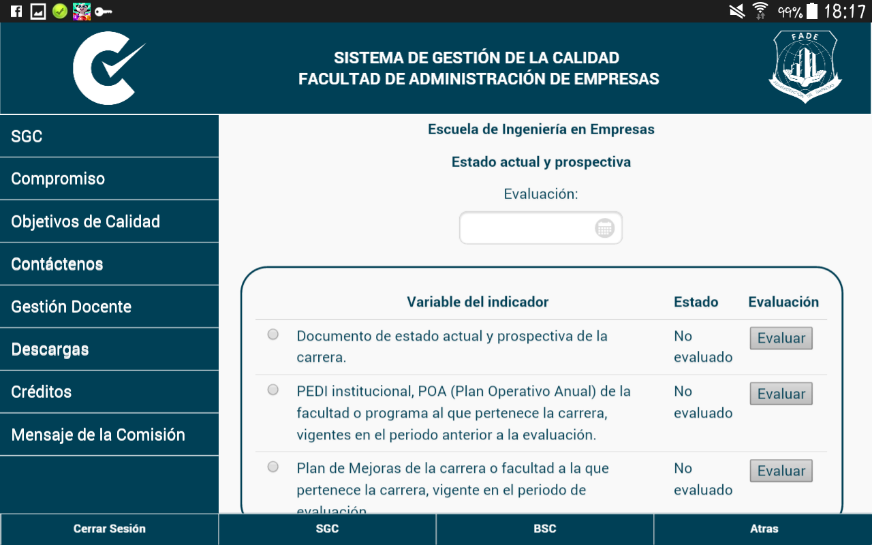
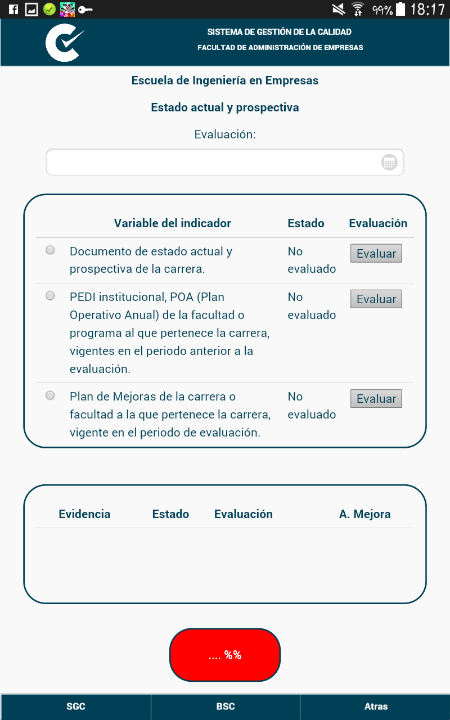


Figura 4‑11 Interfaz de Auditoría de Criterios

Fuente: Estándar de Interfaces.

La figura 4-11 permite apreciar las interfaces que se presentan al usuario para realizar la auditoría de acreditación dentro de un mapa de entorno de aprendizaje, el mismo que consta de tres secciones, la primera permite evaluar los indicadores de los criterios, la segunda sección permite el ingreso de las evidencias y en la tercera sección se mide el porcentaje de cumplimiento de cada variable, esta orientación es vertical en los dispositivos móviles y en las tabletas en horizontal, cada sección de evaluación cuenta con listas de check boxes, descripciones y botones para su evaluación, en las evidencias se permite la subida de archivos al servidor.

##### Especificación de Objetivos de Seguridad

Se ha estudiado las políticas de seguridad existentes dentro del desarrollo de aplicaciones móviles en el estudio de investigación, al no contarse con un estándar específico se adoptarán las prácticas establecidas, en específico la capa de presentación que incluye a la aplicación, la misma que consume servicios web.

Para implementar estas políticas de seguridad se necesitan especificar algunas metodologías de las cuales se especifican las siguientes:

Metodología para el manejo de datos geográficos.- Esta metodología no se realizará puesto que la aplicación no utiliza la localización del dispositivo, ni requiere conocer la ubicación del usuario.

Metodología para el manejo de archivos.- En los archivos se cifrará su nombre, se evitará asignar permisos de ejecución y se verificará su extensión, con lo que se evitará su reconocimiento y verificará que es el tipo de archivos que requiere la aplicación como por ejemplo solo archivos PDF.

Metodología para los archivos de configuración.- Los archivos de configuración deben acoparse al sistema operativo huésped, cuando se compile la aplicación se debe verificar que no queden configuraciones antiguas o de otros entornos.

Metodología para el manejo de archivos XML.- Todos los archivos XML deben manejar una estructura jerárquica diferenciada de igual forma que su sintaxis.

Metodología para el manejo de cookies.- Para el manejo de cookies lo que se implementará es el cifrado del archivo mediante un algoritmo como por ejemplo md5, de esta manera se podrá verificar si existe modificación de su contenido al comparar cifrados así como también dificultará al atacante inspeccionar su contenido.

Metodología para el manejo de servicios web.- En los servicios web en caso específico se acogerá a los servicios web que son asignados para la aplicación.

Metodología para el manejo de sesiones.- Para el manejo de sesiones se acogerá a la metodología de la aplicación web puesto que si se realiza un manejo de sesiones de otra forma se podrían producir fallos en su uso.

Metodología para el manejo de URL.- Todas las URL que se empleen en la aplicación deben coincidir con la dirección de los servicios web, las URL internas para la paginación deben ser especificadas como rutas relativas en caso de un atacante vulnerar las archivos le sea difícil encontrar su origen.

Implementar una metodología para el cifrado de datos.- Para cifrar los datos se deben emplear algoritmos criptográficos siempre que el framework de desarrollo lo soporte para no tener conflictos con la aplicación web se implementará un cifrado a base de md5.

Implementar una metodología para el manejo de Logs.- Los logs serán manejados por el servidor ya que es quien procesa los servicios web no se recomienda almacenar logs en el mismo lugar en el que se producen las acciones.

Implementar una metodología para procesos de autenticación de doble factor.- Este método de autenticación no se ha contemplado en el servidor por lo que no se considera su aplicación.

Verificar los canales de distribución.- Esta aplicación al ser de uso exclusivo de la facultad no se subirá a ninguna tienda móvil sino que se instalará en dispositivos de la facultad autorizados como por ejemplo los dispositivos de los auditores.

Implementar una metodología de codificación.- Todos los procesos, funciones, variables deben ser declarados y nombrados en base al estándar de codificación.

La aplicación móvil no emplea o no necesita canales de conexión internas del dispositivo por lo que no se crean metodologías para comunicaciones RF, la aplicación no hace uso de servicios de mensajería por lo que no se prevendrá ataques como SMiShing o ataques de hombre en el móvil pero si debe hacerse una aclaración al usuario de que estos ataques existen y deben tenerlos en consideración, las aplicaciones creadas en la ESPOCH así como en CIMOGSYS no poseen certificados SSL seguros o producidos por empresas reconocidas por lo que ataques de SlStrip no se ven considerados.

Una vez finalizadas las historias técnicas correspondientes al primer Sprint el equipo se reúne para analizar el resultado del trabajo de la semana, el mismo que ha dejado el diseño de la arquitectura que explicará de forma general como funcionará la aplicación móvil y cómo será su implementación, se ha definido una arquitectura n-capas ya que de esta manera el sistema puede tener una mayor escalabilidad, la aplicación móvil consume servicios web, se ha definido el estándar de codificación a implantarse empleando Upper Camel Case por su facilidad de memoria y uso, el estándar de interfaces que guiará a los desarrolladores hacia las interfaces finales que empleará el usuario, se ha definido el responsable de seguridad en la persona de Fausto Cevallos de igual forma se han determinado las políticas de seguridad, como la aplicación solo se desarrolla desde la capa de presentación se aplicarán las políticas respectivas.

Los productos entregados por el equipo han cumplido con las especificaciones requeridas por lo que se recomienda que se continúe con el proyecto resolviendo las Historias de Usuario asignadas en el Sprint 2.

#### Sprint 2

Para la realización del segundo Sprint se han reunido los miembros del proyecto para continuar con las Historias de Usuario planificadas, las mismas que corresponden al despliegue y visualización de los mapas de procesos y estratégicos de la facultad con sus escuelas, al ser estas historias de tamaño XL se han dividido en dos, cada una con un tiempo estimado de 20 puntos por lo que serán realizadas en dos Sprints.

Despliegue de Mapas de Procesos, se genera todas las interfaces necesarias para desplegar los mapas de procesos de la Facultad, por lo que se cuenta con 3 archivos en los que se generará el código, fruto de la resolución de las teteras de ingeniería identificadas, este proceso se repite con el  despliegue de Mapas Estratégicos.

Una vez finalizadas las historias de usuario del sprint 2, el equipo del proyecto se reúne para revisar el avance de la aplicación, en esta ocasión se entrega ya productos funcionales, se pueden visualizar los mapas de procesos de la Facultad, de las Escuelas de Contabilidad y Auditoría, Empresas y Gestión de Transporte, se visualizan los macroprocesos sus procesos e indicadores con sus semáforos de cumplimiento, la aplicación cumple con los estándares de programación, interfaces y de seguridad, estas medidas de seguridad han sido escogidas en base a las operaciones actuales del sprint del listado general de seguridad para la capa de presentación, con un factor, los datos no son enviados de forma cifrada desde el servidor.

Desde el Sprint 3 hasta el Sprint 11, siguen la misma estructura que el Sprint 2, implementan la creación del código para cumplir con los requerimientos del usuario asignados en las Historias pertinentes por lo que si existe alguna inquietud e sugiere revisar el anexo B desde la página 49 hasta la página 224, el código generado a su vez por este desarrollo se encuentra en la aplicación móvil creada para la Facultad de Administración de Empresas.

#### Sprint 12

Para la realización del décimo segundo Sprint se han reunido los miembros del proyecto para continuar con las historias técnicas de usuario faltantes que son la realización del manual de usuario y manual técnico.

El Manual Técnico ha sido desarrollado en base a la metodología SCRUM, donde se ha desarrollado de forma minuciosa la estimación, especificación de requerimientos, estudios de factibilidad, la planificación y el desarrollo del proyecto dono han sido generadas las historias de usuario, tareas de ingeniería, pruebas de aceptación y le gráfico de seguimiento del proyecto (véase el Anexo B).

El Manual de Usuario ha sido empleado en base a la guía proporcionada por la Ing. Alena Gonzáles de Cuba, 2010, donde se especifican las principales características de la aplicación, sus requerimientos técnicos, su proceso de instalación, las generalidades del sistema, como poder iniciar sesión y cerrar sesión, la explicación de cada uno de los módulos que se encuentran integrados, el manejo de errores, y los contactos de soporte técnico (véase el Anexo C).

Se ha finalizado las historias de usuario del sprint 12, el equipo del proyecto se reúne para revisar el avance de la documentación, se entrega el manual técnico y de usuario con la finalidad de explicar cómo fue construida la aplicación y su funcionamiento, se procede a realizar el gráfico de Seguimiento del Proyecto.

#### Seguimiento del Proyecto

El gráfico de seguimiento del proyecto permite identificar en que tiempo o cuantos puntos estimados se ha tomado para la realización de las historias de usuario, esto nos permite verificar si el proyecto se mantiene en la línea de tiempo ideal, va más rápido o lento, en la aplicación móvil se generó el siguiente gráfico de seguimiento:

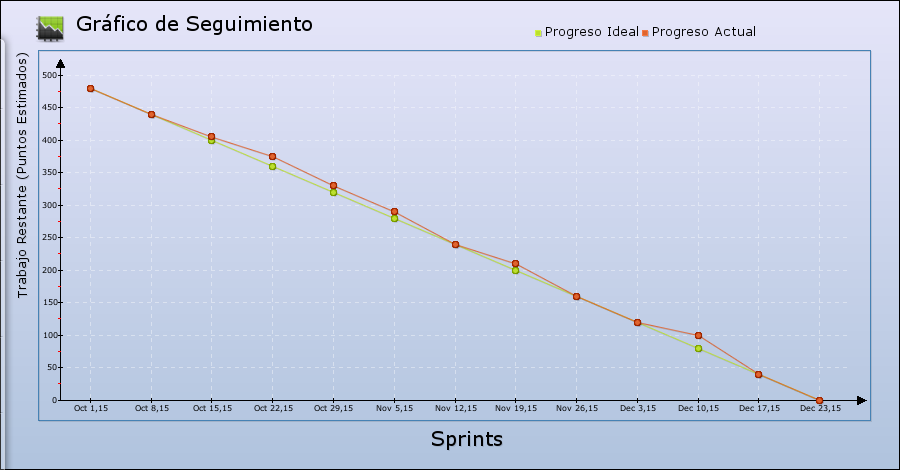


Figura 4‑12 Gráfico de Seguimiento del Proyecto

Fuente: Seguimiento del proyecto de creación de la aplicación móvil.

En la Figura 4-12 las estimaciones realizadas a las historias de usuario se encuentran por debajo de los puntos estimados reales, la principal causa de este desfase radica en que la aplicación móvil integra 3 sistemas informáticos dos de la misma arquitectura por lo que se dificultó el desarrollo da la aplicación otro factor importante es que por lo general los proyectos de software no estiman la seguridad que incluirá el mismo, en este proyecto se identifica que agregar seguridad de forma adecuada incrementa el tiempo de desarrollo del proyecto sin embargo este costo de tiempo debe ser considerado ya que no es posible que software en producción mantenga muchas vulnerabilidades, la arquitectura independiente dificultó sus estandarización, a más de tener muchos más detalles al evaluar las evidencias y los criterios.

# CONCLUSIONES

Se ha identificado que la Escuela Superior Politécnica de Chimborazo, posee vulnerabilidades en las capas de almacenamiento de datos, lógica del negocio, física de transporte, y de presentación, las personas encuestadas conocen los ataques y vulnerabilidades pero no se toman medidas que permitan prevenir estas falencias, no se aplican metodologías conocidas para la prevención de problemas de seguridad y no se registran logs que permitan verificar la ocurrencia de ataques.

Se identificaron problemas de disponibilidad de información en las aplicaciones que integran el Sistema de Gestión de Información de la Facultad de Administración de Empresas, estos inconvenientes se encuentran en las dimensiones de lugar y dispositivo puesto que no se permite el ingreso oportuno al sistema por restricciones de conexión a internet y la falta de equipos.

Se desarrolló una aplicación móvil para la Facultad de Administración de Empresas, que permite incrementar la disponibilidad de información, empleando buenas prácticas de seguridad, las mismas que han resultado de la investigación y pueden ser aplicadas en cualquier proyecto de desarrollo de software.

Se ha realiza el desarrollo de la aplicación móvil mediante el uso de la Metodología Ágil SCRUM, la misma que ha podido documentar a detalle la solución de los requerimientos del usuario, no obstante al agregar como historia técnica la especificación de los objetivos de seguridad así como sus pruebas realizadas, la documentación ha incrementado su volumen lo que la vuelve difícil de manejar.

Se pudo verificar que hubo una variación entre el tiempo de estimación y el tiempo real del desarrollo de software, así como las líneas de código estimadas y las reales, por lo que se verifica que los modelos de estimación no son los adecuados para la Escuela Superior Politécnica de Chimborazo.

# RECOMENDACIONES

Se recomienda realizar una investigación que permita ajustar los modelos de estimación para la realización de proyectos de desarrollo de software dentro de la Escuela Superior Politécnica de Chimborazo, sus Facultades y Centros de Investigación, con la finalidad de obtener datos más acercados a la realidad de la institución.

Se recomienda realizar una investigación que permita identificar qué metodología de desarrollo de aplicaciones, se acopla de mejor manera con las pruebas de seguridad planteadas, con la finalidad de mejorar su implementación sin incrementar su volumen de forma incontrolable.

Se recomienda que se desarrollen propuestas específicas, a las metodologías que se requiere en las prácticas de seguridad, como por ejemplo la metodología de asignación de permisos y privilegios a los usuarios.

Se recomienda capacitar a los usuarios y técnicos de las diferentes facultades en aspectos de seguridad en los proyectos de software, debido a que los ataques y las vulnerabilidades incrementan con el paso del tiempo y los conocimientos pueden quedar obsoletos ante una nueva variante de estas amenazas.

Se recomienda realizar un estudio para complementar la dimisión de dispositivo, verificar si es necesario la creación de aplicaciones para televisión y automóviles, dentro de la Facultad de Administración de Empresas o de la Escuela Superior Politécnica de Chimborazo.

Se recomienda realizar una investigación de las buenas prácticas de seguridad sobre aplicaciones de escritorio, televisión y auto con la finalidad de mantener actualizadas las listas de vulnerabilidades y amenazas de software de forma global.

Se recomienda realizar un estudio de usabilidad web en los sistemas de Gestión de Procesos, Balance Score Card e Indicadores de Acreditación, con la finalidad de verificar la usabilidad del SGI.

Se recomienda realizar un sistema de control de productos de software, con la finalidad, de que, cada facultad o unidad dentro de la Escuela Superior Politécnica de Chimborazo mantenga un control de las aplicaciones creadas, dado que al ser encuestados sobre el tema, los responsables no poseían datos concretos sino estimados.

# BIBLIOGRAFÍA

**AGUILERA, Purificación.** *Seguridad Informática.* Gonzalo Morlanes [ed.]**.** Madrid: Pozuelo de Alarcón, 2010. 239p. pag 14. ISBN: 978-84-9771-761-8

**ALTIRRIBA, Narcís.** “Guía para proteger y usar de forma segura su móvil en la empresa”. Director: Jorge Chinea. Universitat Oberta de Catalunya (2015). [Consultada en: 5 septiembre 2015]. Disponible en: http://hdl.handle.net/10609/39541

**BANSAY, Vinal; et al.,**  *Smartphone Secure Development Guidelines for App Developers*[en línea], 25 noviembre 2011, ENISA, [Consultada en: 5 septiembre 2015]. Disponible en: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines

**BARONA, Jorge.** *Ecuador le declara la guerra al robo de teléfonos celulares* [en línea].Guayaquil: Andes. [Consultada: 7 septiembre 2015]. Disponible en: http://www.andes.info.ec/es/noticias/ecuador-declara-guerra-robo-telefonos-celulares.html

**CARTAYA, Marcelo.** *Riesgo de Auditoría.* [en línea]. Instituto de Altos Estudios de Control Fiscal y Auditoría de Estado (COFAE). [Consultada en: 18 de septiembre de 2015]. Disponible en: http://www.oas.org/juridico/PDFs/mesicic4\_ven\_ries\_aud\_2014.pdf.

**CEAACES.** *Evaluación de universidades 2013* [en línea]. 2013. [Consultada: 5 septiembre 2015]. Disponible en: http://www.ceaaces.gob.ec/sitio/evaluacion-universidades-2013/

**CENTRO E INVESTIGACIÓN EN MODELOS DE GESTIÓN Y SISTEMAS INFORMÁTICOS.** *Sistema de Gestión de Calidad* [en línea]. 2014. [Consultada: 22 noviembre 2015], Disponible en: http://sgc.fade.cimogsys.com/

**CEQUEDA, Jean.** *Amenazas a la Seguridad Informática.* [en línea]. Abril, 2012. [Consultada en: 28 de septiembre de 2015]. Disponible en: https://seguridadinformaticaufps.wikispaces.com/file/view/U4\_Amenazas\_SI.pdf

**CHICANO, Ester.** *Auditoría de Seguridad Informática.* Primera Edición. España: Antequera, 2014. ISBN: 978-84-16433-23-0

**COMUNIDAD DE MADRID.** *Tratamiento de Riesgos.* [en línea]. Estrategias de tratamiento de riesgos. [Consultada en 22 de septiembre de 2015]. Disponible en: http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis\_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo(AR)\_es.pdf

**CONSORCIO WORLD WIDE WEB,** *Guía Breve sobre Estándares Web* [en línea]. [Consultada en: 8 septiembre 2015]**.** Disponible en: http://www.w3c.es/Divulgacion/GuiasBreves/Estandares

**COREO NE IT.** *Disponibilidad de la Información.* [en línea]. México. DF. Disponibilidad de la Información. [Consultada en: 30 de noviembre de 2015]. Disponible en: http://www.coreoneit.com/disponibilidad-de-la-informacion/

**COSTAS, José.** *Seguridad y Alta Disponibilidad.* Editorial: RA-MA. 2011. P 1-144. ISBN: 978-84-9964-104-1.

**DAMITEL NETWORKS.** *Alta Disponibilidad.* [En línea]. Madrid. [Consultada en: 30 de noviembre de 2015]. Disponible en: http://www.damitel.com/ingenieria-de-sistemas/alta-disponibilidad/

**DELGADILLO, Patricia et al. “**Los dispositivos móviles en el modelo educativo basado en competencias en el sector público de la licenciatura en ingeniería en computación”. *Revista Iberoamericana de Producción Académica y Gestión Educativa.* ISSN 2007 – 8412. Publicación 2. Junio 2015. p. 7, 23.

**ECUADOR.** Ley Orgánica de Educación Superior, *Registro Oficial N°298*, de 12 de octubre de 2010, p. 17, Título IV, Capítulo I. http://www.ces.gob.ec/descargas/ley-organica-de-educacion-superior

**ESET,** Guía de Seguridad para usuarios de Smartphones. [En línea]. 2014. [Consultada en 20 de diciembre de 2015]. Disponible en: http://www.welivesecurity.com/wp-content/uploads/2014/01/documento\_guia\_de\_seguridad\_para\_usuarios\_de\_smartphone\_baj.pdf

**ESPAÑA.** Ley 51/2003de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. Artículo 8. Inciso 1. http://noticias.juridicas.com/base\_datos/Admin/l51-2003.html#a2

**GARCÍA, Alexander.** *Dispositivos Móviles,* [en línea]. 2011. [Consultada en: 12 septiembre 2015]. Disponible en: http://augusta.uao.edu.co/moodle/file.php/2896/pres\_dispositivos\_moviles-2011.pdf.

**GARNAEVA María et al.,**  *IT Thread evolution in Q1 2015* [en línea]*.* 6 mayo 2015. [Consultada: 5 septiembre 2015]. Disponible en: https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/

**GOBIERNO DE CHILE.** *Guía Digital/¿Qué es Usabilidad?* [En línea]. [Consultada en: 30 noviembre de 2015]. Disponible en: http://www.guiadigital.gob.cl/articulo/que-es-la-usabilidad

**GÓMEZ, M. C.** *Notas del Curso Análisis de Requerimientos.* Tlalpan, México DF, 2011, pp. 3. ISBN: 978-607-477-442-9. Disponible en: http://www.cua.uam.mx/pdfs/conoce/libroselec/Notas\_Analisis\_Requerimiento.pdf

**HASSAN, YUSEF; ORTEGA SERGIO.** “Informe APEI de Usabilidad”. *No solo usabilidad.* Definición y Conceptos. [Consultada en: 30 de noviembre de 2015]. ISSN1886-8592.

**INSTITUTO ECUATORIANO DE NORMALIZACIÓN,** *Normalización y Actividades Conexas Vocabulario General.* GPE INEN-ISO/IEC 2:2006. Primera Edición. Quito-Ecuador. 2006.

**INSTITUTO MODERNO DE MEJORES PRÁCTICAS CORPORATIVAS.** *“Qué son las mejores prácticas corporativas”*. Jalisco, México. [Consultada en: 7 septiembre 2015] Disponible en: http://www.immpc.org.mx/mejores-practicas-corporativas

**ISO/IEC 25010:2011.** *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.*

**ISOTOOLS EXCELLENCE.** *ISO 27001.**El inventario de activos en la implementación de la norma.* [en línea]. [Consultada en: 16 de septiembre 2015]. Disponible en: https://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

**ISOTOOLS EXCELLENCE.** *ISO 27001.**Las Claves del Éxito para la Gestión de Riesgos.* [en línea]. [Consultada en: 21 de septiembre 2015]. Disponible en: https://www.isotools.org/pdfs-pro/whitepaper-claves-exito-gestion-riesgos.pdf

**LISANDRO, Delia; et al.** “Un análisis experimental de tipo de aplicaciones para dispositivos móviles” [en línea]. En: XVIII Congreso Argentino de Ciencias de la Computación. (Octubre del 2013). [S.I.] [s.n]. Disponible en: http://sedici.unlp.edu.ar/handle/10915/32397

**MACIA, Nicolás et al.,** *Seguridad en dispositivos móviles: un enfoque práctico* [en línea]. WICC 2014 XVI Workshop de Investigadores en Ciencias de la Computación. [Buenos Aires: Argentina]: La Plata. [Consultada en: 5 septiembre 2015]. Disponible en:http://sedici.unlp.edu.ar/bitstream/handle/10915/43678/Documento\_completo.pdf?sequence=1.

[**MALENKOVICH**](https://blog.kaspersky.es/author/sym451/)**, Serge.** *Root y Jailbreak: ¿Cómo afectan a la seguridad?* [en línea]. 31 mayo 2013. Riesgos en la Seguridad. [Consultada en: 17 noviembre 2015]. Disponible en: https://blog.kaspersky.es/root-y-jailbreak-como-afectan-a-la-seguridad/907/

**MARTÍNEZ, Evelio.** *Estándares y Organizaciones* [blog]. 8 mayo, 2014 [Consultada en: 8 septiembre 2014]. Disponible en: http://www.eveliux.com/mx/curso/estandares-y-organizaciones.html

**MIERES, Jorge.** *Ataques informáticos – Debilidades de Seguridad Comunmente Explotadas.* [En línea] Evil Fingers. Enero, 2009. [Consultada en 22 de septiembre de 2014]. Disponible en: https://www.evilfingers.com/publications/white\_AR/01\_Ataques\_informaticos.pdf

**MINISTERIO DE SALUD.** *Conceptos Básicos de la Gestión de Riesgos.* [en línea]. Av. 9 de Julio 1925 (C1073ABA) Buenos Aires - República Argentina. [Consultada en: 16 de septiembre de 2015]. Disponible en: http://www.msal.gob.ar/salud-y-desastres/index.php/informacion-para-comunicadores/conceptos-basicos-de-la-gestion-de-riesgos

**NORTON.** *Cómo atacan: Vulnerabilidades.* [En línea]. España. 2015. [Consultada en: 15 de septiembre de 2015]. Disponible en: http://es.norton.com/security\_response/vulnerabilities.jsp

**NOWSECURE,** *Secure Mobile Development* [en línea]. 8 julio 2015. [Consultada: 5 septiembre 2015], Disponible en: https://www.nowsecure.com/resources/secure-mobile-development/

**NOWSECURE.** *Secure Mobile Development.* [en línea]. 26 de Noviembre de 2014. Mobile Security Premier. [Consultada en: 22 de septiembre de 2015]. Disponible en: https://www.nowsecure.com/resources/secure-mobile-development/primer/mobile-security/

**OBSERVATORIO DE LA ACCESIBILIDAD,** *Definición de Accesibilidad* [en línea]. 2015. [Consultada: 6 diciembre de 2015], Disponible en: http://www.observatoriodelaaccesibilidad.es/accesibilidad/accesibilidad/definicion/

**OPEN WEB APPLICATION SECURITY PROYECT,** *Mobile Security Project – Top Ten Mobile Risks* [en línea]. 2014. [Consultada en: 5 septiembre 2015], Disponible en: https://www.owasp.org/index.php/Projects/OWASP\_Mobile\_Security\_Project\_-\_Top\_Ten\_Mobile\_Risks

**ORGANIZACIÓN DE NACIONES UNIDAS PARA LA ALIMENTACIÓN Y AGRICULTURA.** *Plantilla de buenas prácticas* [en línea]. Julio 2015. [Consultada en: 7 septiembre 2015] Disponible en: http://www.fao.org/3/a-as547s.pdf

**PANDA.** Informe Especial: Predicciones 2015. [En línea]. Junio 2014. [Consultada en: 20 de diciembre de 2015]. Disponible en: http://www.pandasecurity.com/spain/mediacenter/src/uploads/2014/07/pandalabs-predicciones-2015.pdf

**PASTOR, Javier.** *Desarrollo de Aplicaciones Móviles (I): Así Está el Mercado.* [en línea]. 12 marzo 2014. HTML5, un gigante dormido. [Consultada en: 17 noviembre 2015]. Disponible en: http://www.xatakamovil.com/mercado/desarrollo-de-aplicaciones-moviles-i-asi-esta-el-mercado

**RODRIGO, María; MÁIQUEZ, María; MARTÍN, Juan Carlos.** *Buenas prácticas profesionales para el apoyo a la Parentalidad positiva* [en línea]. Madrid, FEMP. C/ Nuncio, 8 28005, 2011. [Consultada en: 7 septiembre 2014]. Disponible en: http://www.msssi.gob.es/ssi/familiasInfancia/docs/BuenasPractParentalidadPositiva.pdf

**SCIENTIAMOBILE.** *Mobile Overview Report.* Informe Inédito.Junio 2015. 32p.

Disponible en: http://data.wurfl.io/MOVR/pdf/2015\_q2/MOVR\_2015\_q2.pdf

**SILBERSCHATZ, Abraham; GALVIN, Peter; GAGNE, Greg.** *Fundamentos de Sistemas Operativos.* Sánchez, Jesús (rev. tec.); Vuelapluma (trad.). Séptima Edición. Madrid, 2006. 828p. ISBN 84-481-4641-7 pag 3.

**STATISTA.** *Worldwide market share forecast of smartphone operating systems from 2010 to 2015.* Disponible en: http://www.statista.com/statistics/266970/market-share-forecast-of-smartphone-operating-systems-from-2010-to-2015/

**SOMMERVILLE, Ian.** *Ingeniería del Software.* Séptima Edición. España: Pearson Educación, S.A., 2005, pp 109-130. ISBN: 84-7829-074-5.

**TAO (T-Systems).** *Disponibilidad de Sistemas Informáticos.* [En línea]. pag 1. [Consultada en: 30 de noviembre de 2015]. Disponible en: http://www.tao.es/documentos/datasheets/DISPONIBILIDAD%20SISTEMAS%20INFORM%C3%81TICOS%20TAO%202.0%20T-SYSTEMS.pdf

**TARDÁGUILA, César.** *Dispositivos Móviles y Multimedia.* [en línea]. Revisión 2009. [Consultada en: 14 de septiembre de 2015]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/9164/1/dispositivos\_moviles\_y\_multimedia.pdf

**THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) AND THE INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC),** *Information technology — Security Techniques — Code of practice for information security controls.* ISO/IEC 27001:2013. Primera Edición. Ginebra-Suiza.

**THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).** Risk Managment - Vocabulary*.* ISO/Guide 73:2009. Primera Edición. Ginebra-Suiza.

**TELESEMANA,** *16 Millones de Dispositivos Móviles están Infectados con Software Malicioso* [blog]. 16 febrero 2015. Telesemana.com. Disponible en: http://www.telesemana.com/blog/2015/02/16/16-millones-de-dispositivos-moviles-estan-infectados-por-software-malicioso/.

**TENSTEP.** *Metodología TenStep.* [en línea]. Ecuador, Naciones Unidas E6-99 y Japón Edificio Banco Bolivariano of 601. Gestionar el Riesgo. [Consultada en: 21 de septiembre de 2015]. Disponible en: https://www.tenstep.ec/portal/index.php/nuestros-productos/tenstep/7-0-gestion-del-riesgo

**UNIDAD DE INFORMÁTICA.** *Manual de Procedimiento.* [en línea]. Secretaría de Comunicación Social de la Presidencia, Gobierno de Guatemala. Junio 2015. [Consultada en 23 de septiembre de 2015]. Disponible en: https://www.vicepresidencia.gob.gt/archivos/2015/06.+Manual+de+Procedimientos+Unidad+de+Informatica%202.4.pdf

**WORLD WIDE WEB CONSORTIUM,** *Web of devices*. [en línea]. [Consultada en: 22 de noviembre de 2015]. Disponible en: http://www.w3.org/standards/webofdevices/

# ANEXO A – MODELO DE ENCUESTAS

# ANEXO B – MANUAL TÉCNICO DE LA APLICACIÓN

# ANEXO C – MANUAL DE USUARIO

1. https://securityintelligence.com/man-in-the-mobile-attacks-single-out-android/ [↑](#footnote-ref-1)
2. http://www.infosecurity-magazine.com/news/man-in-the-browser-mitb-becomes-man-in-the-mobile/ [↑](#footnote-ref-2)
3. http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html [↑](#footnote-ref-3)
4. http://sgc.fade.cimogsys.com/ [↑](#footnote-ref-4)
5. http://sgc.fade.cimogsys.com/fadebsc/fade\_bsc [↑](#footnote-ref-5)
6. http://sga.fade.cimogsys.com/ [↑](#footnote-ref-6)
7. http://sunset.usc.edu/COCOMOII/cocomo.html [↑](#footnote-ref-7)
8. http://www.inf.ed.ac.uk/teaching/courses/sapm/2011-2012/slides/estimation.pdf [↑](#footnote-ref-8)
9. http://c2.com/cgi/wiki?CamelCase [↑](#footnote-ref-9)