UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL

MANUAL TÉCNICO

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: CAROLINA ESTEFANÍA MOROCHO CRESPO

TUTOR: ING. ISMELIS CASTELLANOS LÓPEZ, MSc.

GUAYAQUIL – ECUADOR
2016

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

El sistema de aplicación presentado funciona como un asistente metodológico para la evaluación del control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil a través de la ejecución de un análisis de brecha de seguridad de la información. Para esto la aplicación web toma como base los controles de la norma internacional de seguridad de la información ISO/IEC 27001: 2013 (última versión liberada y aprobada) y permite ejecutar la evaluación del control interno, realizando una comparación de la situación actual de la carrera contra el estado ideal propuesto por las buenas prácticas (Nivel Optimizado).

El presente Manual Técnico describe la estructura de la base de datos, diagramas de casos de uso, diagramas de clases y las especificaciones para una correcta instalación de las herramientas para el funcionamiento del sistema. Asimismo, es importante tener en cuenta que en el presente manual se hace mención a las especificaciones mínimas de hardware y software para la correcta instalación del aplicativo.

2. OBJETIVOS

Brindar la información necesaria para poder realizar la instalación y configuración de las herramientas de programación y que permitirán levantar el sistema de aplicación ICSystem.

2.1. Específicos:

- Representar la funcionalidad técnica de la estructura, diseño y definición del aplicativo.
- Detallar la especificación de los requerimientos de Hardware y Software necesarios para la instalación de la aplicación.
- Definir claramente el procedimiento de instalación del aplicativo.
- Describir las herramientas utilizadas para el diseño y desarrollo del prototipo.

3. ESPECIFICACIONES TÉCNICAS

El sistema de aplicación trabajará satisfactoriamente considerando las siguientes características de hardware y software:

3.1. Requisitos de Hardware

- Conectividad a la red.
- Mínimo 1 GB de memoria de RAM.
- Procesador con más de 8 núcleos.
- Mínimo 2 GB de espacio en disco duro.
- Pantalla de 1024 x 768 como mínimo con 256 colores.
- Mouse.

3.2. Requisitos de Software

- Compatibilidad con cualquier sistema operativo.
- Navegador web instalado. (Recomendación: Google Chrome)

4. DIAGRAMAS DE CASOS DE USO

4.1. Definición de actores

A continuación se describen los diferentes actores identificados para el uso de esta herramienta de software:

Nombre del actor: Administrador
Descripción: Este actor se encarga de realizar las tareas de administración de la herramienta así como también podrá realizar las tareas de un usuario final. Entre las tareas que podrá ejecutar este actor tenemos:

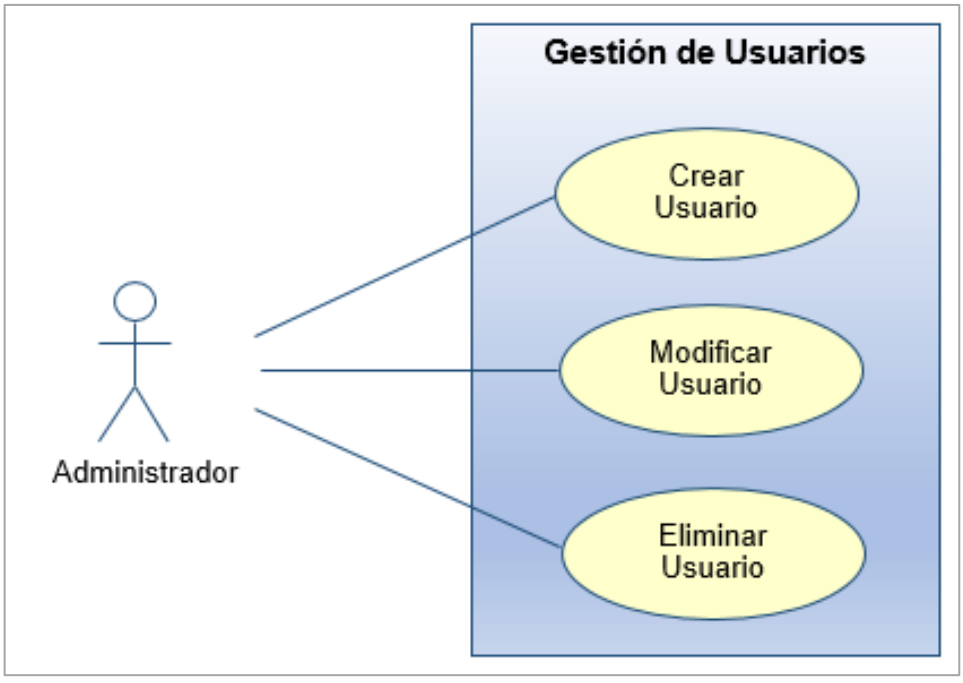
- Gestión de usuarios
  - Alta, modificación y baja de usuarios.
  - Asignación de perfiles de accesos.
- Gestión de unidades
  - Alta, modificación y baja de departamentos/unidades de la carrera.

- Gestión de estándares
  - Alta, modificación y baja de estándares.
- Gestión de niveles de madurez
  - Alta, modificación y baja de niveles de madurez.

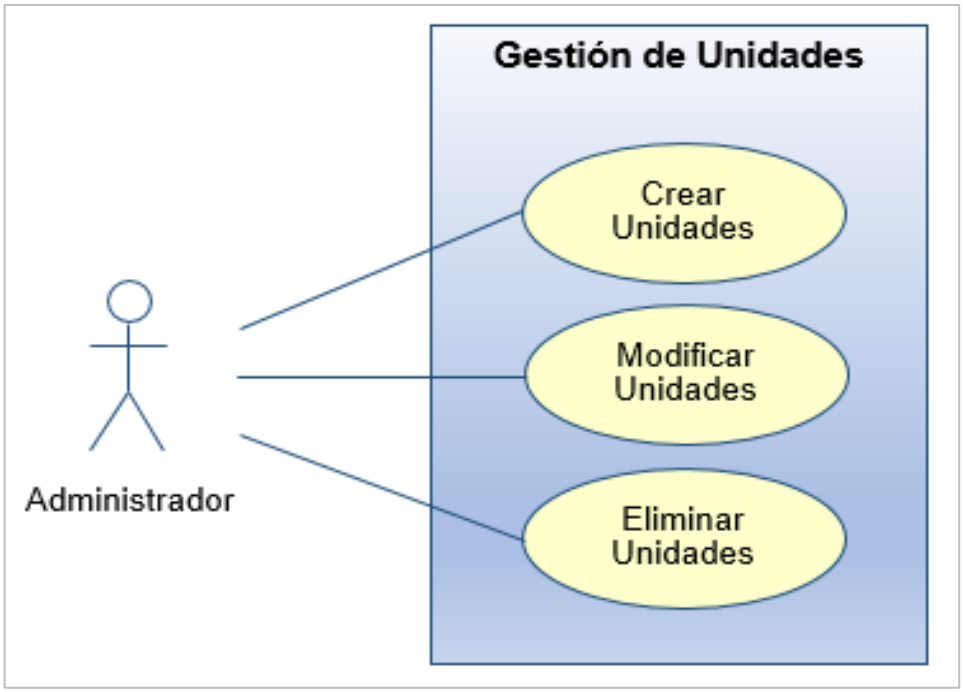
Nombre del actor: Usuario
Descripción: Este actor representa al usuario final que hará uso de la herramienta de software, el cual puede ser cualquier persona involucrada en la evaluación del control interno de la carrera. Entre las tareas que podrá ejecutar este actor tenemos:

- Revisión de los controles
  - Evaluación del control interno.
- Generación de listados de controles
  - Listados con los controles evaluados.
- Generación de gráficas
  - Gráficas que contienen la evaluación del control interno informático.

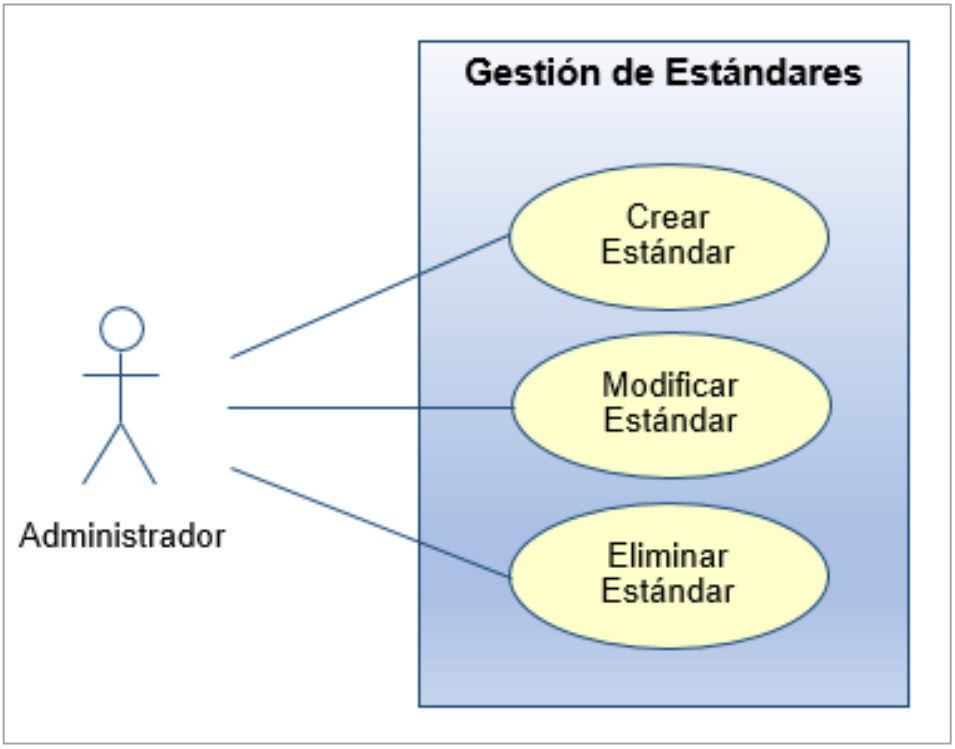
4.2. Caso de Uso: Gestión de Usuarios



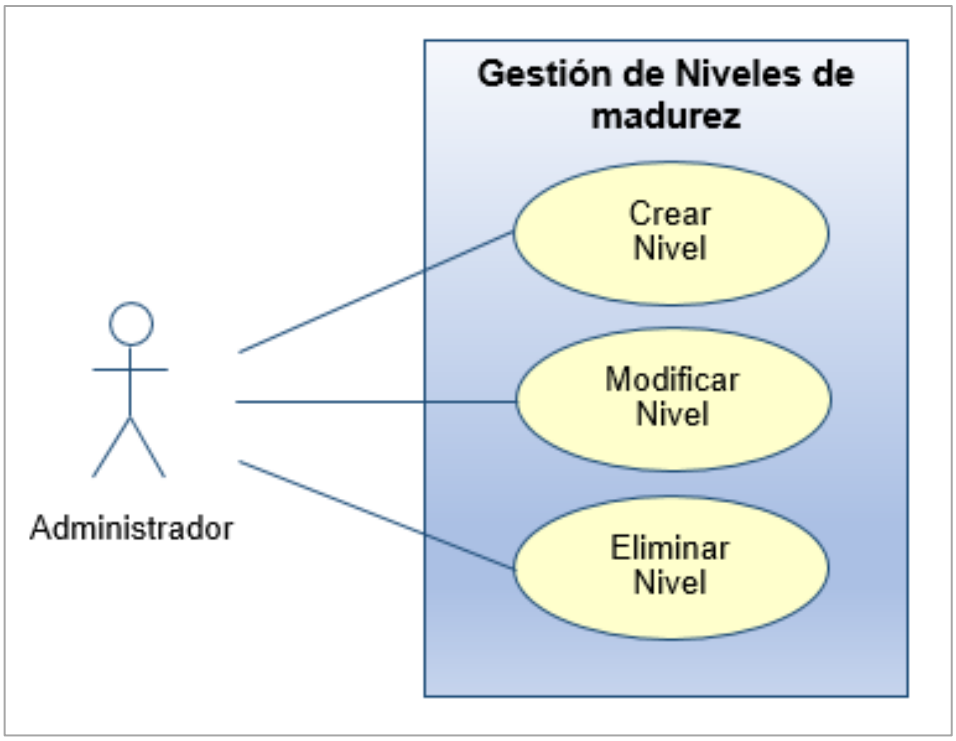
4.3. Caso de Uso: Gestión de Unidades



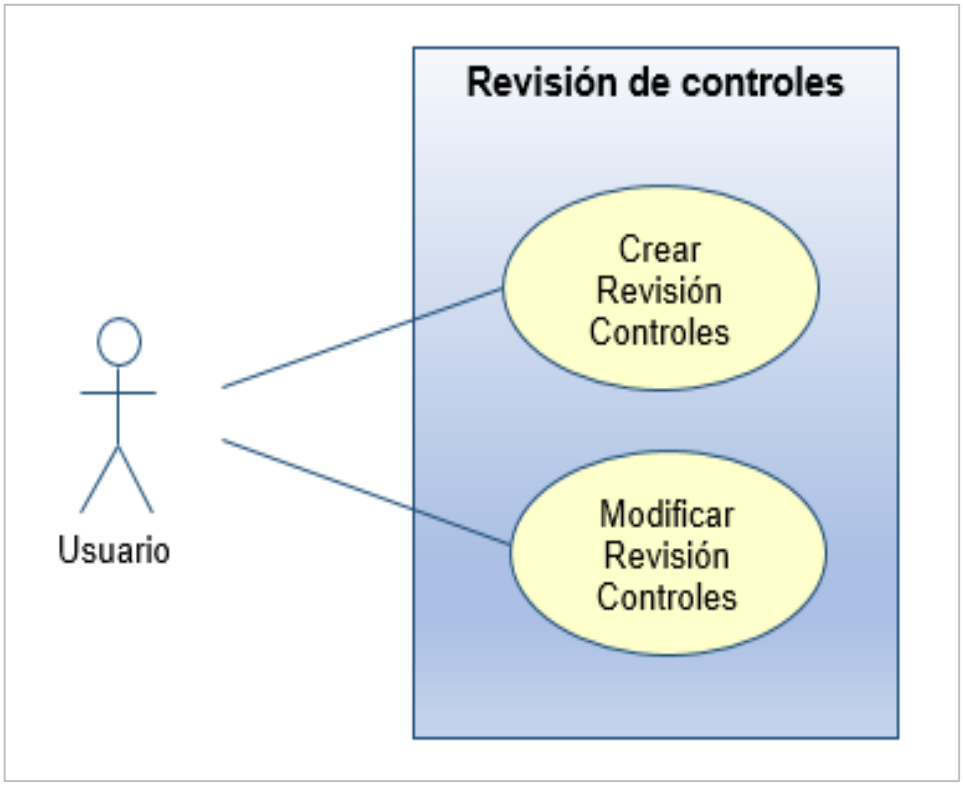
4.4. Caso de Uso: Gestión de Estándares



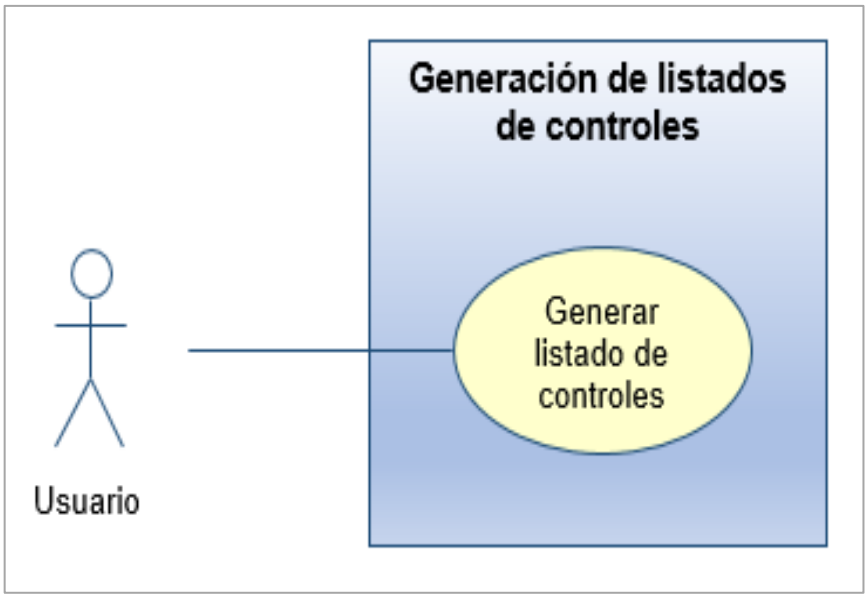
4.5. Caso de Uso: Gestión de Niveles de Madurez



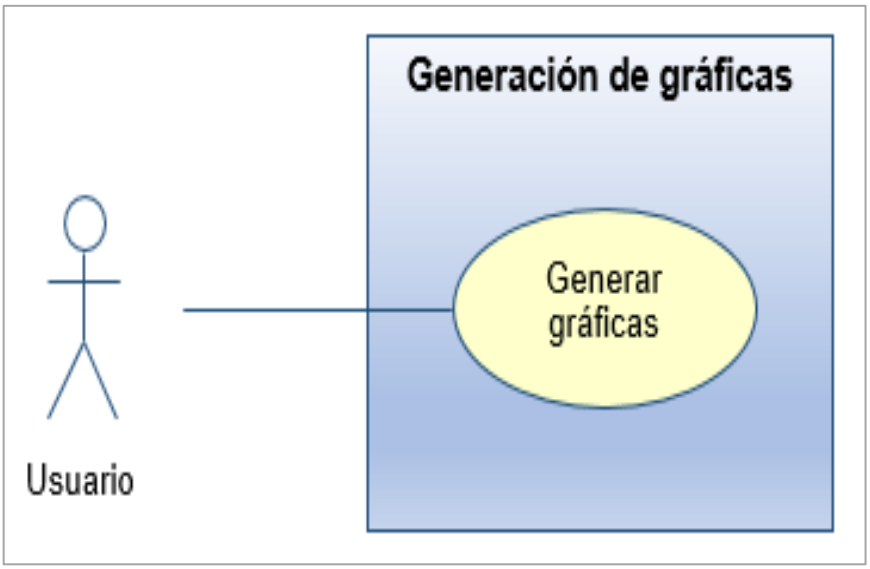
4.6. Caso de Uso: Revisión de Controles



4.7. Caso de Uso: Generación de listados de controles



4.8. Caso de Uso: Generación de gráficas



5. DIAGRAMA ENTIDAD RELACIÓN

Para revisar el modelo entidad relación del presente proyecto de titulación favor referirse al Anexo A de este documento.

6. INSTALACIÓN DE HERRAMIENTAS UTILIZADAS EN EL DESARROLLO

Para el desarrollo y/o modificación del sistema de aplicación denominado ICSystem es necesario la instalación de las siguientes herramientas:

- JDK Java
- MyEclipse 8.5
- Framework ZK
- Apache Tomcat (Ambiente Desarrollo)
- Deploy del sistema en MyEclipse
- Iniciar el servidor en MyEclipse
- Base de datos Oracle 11g Xpress Edition

6.1. JDK Java

6.1.1. Requisitos de sistema para JDK

Para la instalación de Java Development Kit, mejor conocido por sus siglas JDK, se necesitarán los siguientes requisitos del sistema:

- Mínimo un procesador Pentium 2 266 MHz.
- Mínimo de memoria 128 MB.
- Los requisitos de espacio en disco para JDK son:
    - Herramientas de desarrollo, incluyendo JavaFX SDK: 245 MB.
    - Código fuente: 27 MB.
    - Java Runtime Environment pública: 124 MB.
    - Actualización de Java: 2 MB.

6.1.2. Descargar instalador de JDK

El instalador Java Platform (JDK) puede ser descargado del sitio oficial de Oracle, a través del link www.oracle.com/technetwork/java/javase/downloads/index.html.

Se deberá dar clic sobre el botón Java Platform (JDK) 8u101 / 8u102 del producto Java SE Downloads.

Figura 1. Link de descarga del instalador Java Platform

Para comenzar la descarga del instalador Java Platform (JDK) 8u101 / 8u102 debemos seleccionar la plataforma sobre la cual correrá el JDK. Entre las plataformas soportadas para JDK se encuentran Linux, Windows, Mac y Solaris.

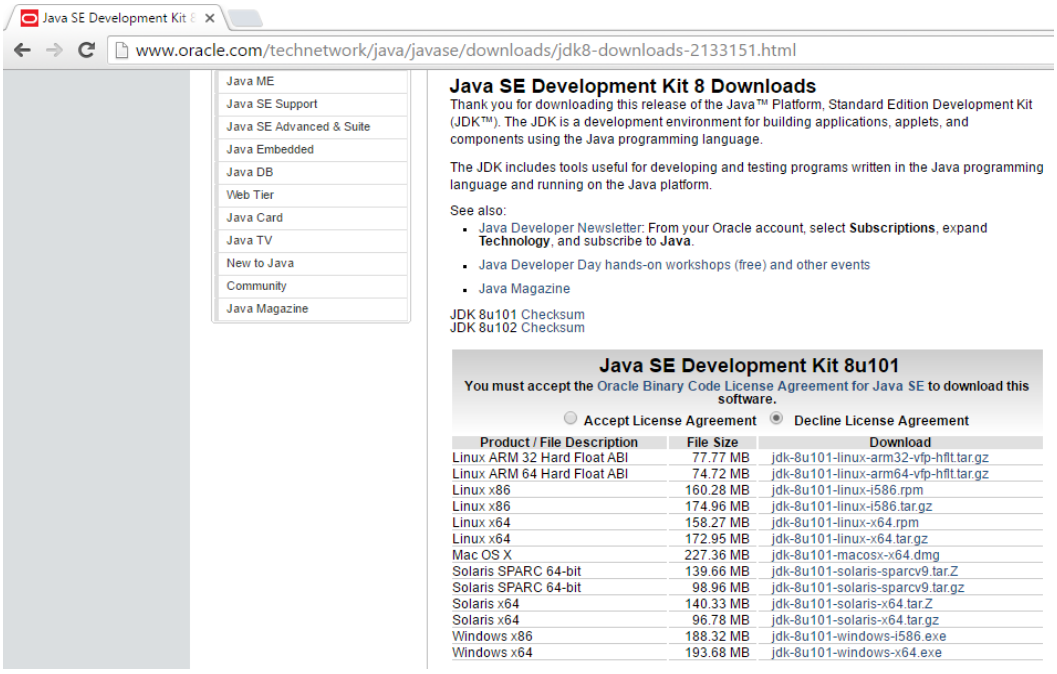
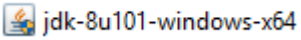


Figura 2. Selección de plataforma para JDK

Finalizada la descarga y dependiendo de la plataforma seleccionada obtendremos un fichero como el siguiente: 

6.1.3. Instalación de JDK

Para iniciar con la instalación debemos ejecutar el fichero descargado, lo cual se puede realizar de la siguiente manera:

- Doble clic sobre el fichero o
- Hacer clic derecho y seleccionar la opción Ejecutar como Administrador.

Enseguida nos aparecerá el Asistente de Instalación del JDK (Wizard). El Asistente de Instalación muestra una breve introducción de su uso y para continuar con el proceso debemos hacer clic en el botón Next >

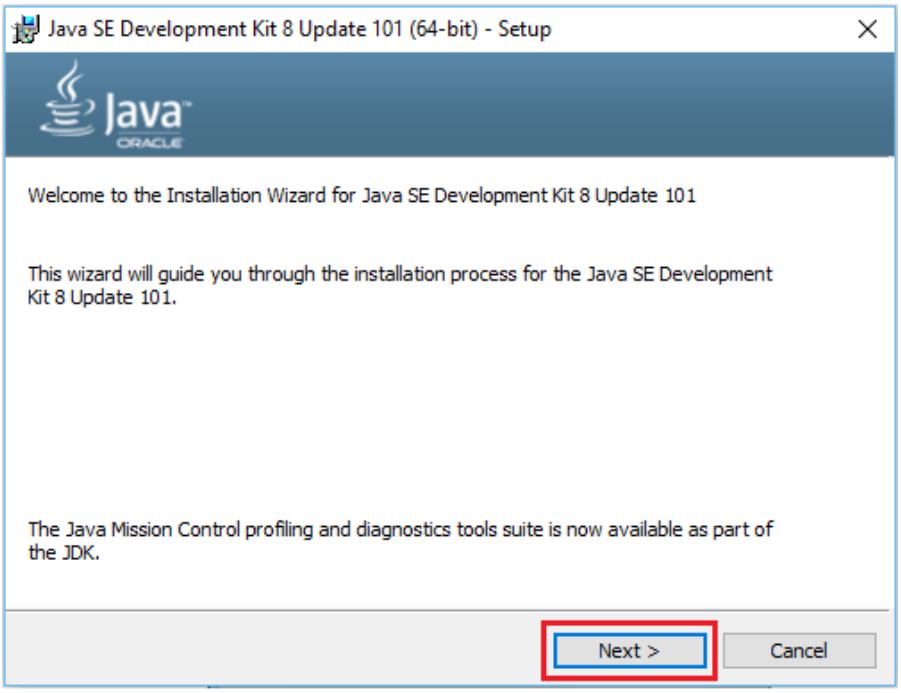


Figura 3. Asistente de instalación del JDK

Posteriormente debemos seleccionar los componentes a instalar, que son aquellos componentes que el asistente de instalación indica como default (Verificar que las casillas Development Tools - Source Code - Public JRE se encuentren con un visto), para continuar deberá hacer clic en el botón Next >

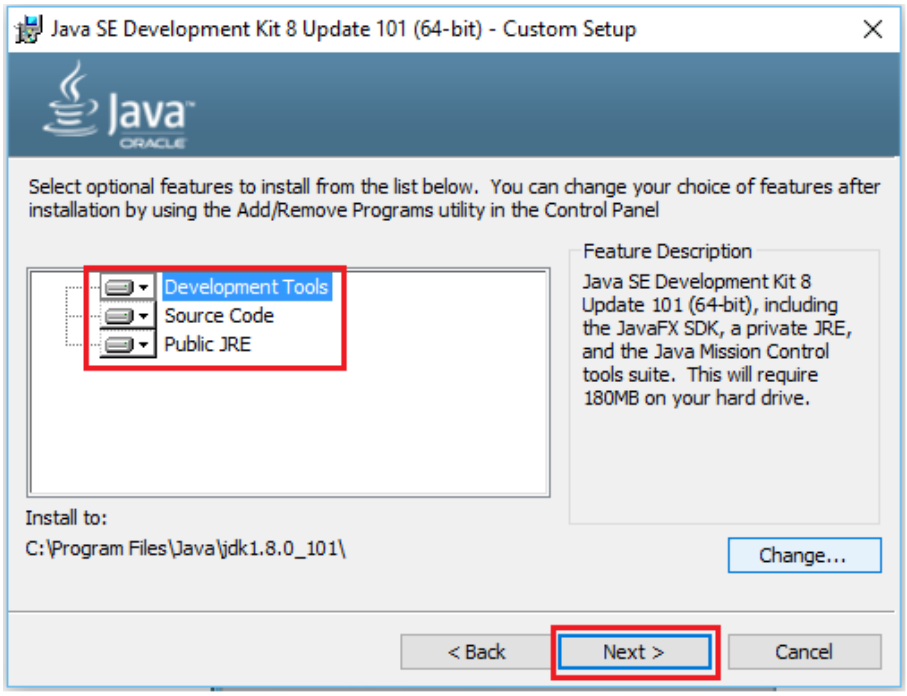


Figura 4. Selección de componentes a instalar

El Asistente de Instalación nos mostrará el avance de instalación y configuración de los componentes seleccionados.

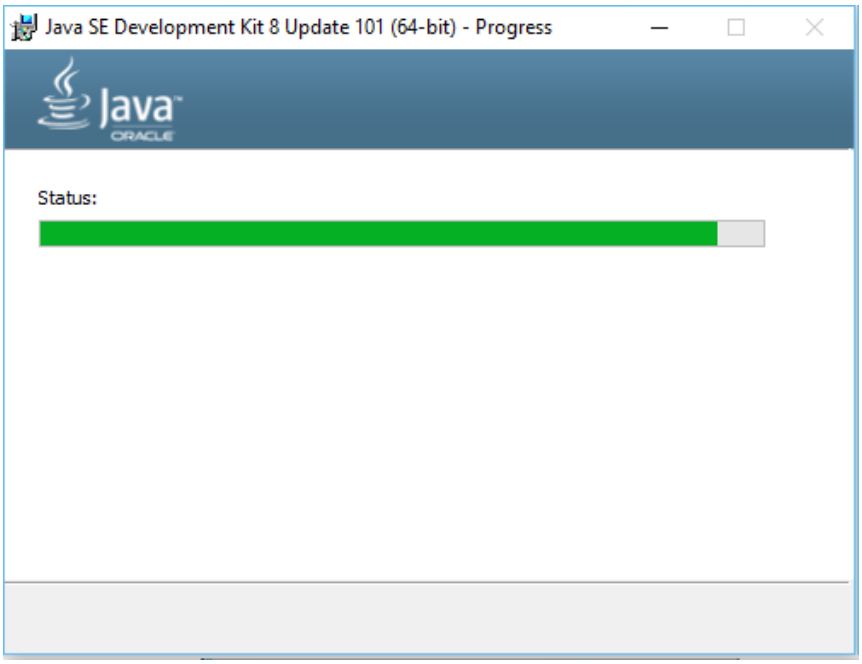


Figura 5. Avance de instalación del JDK

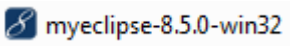
Finalmente, el Asistente de Instalación nos indica que la instalación fue ejecutada satisfactoriamente. Para cerrar el wizard dar clic en el botón Close.

Figura 6. Pantalla final de instalación del JDK

6.2. IDE MyEclipse

6.2.1. Descargar instalador de MyEclipse

MyEclipse puede ser descargado del sitio oficial de dicha herramienta a través del link https://www.genuitec.com/products/myeclipse/download/.

Se descargará un archivo de nombre 

6.2.2. Instalación de MyEclipse

Para iniciar con la instalación debemos ejecutar el fichero descargado myeclipse-8.5.0, lo cual se puede realizar de la siguiente manera:

- Doble clic sobre el fichero o
- Hacer clic derecho y seleccionar la opción Ejecutar como Administrador.

Posteriormente aparecerá una ventana indicando la extracción de los componentes necesarios para la instalación del IDE.

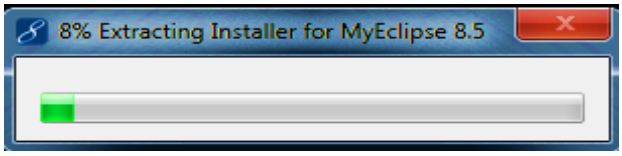


Figura 7. Extracción de componentes para instalación del IDE

Se abrirá una ventana preparando los componentes extraídos en el paso anterior.

Figura 8. Preparando componentes de instalación

Se abrirá la pantalla de bienvenida al Asistente de Instalación. Para continuar con el proceso dar click en el botón Next >

Figura 9. Asistente de instalación del IDE

El Asistente de Instalación de MyEclipse nos mostrará el avance de validación de las dependencias del software a instalar, se deberá esperar hasta que se complete la barra con el estado de la instalación.

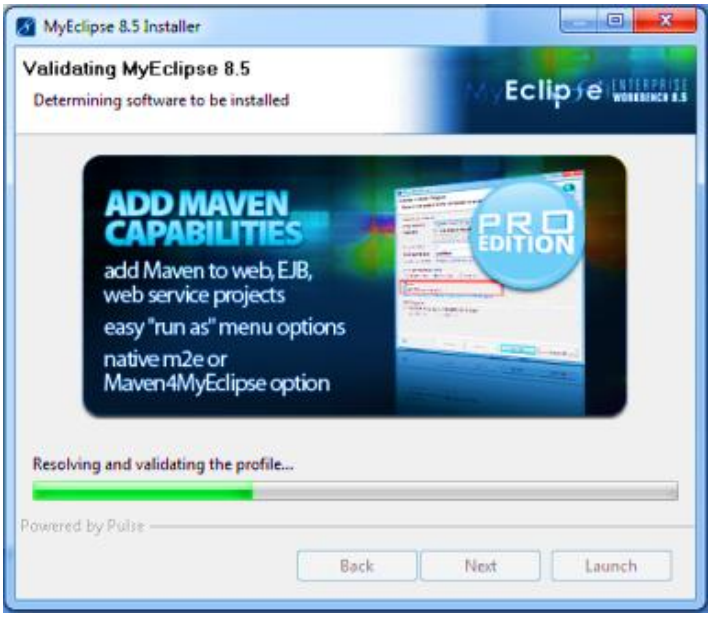


Figura 10. Validación de dependencias del IDE

Leer detenidamente y aceptar la licencia del software marcando el check box indicado I accept teh terms of the license agreement. Dar click en el botón Next.

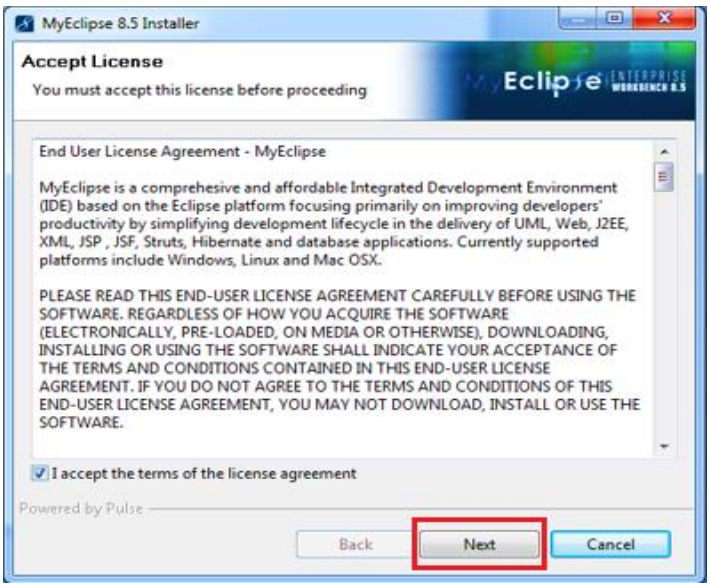


Figura 11. Aceptación de licencia del IDE

En la siguiente pantalla, elegimos la ruta donde deseamos que se instale el software y luego click en el botón Install.

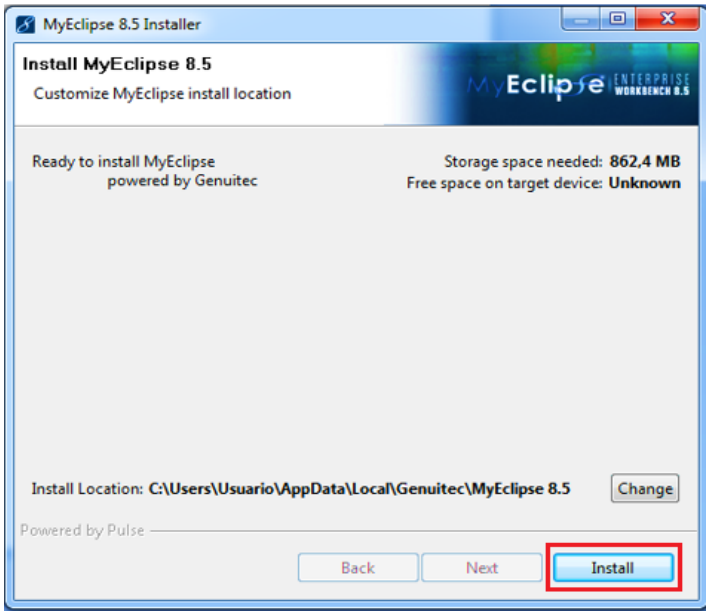


Figura 12. Ruta de instalación del IDE

El Asistente de Instalación nos mostrará el avance de instalación del IDE. Debemos esperar hasta que el estado de la instalación se haya completado.

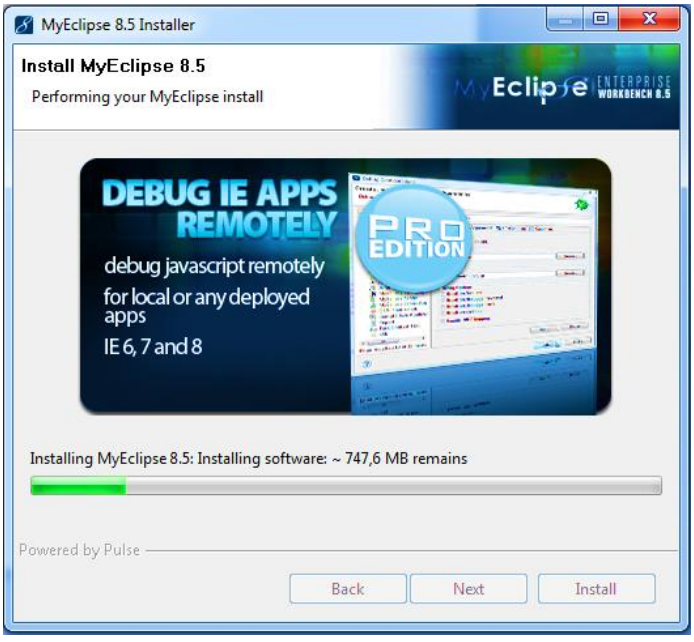


Figura 13. Proceso de instalación del IDE

El Asistente de Instalación nos preguntará la ruta de nuestro espacio de trabajo o workspace para importar y crear los proyectos desarrollados en el IDE instalado. Si deseamos que la ruta especificada sea la ruta por default de nuestros proyectos, marcamos el check box ubicado en la parte inferior de la pantalla. Continuar con el proceso haciendo clic en el botón OK.

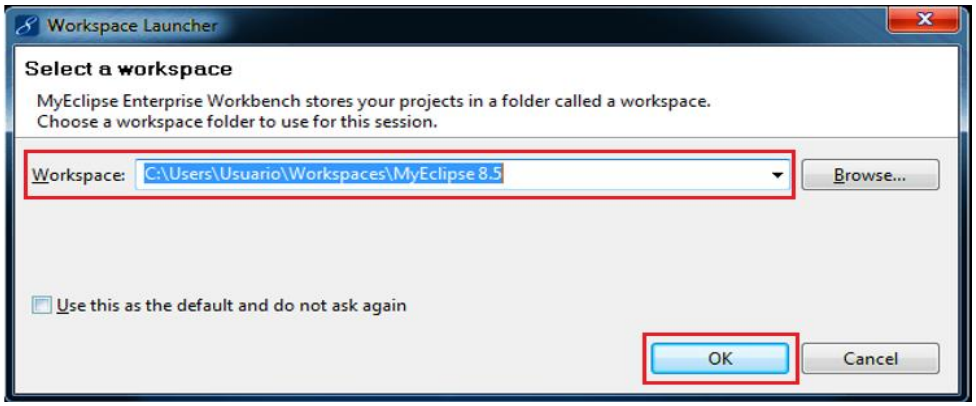


Figura 14. Asignación del espacio de trabajo

Finalmente, se abrirá el IDE MyEclipse dividido en ventanas útiles, con íconos de fácil acceso a las utilidades para el desarrollo de los proyectos.

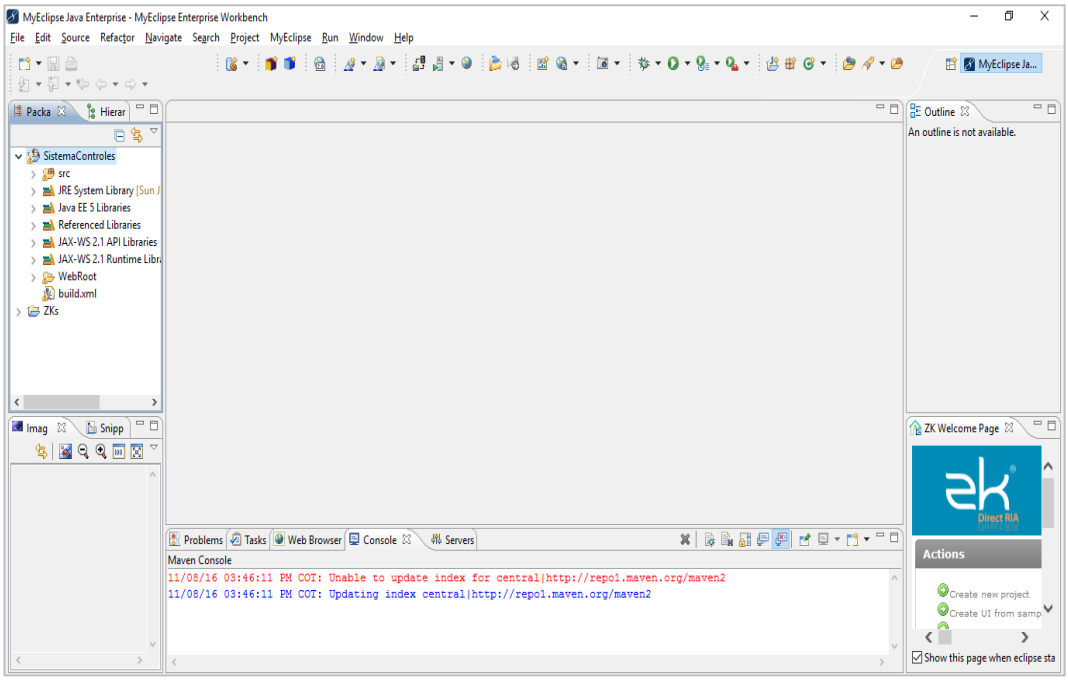
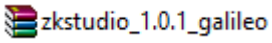


Figura 15. Ventana y opciones del IDE

6.3. Framework ZK

6.3.1. Descargar instalador ZK

El instalador ZK puede ser descargado directamente del sitio oficial https://www.zkoss.org, para la descarga solo se necesita registrarse en la página.

La versión que escogeremos es la indicada para Eclipse Galileo. Una vez descargado ZK, obtendremos un fichero con el nombre 

6.3.2. Instalación de ZK

Para la instalación del plugin en el IDE, en la ventana principal de MyEclipse seleccionar la opción de menú:

- MyEclipse
  - MyEclipse Configuration Center.

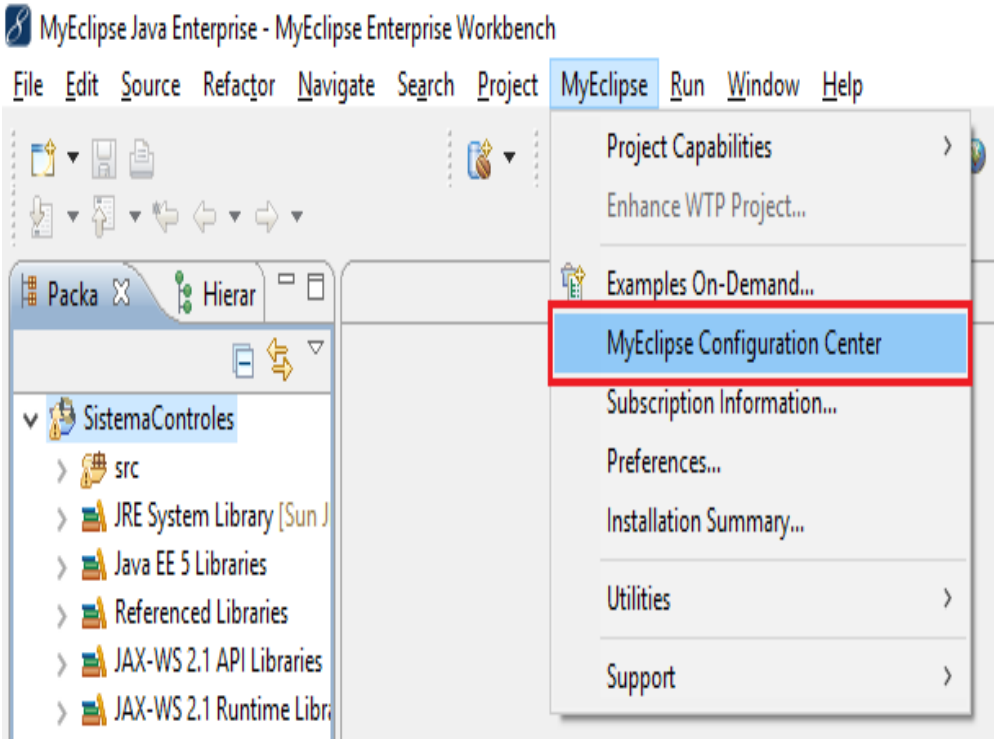


Figura 16. Centro de configuración de MyEclipse

Inmediatamente se muestra una nueva ventana en donde se deberá elegir la pestaña Software.

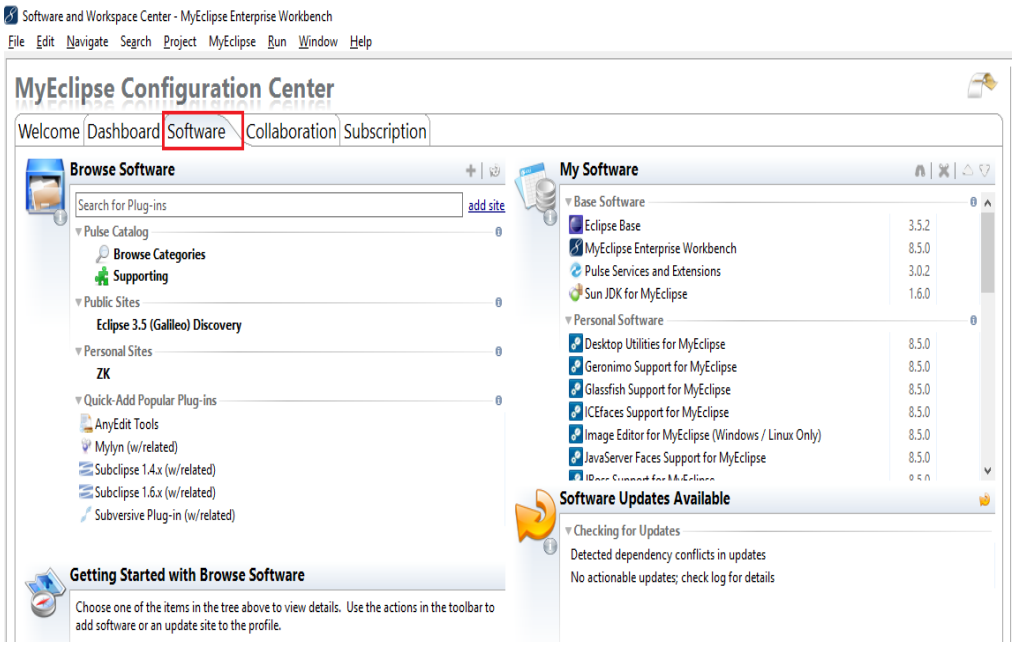


Figura 17. Pestaña Software del Centro de Configuración MyEclipse

Posteriormente dar clic en la opción add site y se mostrará una ventana que debe completarse de acuerdo a lo siguiente:

- En la caja de texto Name escribimos un nombre para identificar el plugin a instalar.
- En la caja de texto URL aparece la ruta del plugin de ZK a instalar.

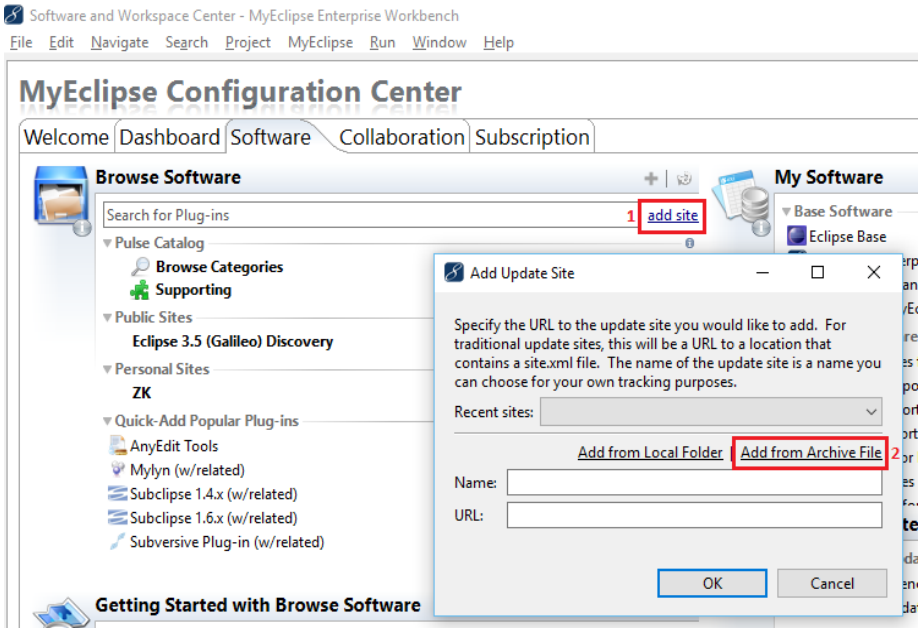


Figura 18. Añadir plugin de ZK

Luego de registrar los datos anteriores se deberá dar click en el botón OK para iniciar la instalación del plugin de ZK en el IDE MyEclipse.

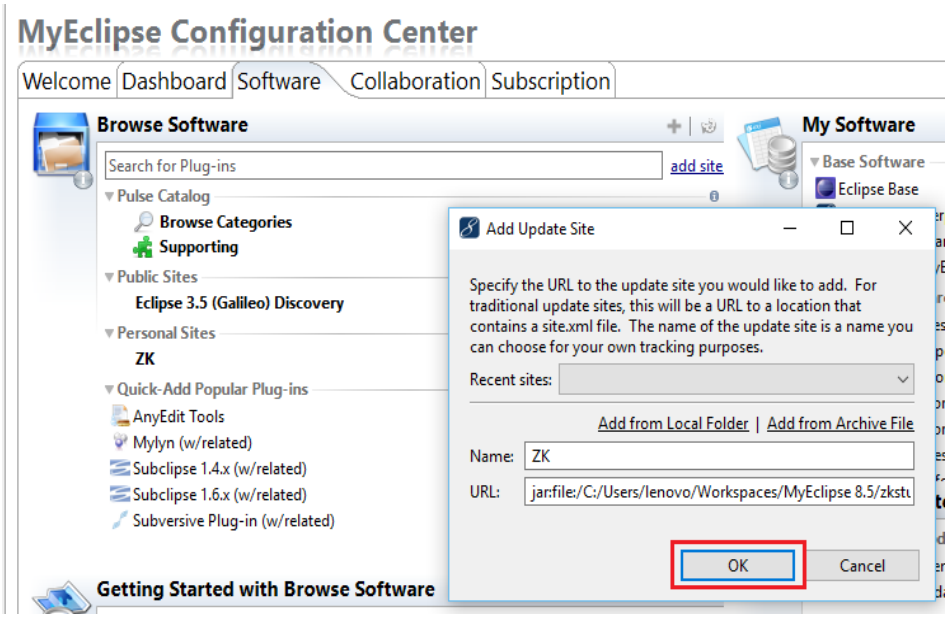


Figura 19. Instalación del plugin de ZK

6.4. Apache Tomcat

6.4.1. Descargar instalador de Apache

El servidor de aplicaciones para el ambiente de desarrollo puede ser descargado directamente del sitio oficial http://tomcat.apache.org.

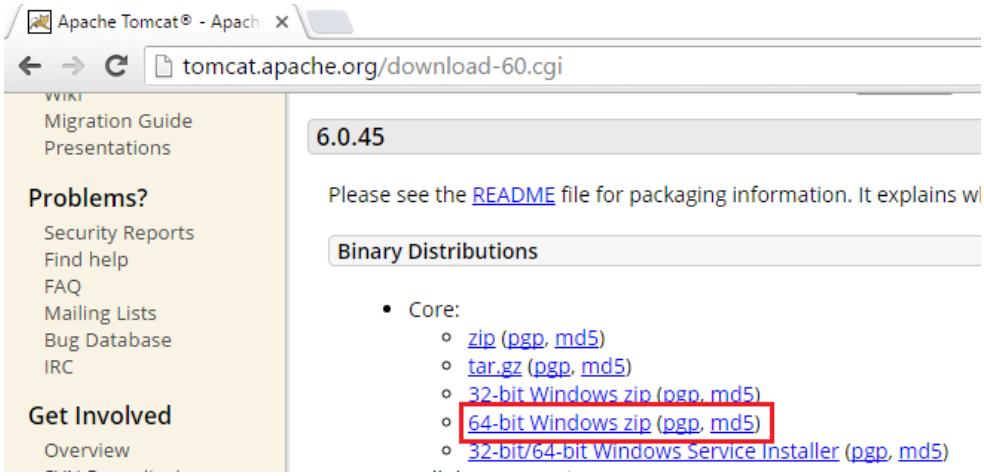
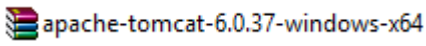


Figura 20. Descarga del servidor Apache

Una vez descargado Apache Tomcat, obtendremos un fichero con el nombre



6.4.2. Instalación de Apache

Extraer el contenido del zipeado en la ruta escogida para alojar el servidor web. Luego de descomprimir el fichero se creará una carpeta con los archivos necesarios para el funcionamiento del servidor de aplicaciones.

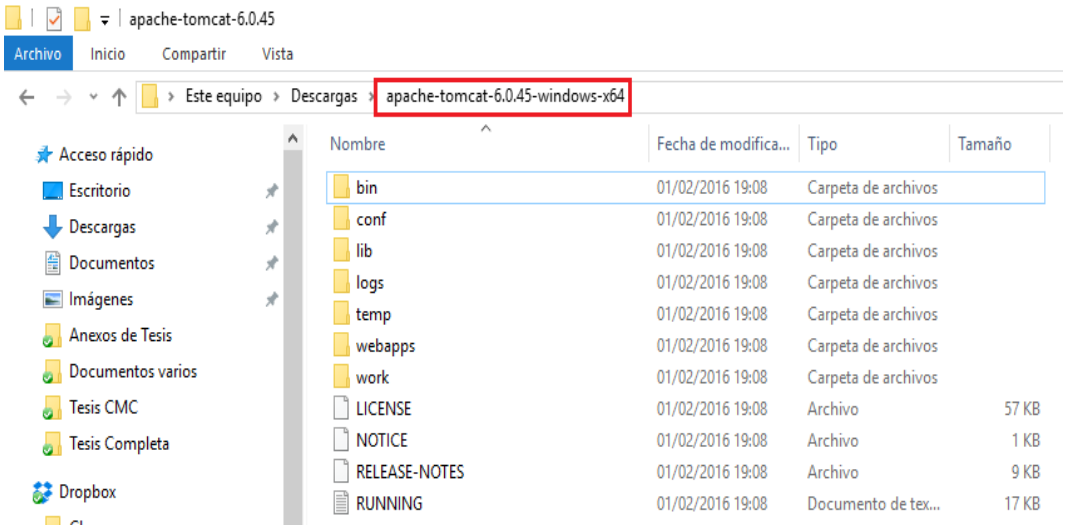


Figura 21. Instalación de Apache Tomcat

Para las conexiones con la base de datos debemos seguir los siguientes pasos:

- Crear un datasource con los parámetros correspondientes a la conexión. El datasource se lo creará en el archivo de apache context.xml ubicado en la ruta apache-tomcat-6.0.45-windows-x64\conf

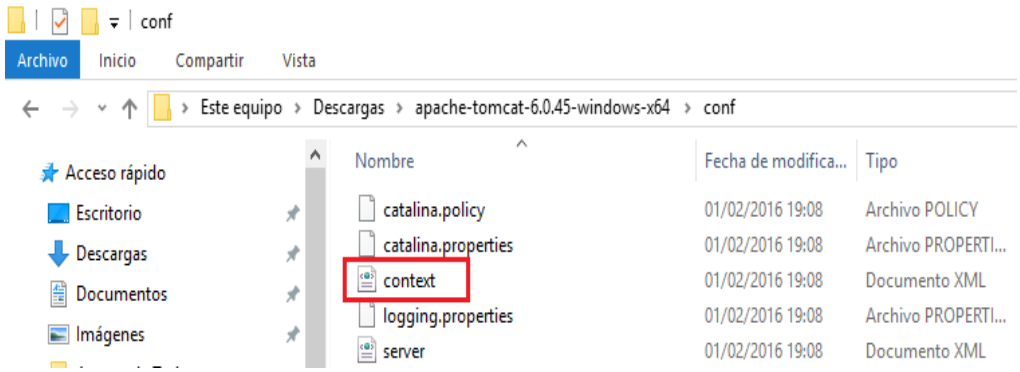


Figura 22. Configuración de Tomcat en MyEclipse

- Editar el archivo context.uml y dentro de la etiqueta <Context> </Context> ubicaremos lo siguiente:

```
<Resource name="jdbc/SistemaControles"
          auth="Container"
          type="oracle.jdbc.pool.OracleDataSource"
          driverClassName="oracle.jdbc.OracleDriver"
          factory="oracle.jdbc.pool.OracleDataSourceFactory"
          url="jdbc:oracle:thin:@localhost:1521:xe"
          user="sistema_controles"
          password="sistema_controles"
          maxActive="20"
          maxIdle="10"
          maxWait="-1"
/>
```

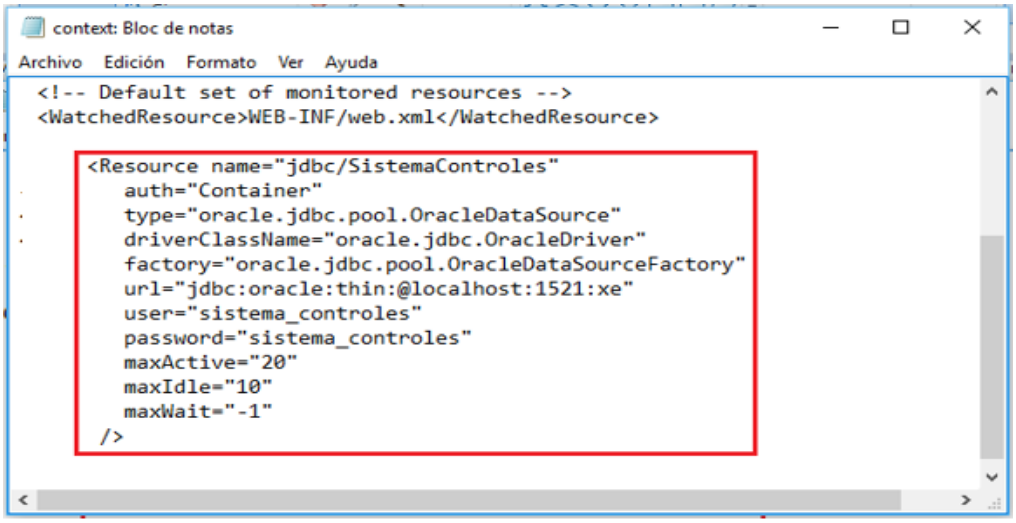


Figura 23. Editando el archivo context.uml

Parámetro	Descripción del Parámetro
Name	Nombre con el que identificaremos el datasource.
Auth	Se utiliza para controlar los recursos en la seguridad.
Type	Define el tipo de datasource.
DriverClassName	Nombre completo de la clase Java del controlador JDBC que se utilizará.
Factory	Crea y configure la propia agrupación de conexiones.

Parámetro	Descripción del Parámetro
URL	URL de conexión que se pasa a nuestro conector de JDBC.
User	Usuario para conectarse a la base de datos.
Password	Contraseña del usuario a conectarse con la base de datos.
MaxActive	Número máximo de conexiones de base de datos en el pool. Si se establece en -1 indica conexiones sin límite.
MaxIdle	El número máximo de conexiones de base de inactividad para conservar en el pool. Si se establece en -1 indica sin límite.
MaxWait	Tiempo máximo en milisegundos para esperar que una conexión de base de datos esté disponible. Se establece en -1 para esperar indefinidamente.

Iniciar MyEclipse para configurar el servidor y deployar el sistema. Abrimos MyEclipse y en la barra de menú escogemos la opción:

- MyEclipse
  - Preferences.

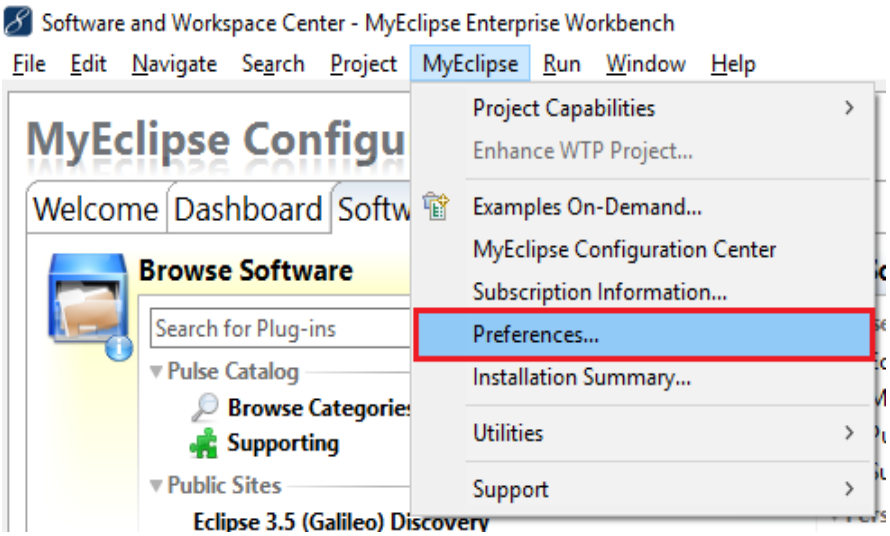


Figura 24. Iniciar configuración de Apache

Se abrirá una nueva ventana donde se deberá seleccionar las opciones: MyEclipse- Servers – Tomcat. Posteriormente dar clic en la opción Configure Tomcat 6.x

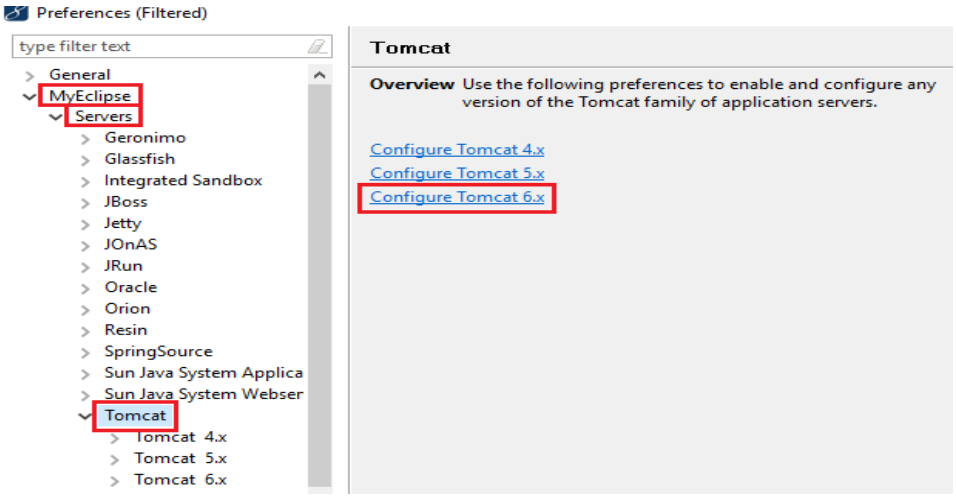


Figura 25. Configuración de Tomcat

Inmediatamente se abrirá una nueva ventana para indicar la ruta del servidor de aplicaciones, en este caso Tomcat 6. Habilitamos el servidor marcando la opción Enable y buscamos su ubicación haciendo click en el primer botón Browse… Las demás ubicaciones se setean solas.

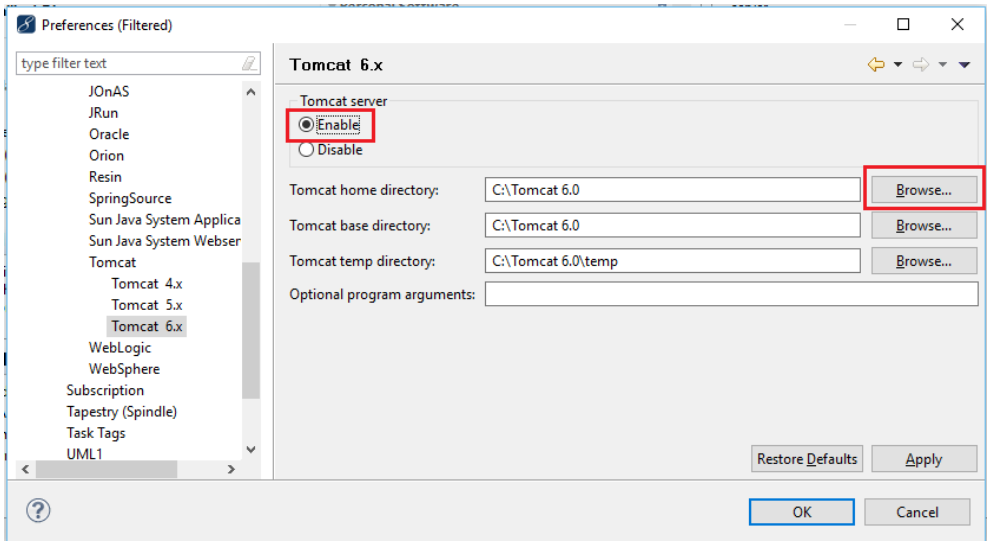


Figura 26. Habilitando el servidor Apache

Hacemos click en la opción JDK y escogemos la versión correspondiente en este caso versión 6, además añadimos ciertos argumentos para el mejor rendimiento de la Java VM. Dar clic en el botón OK.

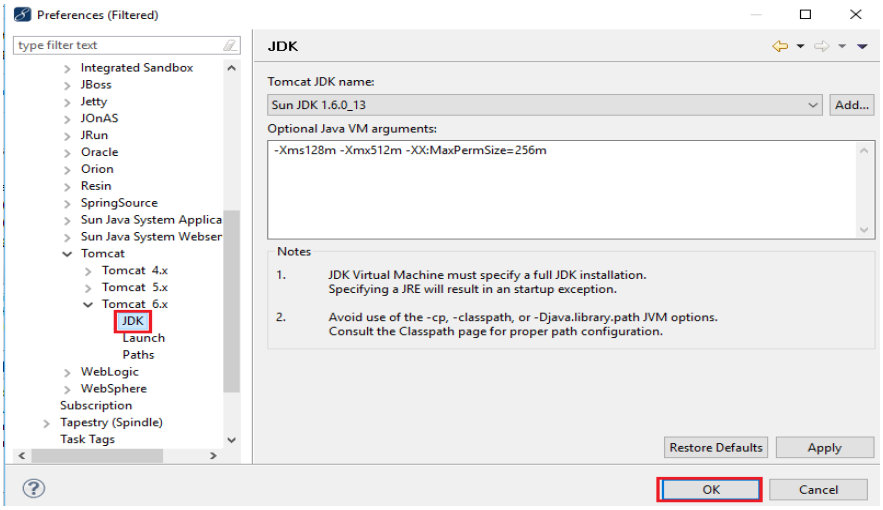


Figura 27. Argumentos JVM en JDK de MyEclipse

Hasta este punto hemos configurado el servidor de aplicaciones Tomcat 6 para deployar el sistema desarrollado. El siguiente paso será importar el proyecto desarrollado para darle mantenimiento o sólo para deployarlo y podernos conectar a el de cualquier pc que se encuentre dentro de la red donde se encuentra instalado el servidor. Para esto hacemos click en la opción File – Import de la barra de menú de MyEclipse.

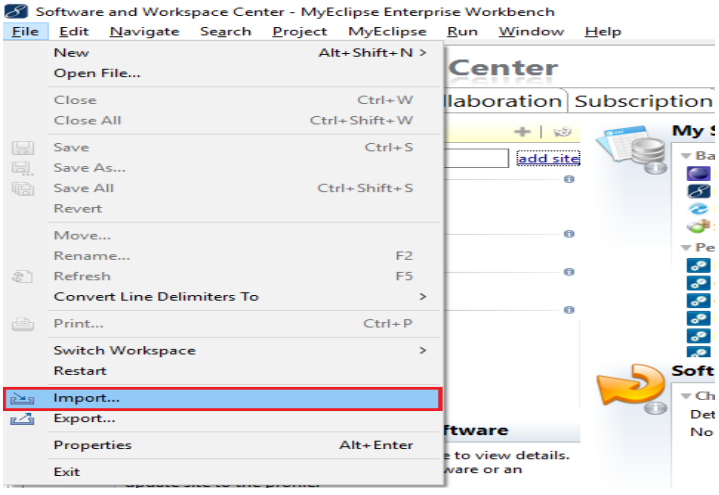


Figura 28. Importar proyecto - Paso 1

Se abrirá una nueva ventana en donde se deberá elegir la opción General – Existing Projects into Workspace y dar clic en el botón Next.

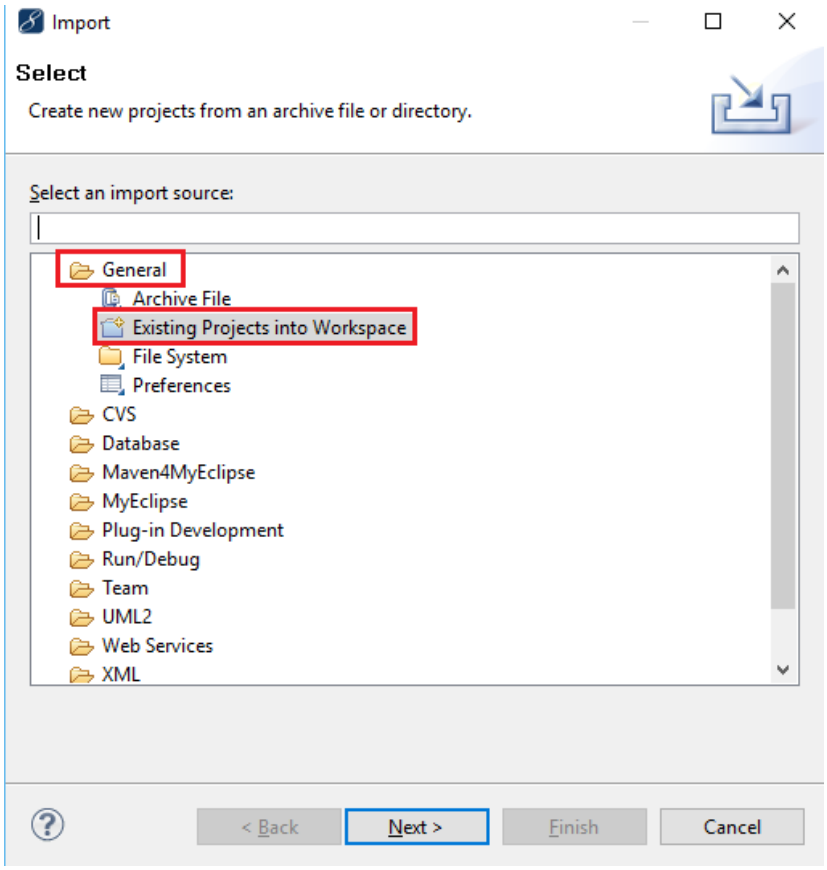


Figura 29. Importar proyecto - Paso 2

Luego escogeremos el proyecto a importar haciendo click en el botón Browse. Se abrirá una ventana para permitirnos escoger el proyecto que deseamos importar.

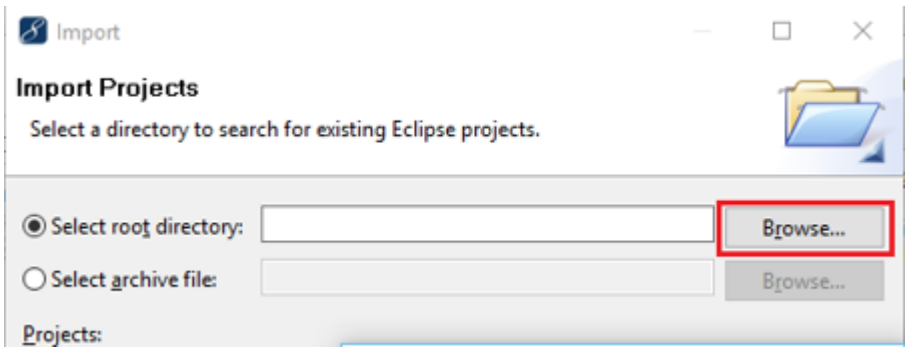


Figura 30. Seleccionar proyecto a importarse

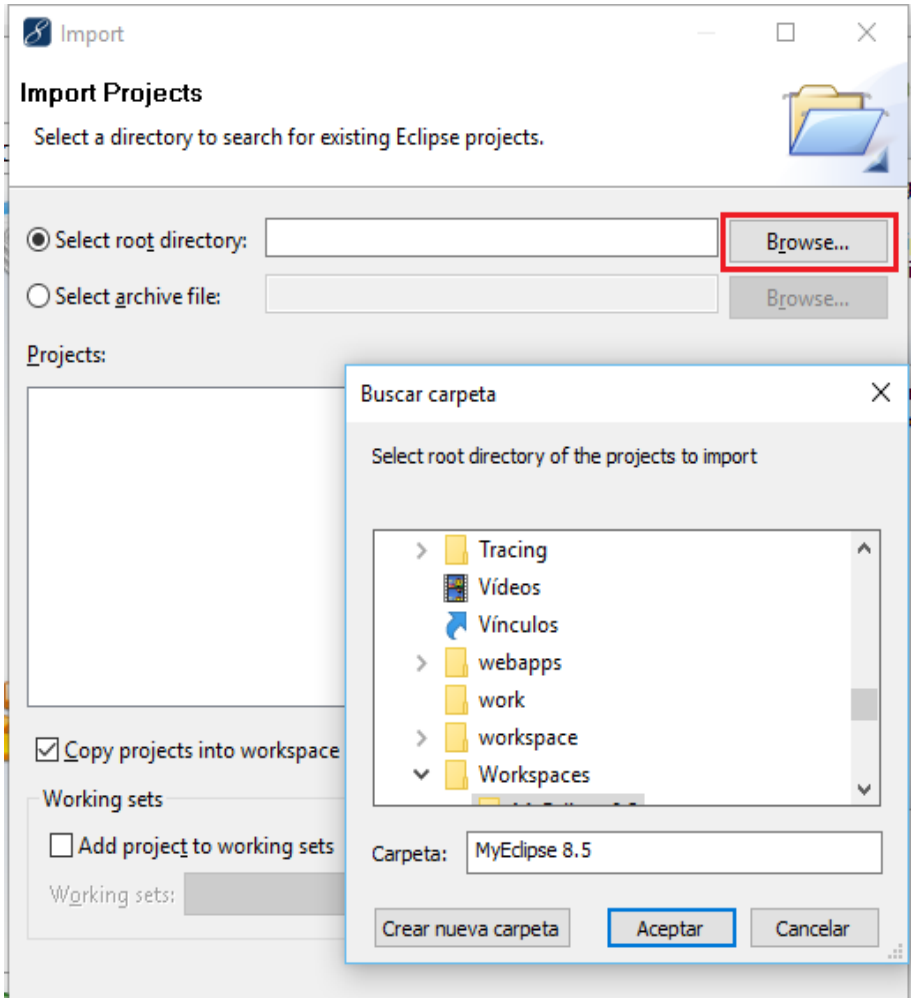


Figura 31. Copiar proyecto en espacio de trabajo

Luego indicaremos que el proyecto se copie en el espacio de trabajo definido en pasos anteriores marcando el checkbox Copy projects into workspace para que el proyecto esté disponible siempre que iniciemos el IDE.

Para finalizar hacemos click en Finish. Esperamos unos segundos hasta que el proceso de importación termine de copiar todos los archivos del proyecto en el workspace.

6.5. Deploy del sistema en MyEclipse

Para deployar el sistema mediante el IDE MyEclipse debemos realizar los siguientes pasos:

Hacemos click en el botón Deploy de la barra de herramientas.

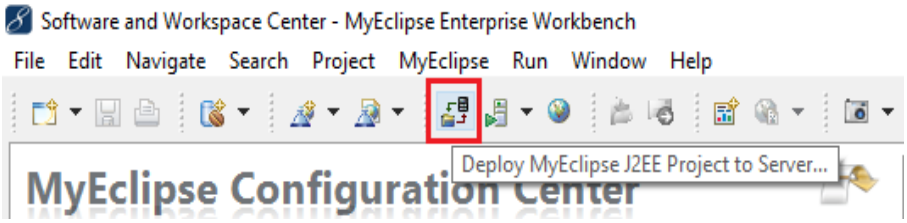


Figura 32. Deploy del sistema en MyEclipse

Hacemos click en el botón el botón Add para indicar el servidor en el cual vamos a deployar la aplicación. Luego dar click en el botón Finish.

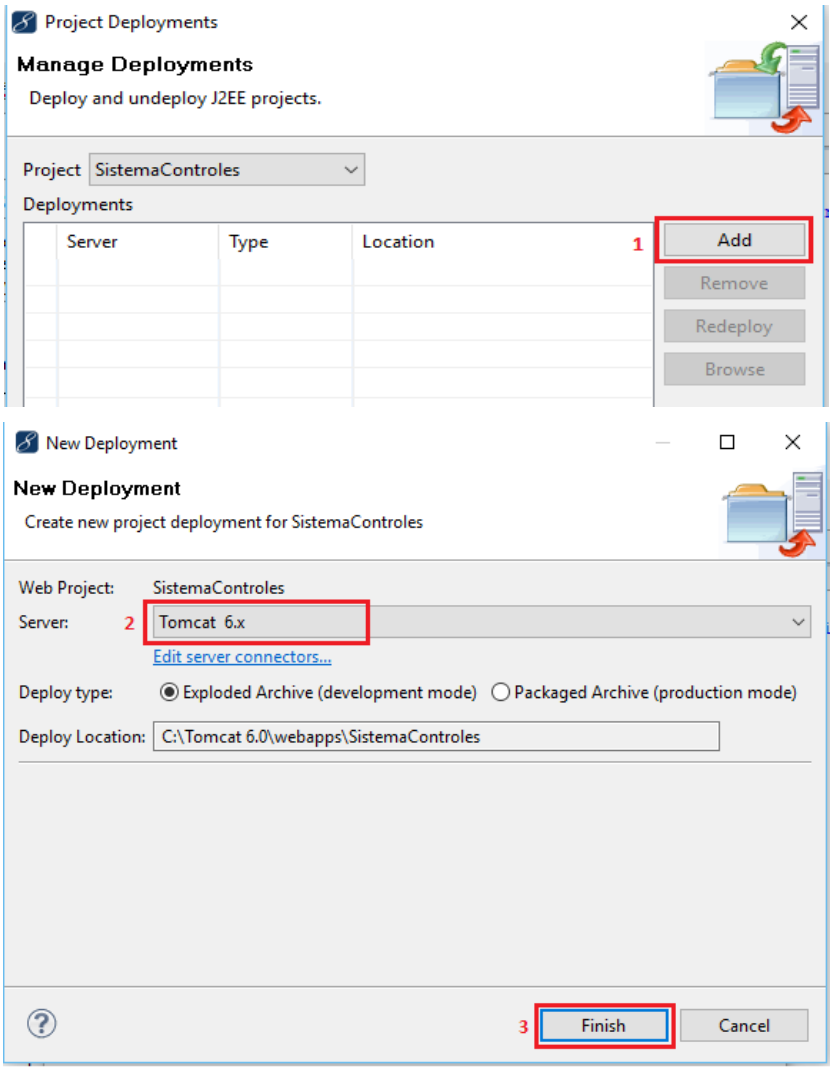


Figura 33. Añadir servidor para deployar la aplicación

Finalmente debemos dar click en el botón OK.

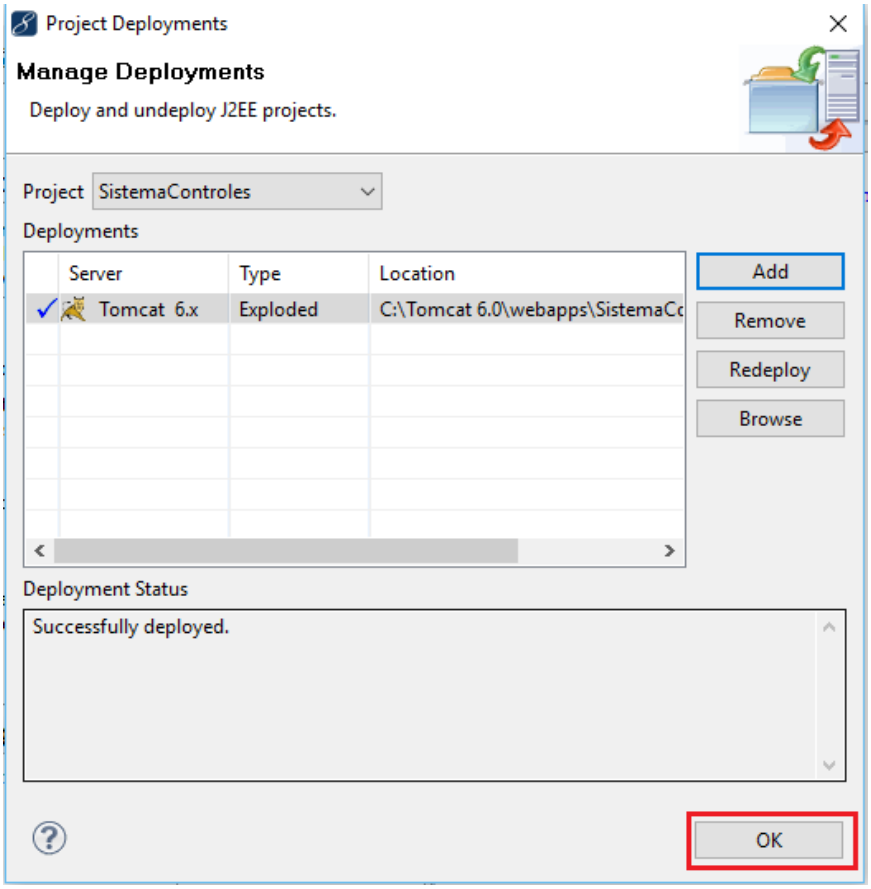


Figura 34. Deploy del servidor finalizado

6.6. Iniciar el servidor en MyEclipse

Para iniciar el servidor sistema mediante el IDE MyEclipse debemos realizar los siguientes pasos:

Dar click en la flecha del botón Stop/Restart/Start de la barra de herramientas.

Figura 35. Iniciar servidor en MyEclipse

Elegimos el servidor configurado y hacemos click en Start.

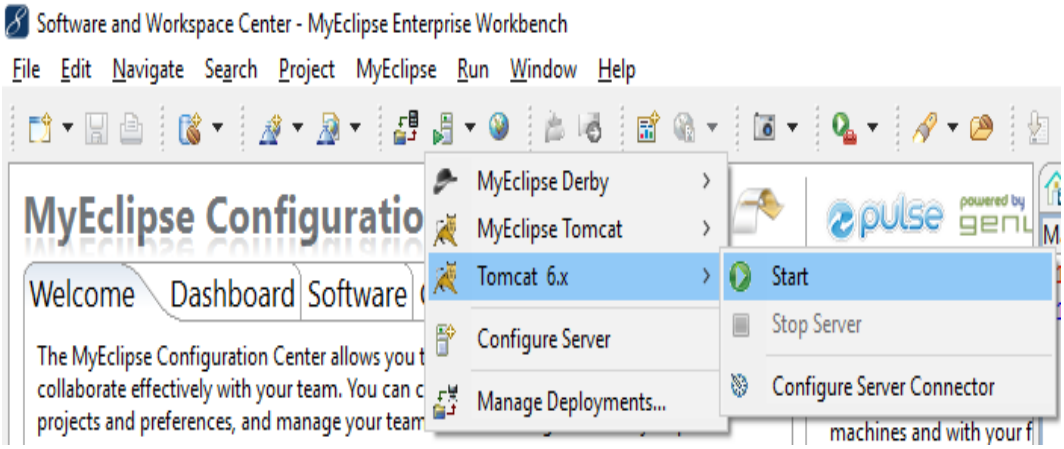


Figura 36. Seleccionar el servidor Tomcat

Como último paso abriremos un navegador web como Google Chrome y accederemos a la ruta: http://direccion_ip:puerto:/proyecto ejemplo: http://192.168.0.1:8081/ICSystem y se presentará la pantalla inicial del sistema desarrollado.

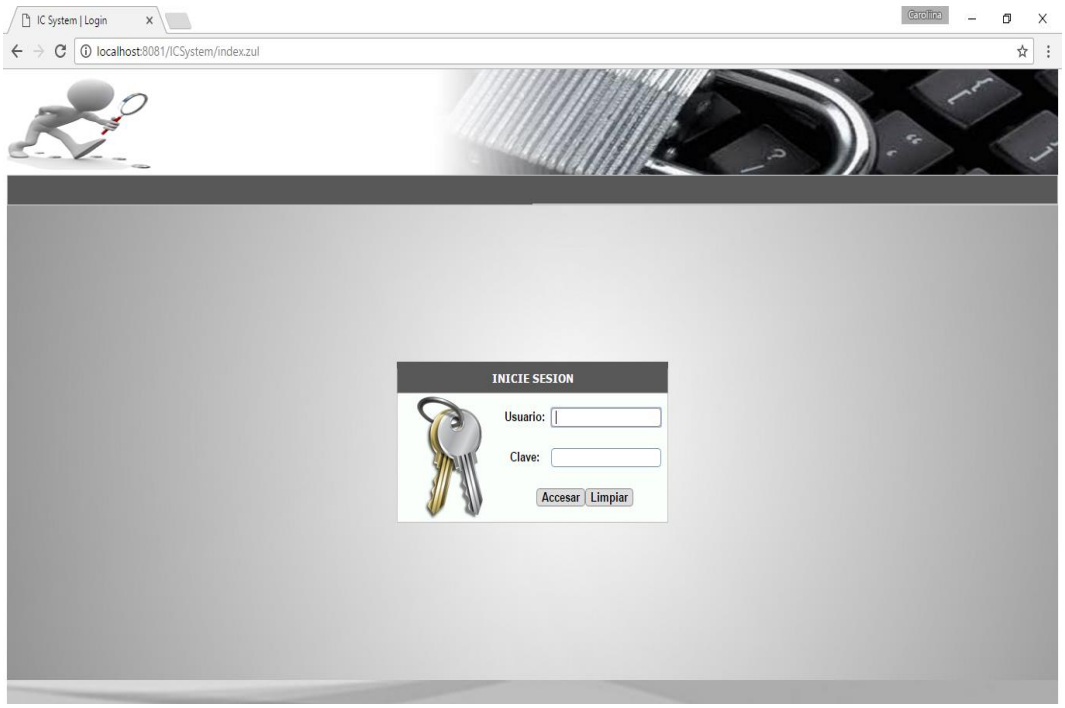


Figura 37. Pantalla inicial de la aplicación ICSystem

6.7. Base de Datos Oracle

6.7.1. Requisitos de sistema para Oracle

Para la instalación de Oracle 11g Xpress Edition se necesitarán los siguientes requisitos del sistema:

- Un mínimo de memoria RAM de 256 MB, 512 MB recomendado para la base de datos Oracle XE.
- Un mínimo de 1.5 GB de espacio en disco y 125 MB para archivos temporales de instalación.
- Protocolos soportados: IPC, TCP/IP, Named Pipes, SDP, TCP/IP con SSL.

6.7.2. Descargar instalador de Oracle

Oracle Database Express Edition 11g Release 2 puede ser descargado del sitio oficial de Oracle https://www.oracle.com/index.html.

Nos posicionamos sobre la opción Downloads e inmeditamente seleccionamos la opción Oracle Database 11g Express Edition.

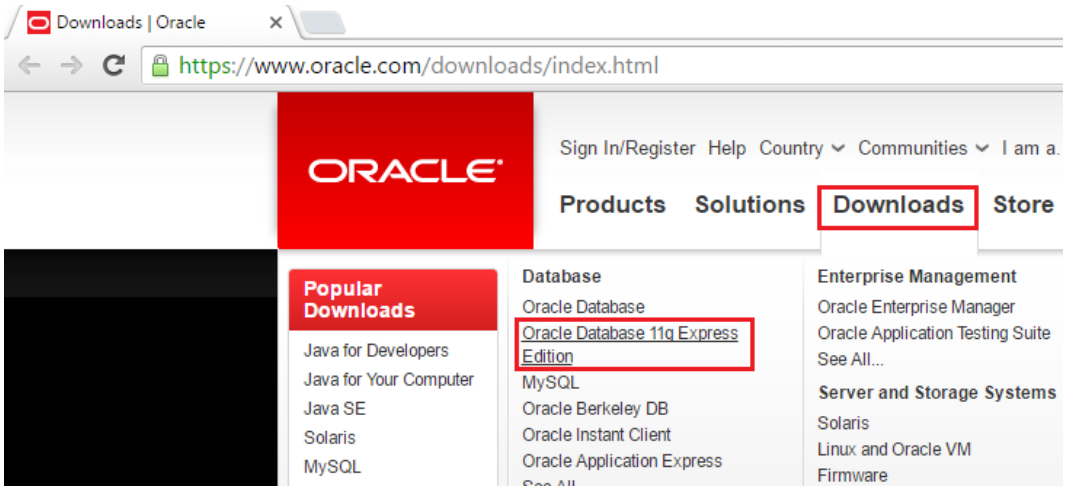


Figura 38. Link de descarga de Oracle

Nos aparecerá una nueva pantalla y para iniciar la descarga del instalador debemos seleccionar la plataforma sobre la cual correrá la base de datos. Es importante considerar que para poder realizar la descarga de la base de datos se debe aceptar el acuerdo de licencia y tener una cuenta de usuario en Oracle.

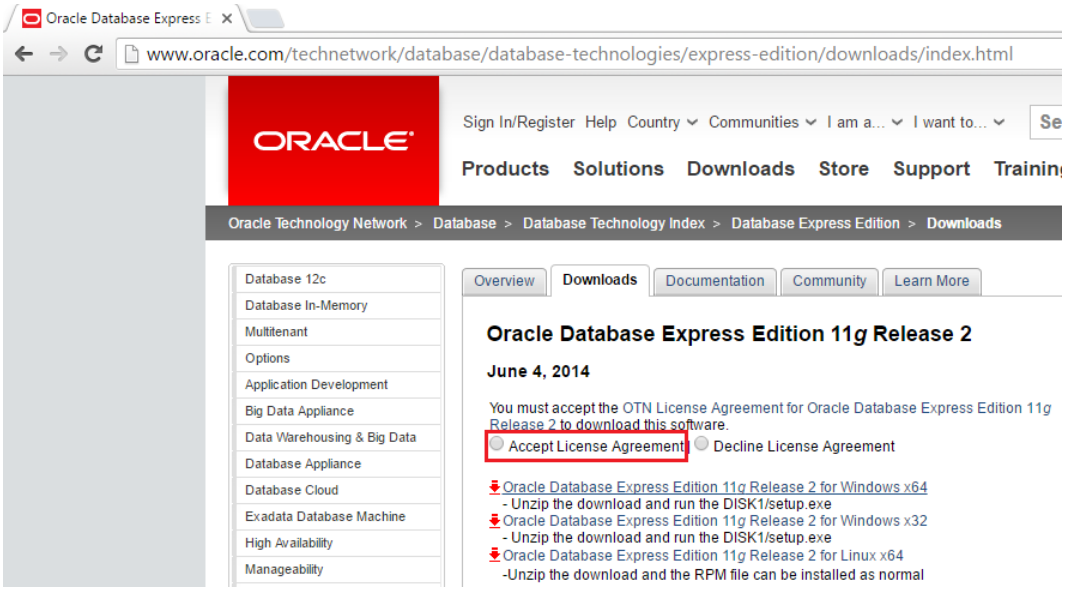


Figura 39. Aceptación de licencia de la base de datos

Finalizada la descarga y dependiendo de la plataforma seleccionada obtendremos un fichero como el siguiente: OracleXE112_Win64

Por último, debemos descomprimir el fichero antes mencionado.

6.7.3. Instalación de Oracle

Pulsaremos el botón derecho del ratón sobre "setup.exe" y seleccionaremos "Ejecutar como administrador" en el menú emergente.

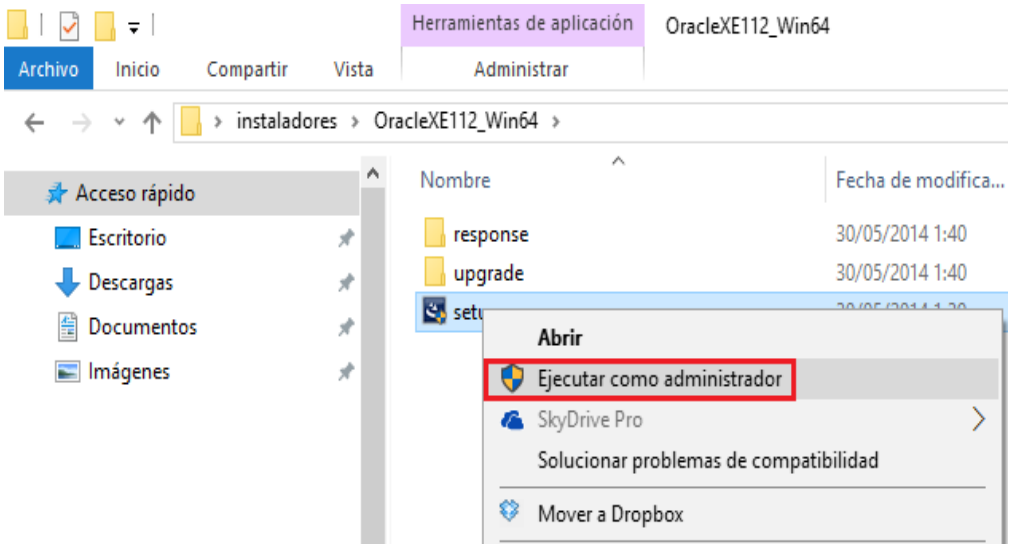


Figura 40. Ejecución del instalador de Oracle

Nos aparecerá una ventana que pedirá confirmación para ejecutar el programa de instalación de Oracle Database, daremos click sobre la opción Sí.

Aparece la pantalla Oracle Universal Installer en donde se iniciará la verificación de los requerimientos necesarios para la instalación de Oracle. Esperar hasta que se termine la verificación.

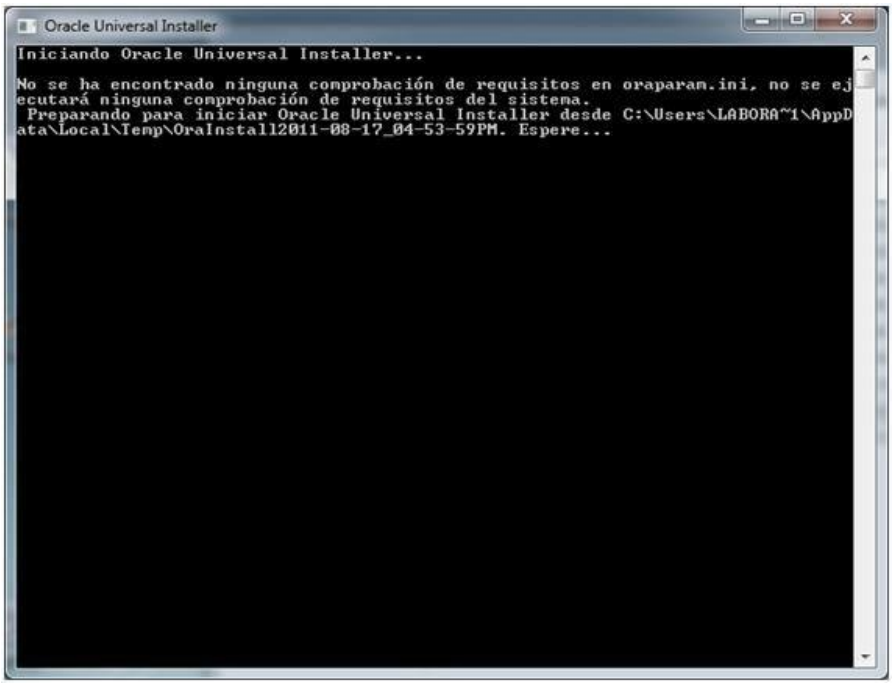


Figura 41. Comprobación de requisitos iniciales

Para la instalación de la base de datos existen dos métodos, los cuales detallamos:

- Instalación Básica: seleccionaremos este método de instalación si deseamos instalar rápidamente Oracle Database 11g. Este método necesita una mínima intervención del usuario. Seleccionando este método también se puede especificar si se desea crear una base de datos de uso general con el esquema SAMPLE y el tablespace EXAMPLE.
- Instalación Avanzada: este método de instalación sirve para cualquiera de las siguientes tareas:
    - Realizar una instalación personalizada del software o seleccionar una configuración diferente de la base de datos.

- Instalar o actualizar Oracle Real Application Clusters.
- Actualizar una base de datos existente.
- Seleccionar un juego de caracteres de la base de datos o idiomas de producto diferentes.
- Crear una base de datos en un sistema de archivos que sea distinto del sistema en el que se copia el software.
- Configurar Gestión Automática de Almacenamiento.
- Especificar contraseñas diferentes para esquemas administrativos.
- Configurar copias de seguridad automáticas o notificaciones de Oracle Enterprise Manager.

Para este caso, seleccionaremos la opción Instalación Avanzada y pulsaremos el botón Siguiente.

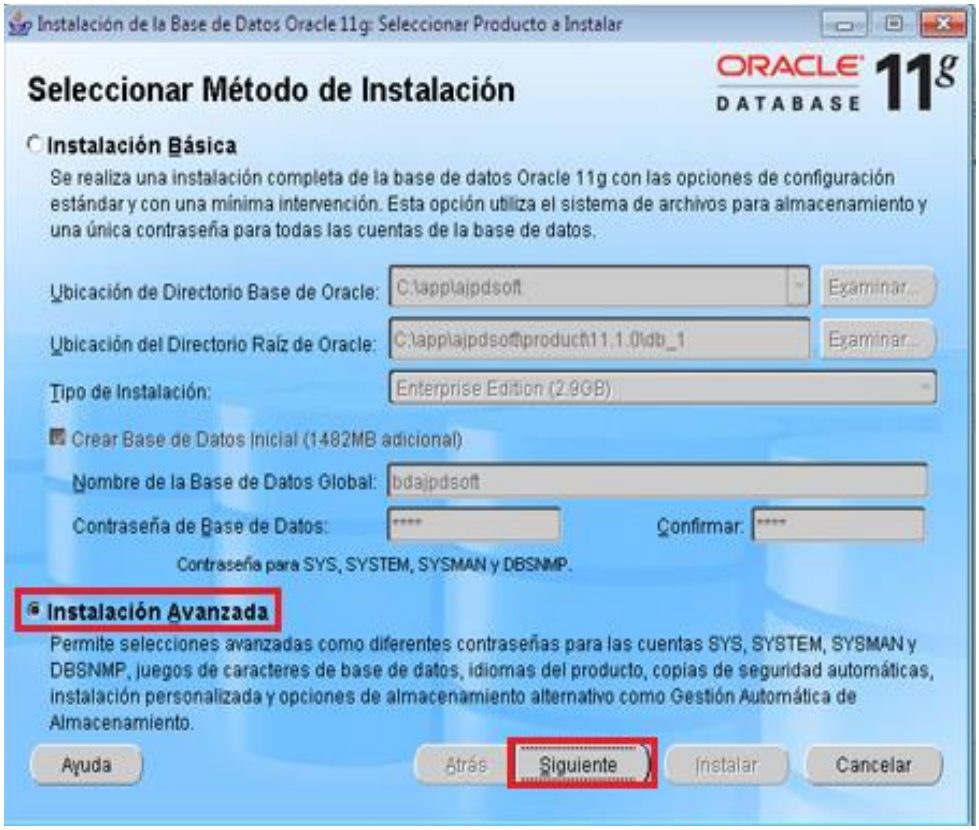


Figura 42. Método de instalación de Oracle

Escogemos la opción de Standard Edition y pulsaremos el botón Siguiente.

Figura 43. Tipo de instalación de Oracle

Especificar en "Directorio Base de Oracle" la ubicación en la que deseemos almacenar todos los archivos de software de Oracle y relacionados con la configuración. En Ubicación del Software especificar el nombre y la ubicación del directorio raíz de Oracle en el que deseemos instalar el producto. Pulsaremos el botón Siguiente.

Figura 44. Especificación del Directorio Raíz de Oracle

La siguiente pantalla se encarga de comprobar los requisitos específicos del producto a instalar e irá marcando cada checkbox si los requisitos son correctos, caso contrario no lo marcará y mostrará un mensaje en el campo Estado. Si todo resulta correcto hacemos clic en la opción Siguiente.

Figura 45. Comprobación de Requisitos de Oracle

A continuación Oracle Universal Installer nos permite elegir entre varias posibilidades de configuración:

- Crear Base de Datos: esta opción crea una base de datos con la configuración de Uso General/Procesamiento de Transacciones, Almacén de Datos o Avanzada.
- Configurar Gestión Automática de Almacenamiento (ASM): esta opción instala sólo Gestión Automática de Almacenamiento en un directorio raíz de Oracle distinto. Si es necesario, también puede proporcionar una contraseña SYS de ASM.
- Instalar sólo Software: esta opción instala sólo el software de la base de datos Oracle. Se podrá configurar la base de datos más tarde.

Seleccionaremos "Instalar sólo Software", puesto que crearemos la base de datos en otro momento:

Figura 46. Opción de Configuración de Oracle

Posteriormente se mostrará una pantalla con el resumen de las opciones y productos que se instalarán, si está de acuerdo con el resumen pulsar la opción Instalar.

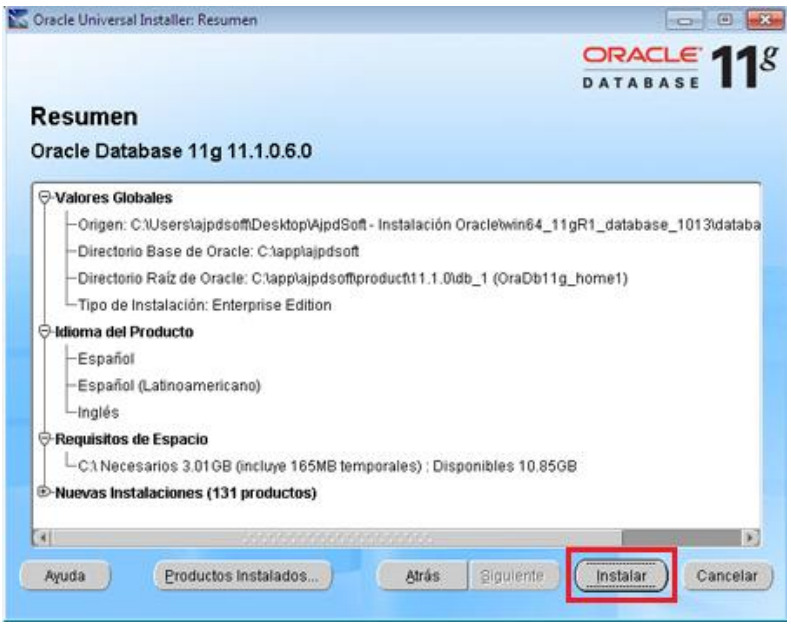


Figura 47. Resumen Configuración de Oracle

El Asistente de Oracle nos mostrará el estado de la instalación de la base de datos.

Figura 48. Proceso de instalación de Oracle

Finalmente, el asistente de instalación de Oracle nos mostrará una ventana informando que la base de datos se encuentra instalada correctamente. Dar clic en el botón Salir.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL

MANUAL DE USUARIO

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: CAROLINA ESTEFANÍA MOROCHO CRESPO

TUTOR: ING. ISMELIS CASTELLANOS LÓPEZ, MSc.

GUAYAQUIL – ECUADOR
2016

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

El sistema de aplicación presentado funciona como un asistente metodológico para la evaluación del control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil a través de la ejecución de un análisis de brecha de seguridad de la información. Para esto la aplicación web toma como base los controles de la norma internacional de seguridad de la información ISO/IEC 27001: 2013 (última versión liberada y aprobada) y permite ejecutar la evaluación del control interno, realizando una comparación de la situación actual de la carrera contra el estado ideal propuesto por las buenas prácticas (Nivel Optimizado).

El presente Manual de Usuario desglosa las funcionalidades y servicios que ofrece el sistema de aplicación de una forma práctica y eficiente.

2. DESCRIPCIÓN DE LAS FUNCIONALIDADES DEL SISTEMA

2.1. ACCESO AL SISTEMA

Para acceder al sistema deberá introducir el usuario y la contraseña que le ha facilitado el administrador de la herramienta y presionar el botón “Accesar”. Al escribir la contraseña es importante considerar mayúsculas, minúsculas, caracteres especiales y números.

Figura 1. Autenticación de usuario en ICSystem

Si los datos ingresados por el usuario no son correctos, el sistema visualiza un mensaje de error: “Identificación incorrecta. Su nombre de usuario o contraseña fue introducido incorrectamente.”

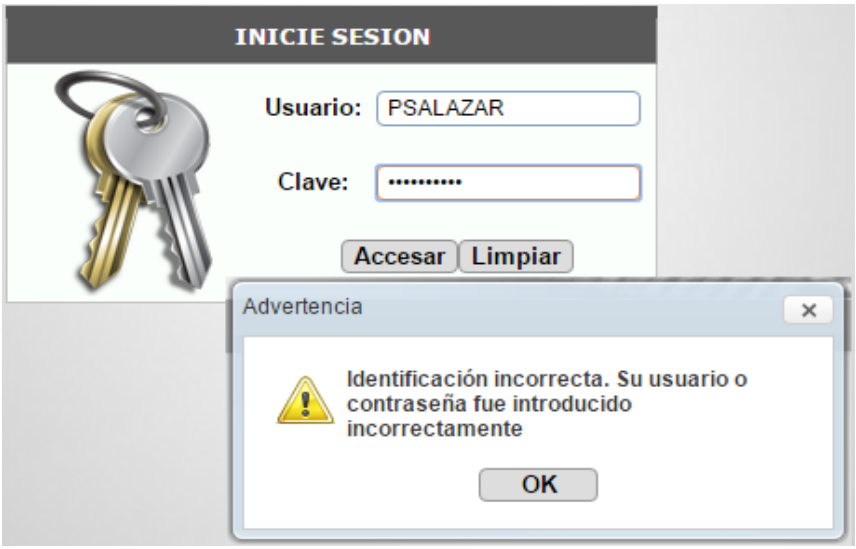


Figura 2. Autenticación incorrecta en ICSystem

Posteriormente, se mostrará por pantalla el o los módulos a los que el usuario tiene acceso de acuerdo a sus funcionalidades y responsabilidades dentro de la institución.

- Para el caso del Administrador del sistema se mostrarán los módulos Administración y Análisis.

Figura 3. Módulos del Administrador de ICSystem

- Para el caso de los usuarios finales se mostrará únicamente el módulo Análisis.

Figura 4. Módulo de Usuarios de ICSsytem

2.2. MÓDULO DE ADMINISTRACIÓN

El módulo de Administración contiene un conjunto de opciones de configuración del sistema a los cuales sólo tendrán acceso los usuarios con un perfil de administrador.

Este módulo contempla un menú con dos opciones, de las cuales se despliega el submenú respectivo. A continuación se detalla cada opción del menú del módulo de Administración.

Figura 5. Opciones de menú del módulo de Administración

Las opciones del menú son:

- Seguridades
- Configuraciones

2.2.1. Menú Seguridades

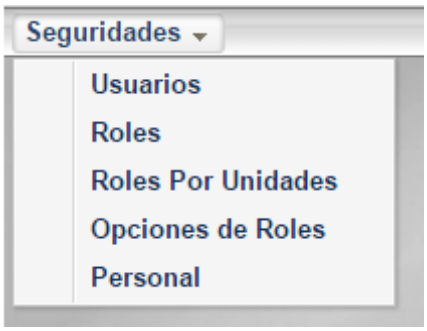


Figura 6. Menú Seguridades del Módulo Administración

2.2.1.1. Usuarios

En este apartado se puede realizar la gestión de usuarios y muestra al gestor una tabla con los distintos usuarios que se encuentran creados para la gestión del sistema. En la parte superior de la tabla se encuentra un botón de lupa que permite seleccionar el personal de la institución al que se le va asignar un usuario para acceder al sistema.

Figura 7. Pantalla de Mantenimiento de Usuarios

La tabla de mantenimiento de usuarios muestra campos como el código del usuario, nombre del usuario, contraseña y el estado.

El botón Guardar se encarga de guardar el nuevo usuario o guardar la modificación de alguno de los usuarios y el botón Limpiar se encarga de limpiar los componentes para un nuevo ingreso de usuario.

El campo contraseña se puede modificar pulsando sobre el nombre del usuario y una vez realizado el cambio de la contraseña se deberá presionar el botón Guardar. Para dar de baja un usuario del sistema, únicamente deberá seleccionar el usuario, quitar el check de la opción Activo y presionar el botón Guardar; de manera inmediata el campo Estado pasará de estar con un visto a estar con una equis.

2.2.1.2. Roles

El apartado de roles permite asignarle un rol a los usuarios creados en el sistema. Los roles disponibles se dividen en dos categorías principales: Administrador y Usuario.

Figura 8. Pantalla de Mantenimiento de Roles

La tabla de mantenimiento de roles muestra campos como el código del rol, nombre del rol, descripción y el estado. El botón Guardar se encarga de guardar el nuevo rol o guardar la modificación de alguno de los roles ya definidos y el botón Limpiar se encarga de limpiar los componentes para un nuevo ingreso de roles.

2.2.1.3. Roles por Unidad

El apartado de roles por unidad permite asignarle las unidades/departamento a los usuarios creados en el sistema.

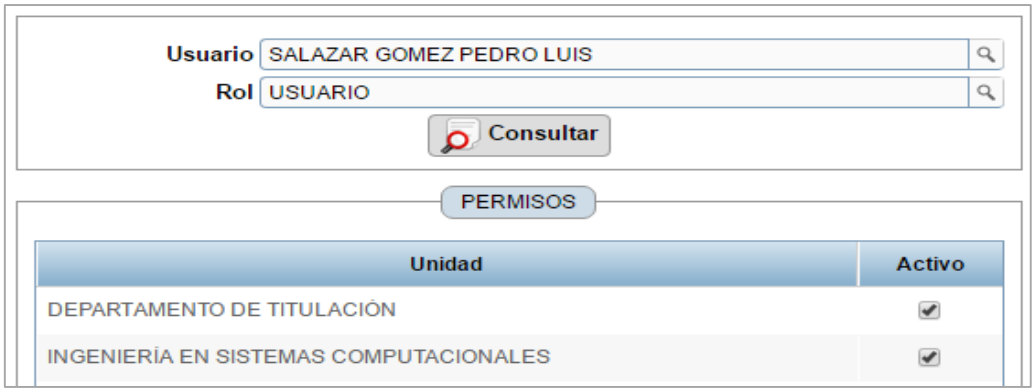


Figura 9. Pantalla de Roles por Unidad

En la parte superior de la tabla se encuentra un botón de lupa que permite buscar el usuario y el rol, presionar el botón Consultar y aparecerán las unidades creadas a las cuales se podrán asignar los usuarios dándole visto en la opción Activo.

Para modificar las unidades asignadas a los usuarios únicamente se deberá quitar el visto de la unidad a los que se desea quitar los accesos y presionar el botón Guardar.

Figura 10. Modificación de accesos en las unidades

Las unidades/departamentos que se pueden seleccionar van a depender de lo registrado en el menú Configuraciones, submenú Departamentos.

2.2.1.4. Opciones de Roles

Para asignar las opciones a los roles, se deberá buscar el rol a través del botón de lupa y posteriormente seleccionar los submenús de cada módulo del sistema.

El botón Guardar se encarga de guardar las selecciones de menús para los roles o guardar la modificación de alguno de los menús ya definidos y el botón Limpiar se encarga de limpiar los componentes para un ingreso nuevo.

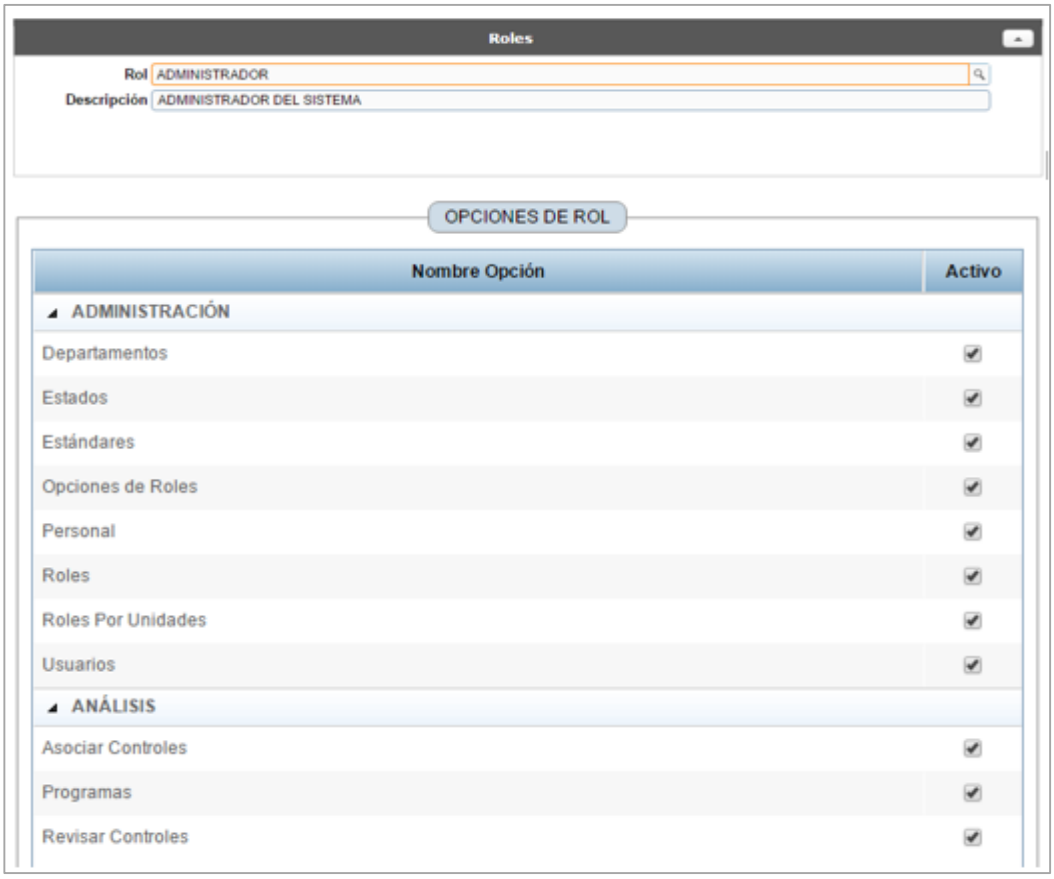


Figura 11. Pantalla de Opciones de menú

2.2.1.5. Personal

La pantalla de Ingreso / Mantenimiento de Personal permite modificar las parametrizaciones para un funcionario que ya consta en la carrera, además

permite ingresar a nuevo personal. Los campos que están marcados con un asterisco son considerados obligatorios, en caso de que no se incluya alguno de estos campos con asterisco el sistema no permitirá guardar los datos del nuevo personal y mostrará el respectivo mensaje de alerta.

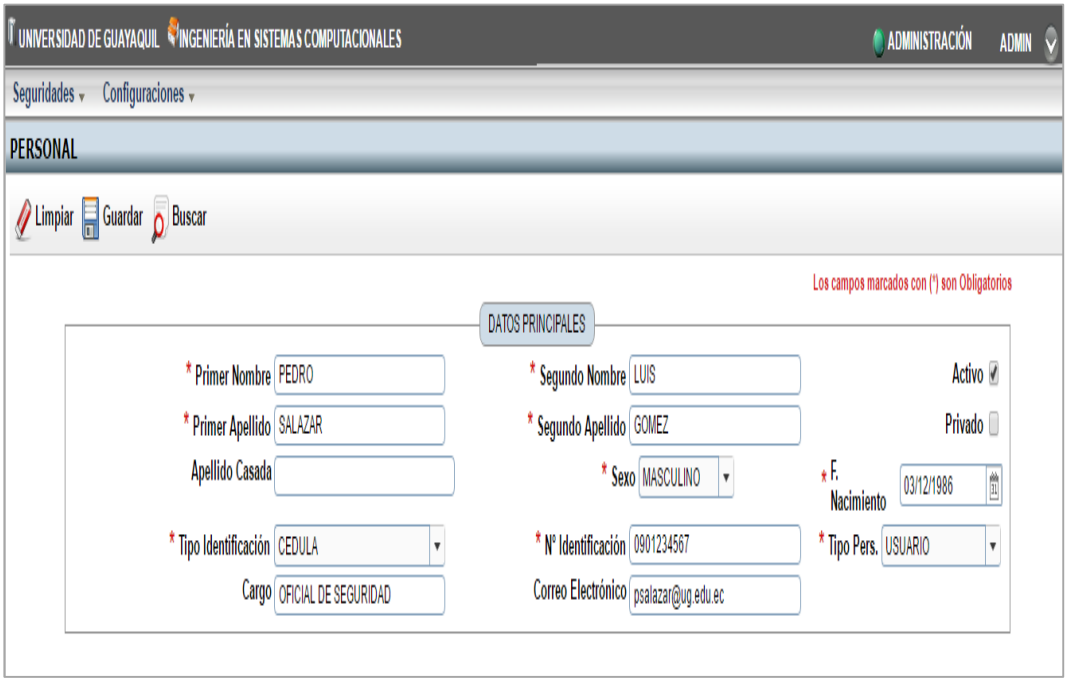


Figura 12. Pantalla de Ingreso/Mantenimiento de Personal

La pantalla consta de tres botones que permiten limpiar, consultar y guardar los datos ingresados. El botón guardar registra los nuevos cambios en la base de datos y el botón Limpiar se encarga de limpiar los componentes para un ingreso nuevo.

2.2.2. Menú Configuraciones

Figura 13. Menú Configuraciones del Módulo Administración

2.2.2.1. Departamentos

En este aparato se puede configurar los departamentos de la carrera a las que se desea realizar una evaluación de los controles.

Figura 14. Pantalla de Mantenimiento de Departamentos

Las opciones que permite la tabla Mantenimiento Departamentos son las siguientes:

- **Crear:** Ingresar código, nombre y descripción del departamento para guardar lo ingresado deberá hacer clic en el botón Guardar.
- **Modificar:** Para modificar un departamento hay que pulsar sobre el nombre del departamento, realizar los cambios deseados y hacer clic en el botón Guardar.

Para dar de baja un departamento del sistema, únicamente deberá seleccionar el departamento, quitar el check de la opción Activo y presionar el botón Guardar; de manera inmediata el campo Estado pasará de estar con un visto a estar con una equis.

2.2.2.2. Estándares

La opción ‘Estándares’ ofrece la posibilidad de disponer de catálogos de cumplimiento normativo generados en la herramienta o crear un catálogo propio. Estos catálogos serán necesarios para la opción ‘Revisión de controles’.

Figura 15. Pantalla de Mantenimiento Tipos de Normas

Figura 16. Pantalla de Mantenimiento Normas

La tabla de mantenimiento de tipos de normas posee las siguientes opciones:

- **Crear:** Permite crear un nuevo catálogo.
- **Modificar:** Para modificar un catálogo hay que pulsar sobre el nombre del catálogo. Al acceder a un catálogo se permite configurar su estructura de requisitos que serán utilizados para evaluar su cumplimiento.

Para dar de baja un tipo de norma del sistema, únicamente deberá seleccionar el tipo de norma, quitar el check de la opción Activo y presionar el botón Guardar; de

manera inmediata el campo Estado pasará de estar con un visto a estar con una equis.

Todas las entradas del catálogo son modificables por el usuario. Para ello, pulsando dos veces sobre la celda correspondiente se permite su edición.

2.2.2.3. Estados

Al acceder a la opción "Estados" se permite configurar el conjunto de estados que van a estar disponibles para analizar los requisitos del catálogo que estamos configurando.

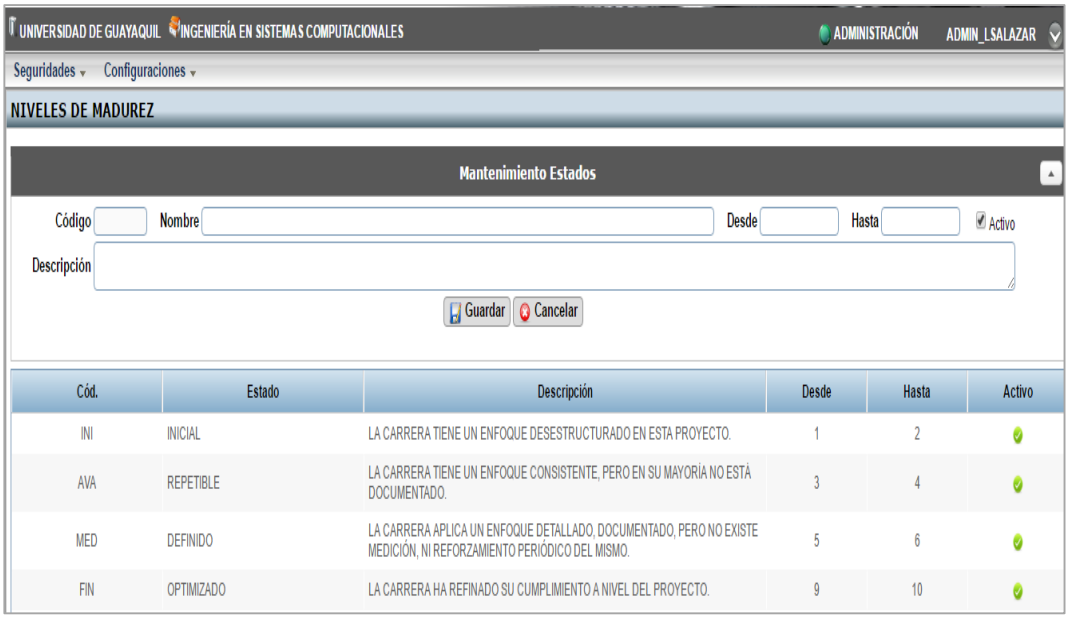


Figura 17. Pantalla de Mantenimiento de Estados

Las opciones que permite la tabla Mantenimiento Estados son las siguientes:

- **Crear:** Ingresar código, nombre, descripción del estado, desde y hasta (porcentajes de completitud) para guardar lo ingresado deberá hacer clic en el botón Guardar.
- **Modificar:** Para modificar un estado hay que pulsar sobre el nombre del estado, realizar los cambios deseados y hacer clic en el botón Guardar.

Estos niveles estarán disponibles por defecto para el catálogo tanto en la opción "Revisión de controles".

2.3. MÓDULO DE ANÁLISIS

El módulo de Análisis contiene un conjunto de opciones de análisis y revisión de catálogos de buenas prácticas.

Figura 18. Opciones de menú del módulo de Análisis

Este módulo está dividido en dos partes:

- Análisis
- Transacciones

2.3.1. Menú Análisis

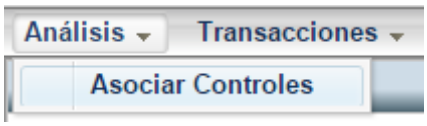


Figura 19. Submenú Asociar Controles del Menú Análisis

2.3.1.1. Asociar Controles

Para asociar controles dar clic sobre el botón de lupa y se deberá seleccionar el tipo de norma que se desea evaluar.

Figura 20. Pantalla de selección del tipo de norma

Posteriormente aparecerá una tabla con los campos código, control, descripción y estado en donde se pueden visualizar los controles definidos para la norma seleccionada.

Figura 21. Tabla Asociar Controles

Para incluir un nuevo control seleccionar el botón Nuevo ubicado en la parte superior derecha de la tabla y completar la información correspondiente al control.

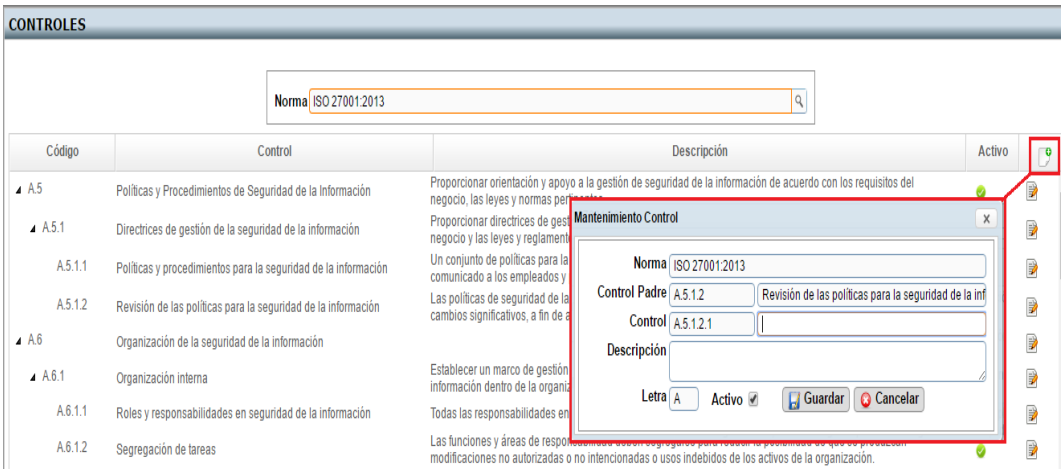


Figura 22. Pantalla para el ingreso de un nuevo control

Para modificar un control previamente ingresado hay que pulsar el botón de Edición ubicado en la parte derecha de cada control, realizar los cambios deseados y hacer clic en el botón Guardar. En esta misma opción se puede dar de baja un control, solo se debe quitar el visto de la opción Activo.

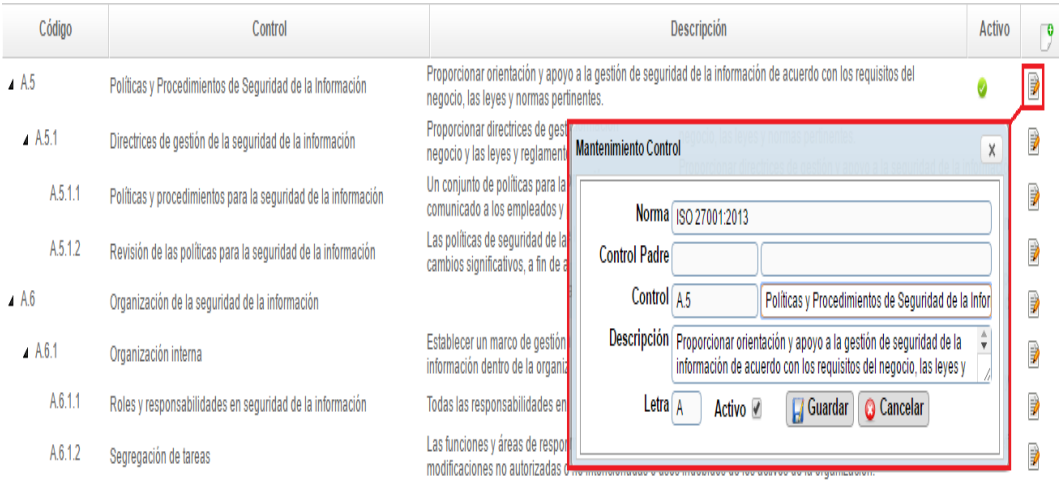


Figura 23. Pantalla para la modificación de un control

2.3.2. Menú Transacciones

Figura 24. Submenús del Menú Transacciones

2.3.2.1. Programas

En este apartado se podrán crear programas de evaluación en donde se deberá ingresar los datos del programa y se deberán asociarán los controles y los estados para la evaluación del control interno informático en la carrera.

Las opciones que permite la tabla Mantenimiento Programas son las siguientes:

- **Crear:** Ingresar, descripción, responsable, departamento, fecha de inicio, fecha de fin y se deberán asociarán los controles y los estados. Para guardar lo ingresado deberá hacer clic en el botón Guardar.

- **Modificar:** Para modificar un programa hay que pulsar sobre el nombre del programa, realizar los cambios deseados y hacer clic en el botón Guardar.

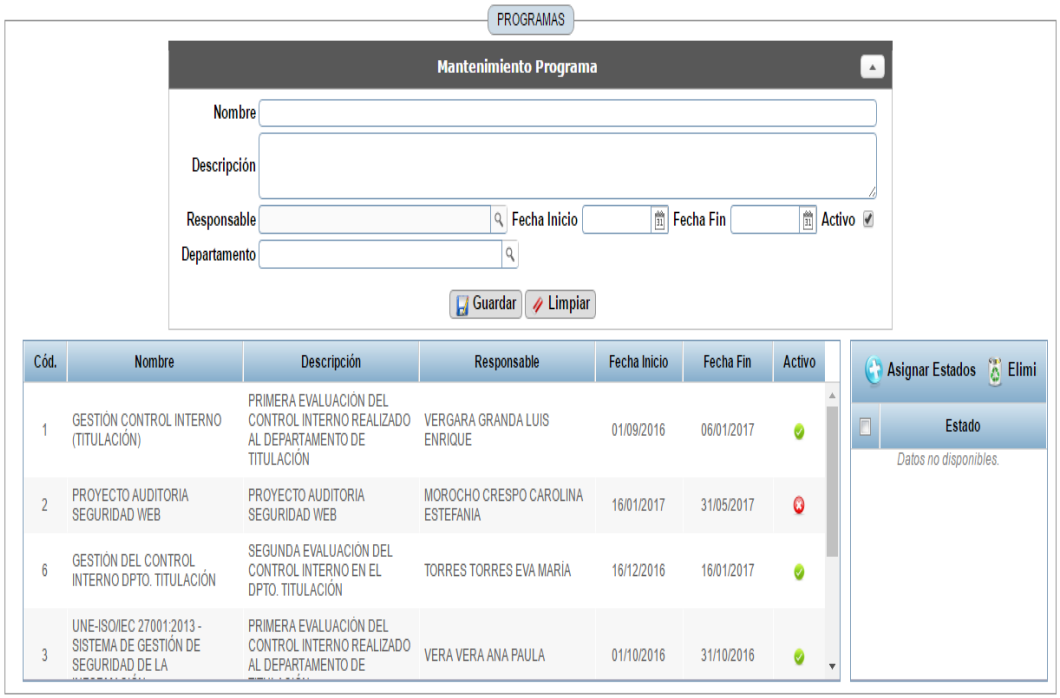


Figura 25. Pantalla de Mantenimiento de programas

2.3.2.2. Revisar controles

La opción de Revisión de controles permite gestionar el estado de cumplimiento de los controles establecidos en los diferentes catálogos, que se establecen en el apartado 'Administración/Estándares'.

Para la evaluación se deberá completar lo siguiente:

- **Madurez:** Permite indicar el estado de implantación del requisito o el control dentro de la organización.
- **Responsable:** Permite incluir el nombre de la persona que ejecuta el control.
- **Revisor:** Permite indicar la persona que realizó la evaluación de los controles.
- **Observaciones:** Permite incluir las observaciones y datos relevantes para justificar el estado del control.

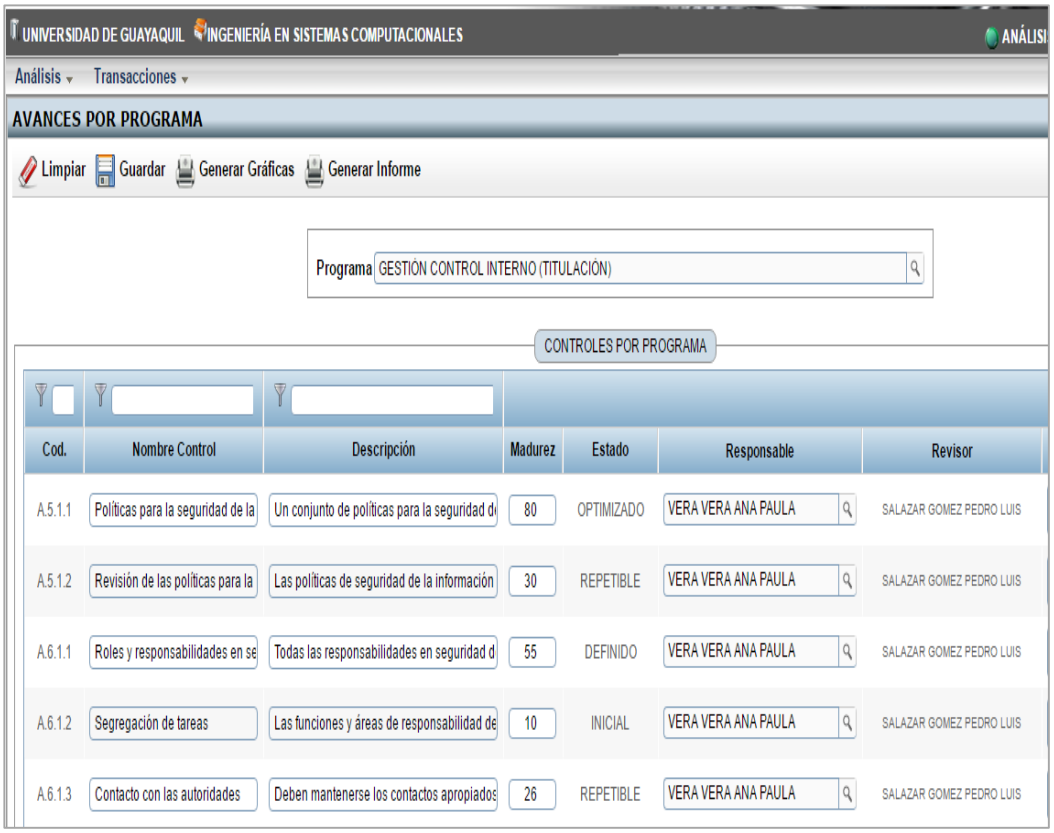


Figura 26. Pantalla de evaluación del control interno informático

La pantalla consta de cuatro botones que permiten limpiar, guardar los datos ingresados, generar gráficas y generar informe. El botón guardar registra los nuevos cambios en la base de datos y el botón Limpiar se encarga de limpiar los componentes para un ingreso nuevo.

Para evaluar un control solo se deberá ingresar el nivel de madurez y dar enter de forma automática se mostrará el estado correspondiente al nivel ingresado. Al finalizar se deberá dar clic en el botón Guardar.

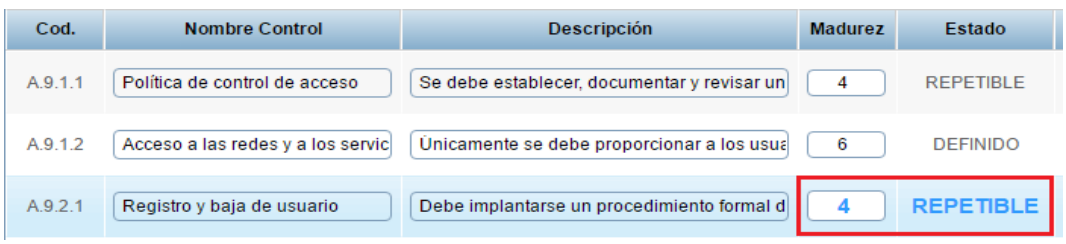


Figura 27. Evaluando un control de la norma

El botón Generar Gráficas en donde empezará la descarga de las gráficas que muestran el estado de implantación de los controles.

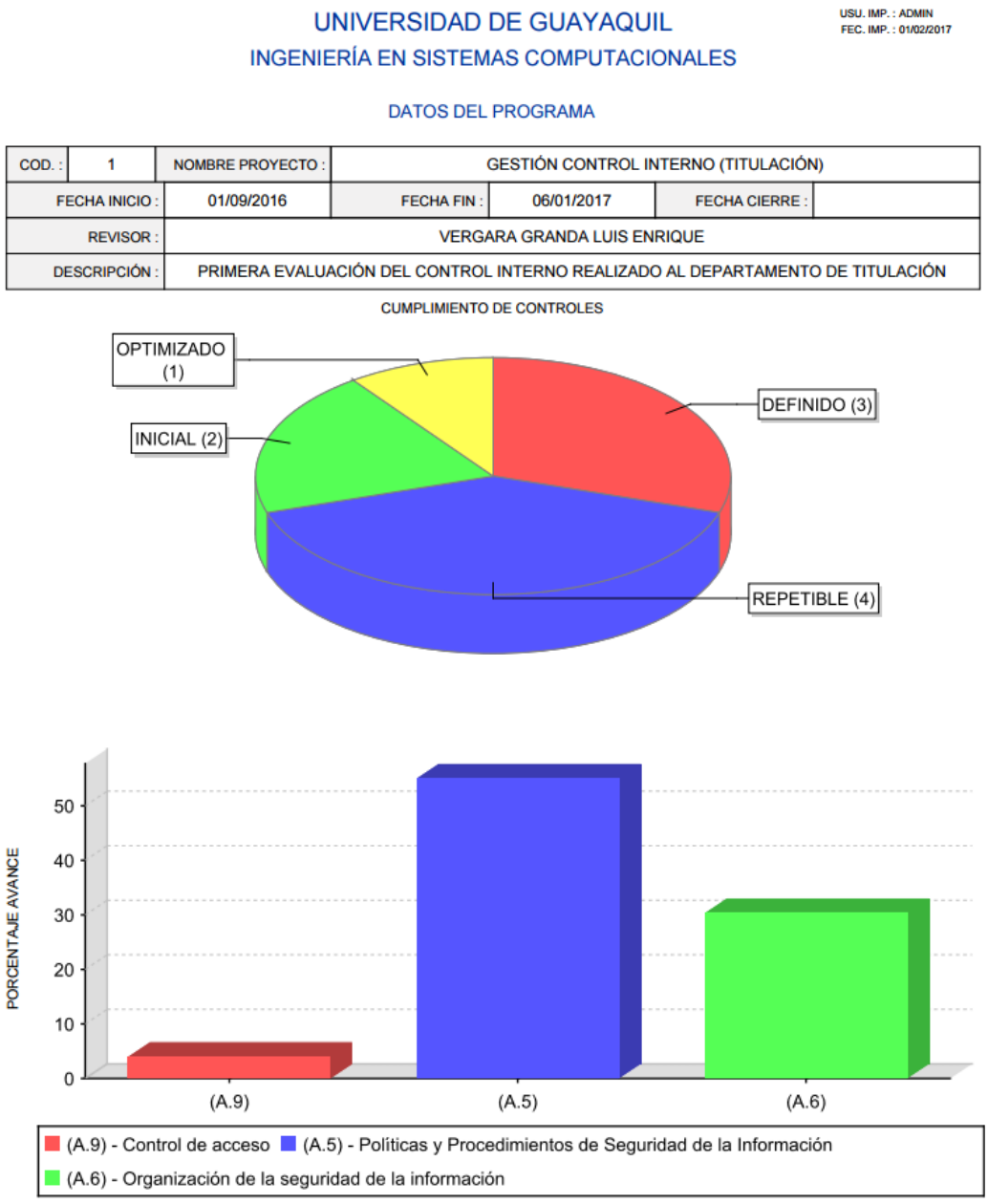
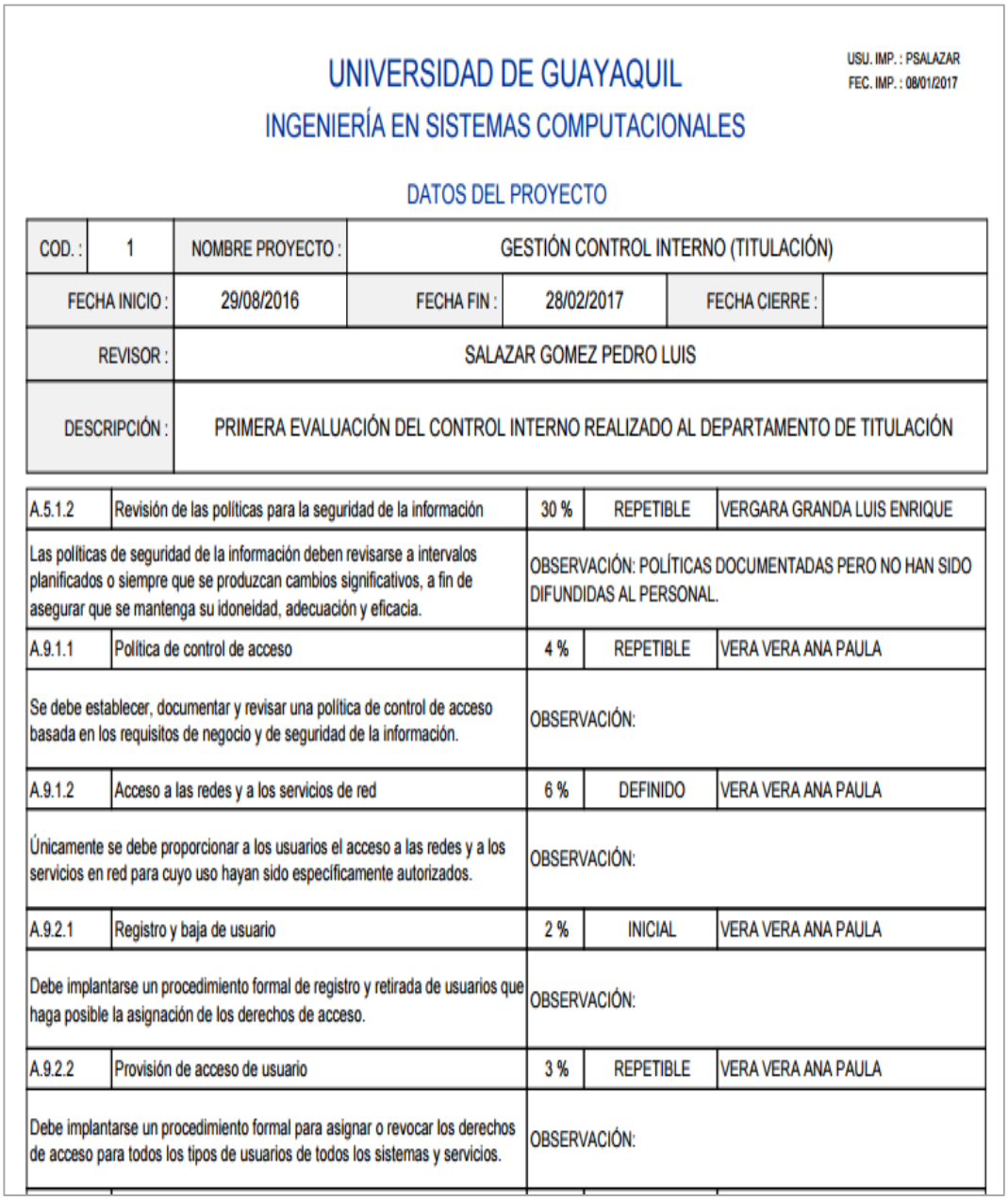


Figura 28. Documento con las gráficas de evaluación de los controles

El botón Generar informe empezará la descarga del informe, en un documento PDF, con el listado de controles evaluados en la Carrera o en alguna unidad de la misma.



UNIVERSIDAD DE GUAYAQUIL

USU. IMP. : PSALAZAR
FEC. IMP. : 08/01/2017

INGENIERÍA EN SISTEMAS COMPUTACIONALES

DATOS DEL PROYECTO

COD. :	1	NOMBRE PROYECTO :	GESTIÓN CONTROL INTERNO (TITULACIÓN)				
FECHA INICIO :	29/08/2016	FECHA FIN :	28/02/2017	FECHA CIERRE :			
REVISOR :	SALAZAR GOMEZ PEDRO LUIS						
DESCRIPCIÓN :	PRIMERA EVALUACIÓN DEL CONTROL INTERNO REALIZADO AL DEPARTAMENTO DE TITULACIÓN						

A.5.1.2	Revisión de las políticas para la seguridad de la información	30 %	REPETIBLE	VERGARA GRANDA LUIS ENRIQUE
Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.		OBSERVACIÓN: POLÍTICAS DOCUMENTADAS PERO NO HAN SIDO DIFUNDIDAS AL PERSONAL.		
A.9.1.1	Política de control de acceso	4 %	REPETIBLE	VERA VERA ANA PAULA
Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.		OBSERVACIÓN:		
A.9.1.2	Acceso a las redes y a los servicios de red	6 %	DEFINIDO	VERA VERA ANA PAULA
Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.		OBSERVACIÓN:		
A.9.2.1	Registro y baja de usuario	2 %	INICIAL	VERA VERA ANA PAULA
Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.		OBSERVACIÓN:		
A.9.2.2	Provisión de acceso de usuario	3 %	REPETIBLE	VERA VERA ANA PAULA
Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.		OBSERVACIÓN:		

Figura 29. Documento con el informe de evaluación del control interno

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL

PROYECTO DE TITULACIÓN

Previo a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: CAROLINA ESTEFANÍA MOROCHO CRESPO

TUTOR: ING. ISMELIS CASTELLANOS LÓPEZ, MSc.

GUAYAQUIL – ECUADOR
2016

 Presidencia de la República del Ecuador  Plan Nacional de Ciencia, Tecnología, Innovación y Saberes  SENESCYT Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación		
REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO: "Desarrollo de una herramienta de software como asistente metodológico para la evaluación del control interno informático en la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil"		
	REVISORES:	
INSTITUCIÓN: Universidad de Guayaquil	**FACULTAD:** Ciencias Matemáticas y Físicas	
CARRERA: Ingeniería en Sistemas Computacionales		
FECHA DE PUBLICACIÓN:	**N° DE PÁGS.:** 176	
ÁREA TEMÁTICA: Sistema Informático, Control Interno		
PALABRAS CLAVES: Herramienta de Software, Control Interno, Desarrollo de Sistema, Auditoría de Sistemas, Seguridad de la Información		
RESUMEN: Cuando hablamos de seguridad debemos tener claro que toda la organización debe involucrarse para conseguir los objetivos de confidencialidad, integridad y disponibilidad de la información. Considerando los constantes ataques a los que se ven expuestos los sistemas de información se ha propuesto el desarrollo de una herramienta de software que permita ejecutar la evaluación del control interno de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil tomando como base el estándar ISO 27001. Para este proyecto se ha considerado trabajar con la metodología de desarrollo de software en cascada, el cual fue estudiado y analizado, llegando a la conclusión de que se adaptaba al proyecto. Esta herramienta ofrecerá una solución amigable al usuario para la evaluación del control interno sin necesidad de contratar especialistas en este campo.		
N° DE REGISTRO (en base de datos):	**N° DE CLASIFICACIÓN:** **N°**	
DIRECCION URL (tesis en la web):		
ADJUNTO PDF:	**SI** [X]	**NO** [ ]
CONTACTO CON EL AUTOR: Carolina Morocho Crespo	**Teléfono:** 2840104	**E-mail:** carolina.morochoc@ug.edu.ec
CONTACTO DE LA INSTITUCIÓN:	**Nombre:** Ing. Roberto Crespo – Director de la Carrera de Ingeniería en Sistemas Computacionales	
	Teléfono: (04) 2307729	

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación, “DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL“, elaborado por la Srta. Carolina Estefanía Morocho Crespo, alumna no titulada de la Carrera de Ingeniería en Sistemas Computacionales, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

_____

Ing. Ismelis Castellanos López, MSc.
TUTOR

DEDICATORIA

Quiero dedicar este proyecto de titulación principalmente a mami, quién ha sido mi motor, apoyo incondicional y guía a lo largo de mi vida. A mi bonito, quién fue parte importante en este nuevo logro y por ser quién inspira mi corazón. A mis amigos, Vania y Luis, quiénes han contribuido con sus consejos, ánimos y fuerzas. Por último y no por eso menos importante, a un ángel que nos bendice desde el cielo… mi querida amiga y compañera de universidad, Lissette Arreaga, este título va por las dos.

AGRADECIMIENTO

Doy gracias a Dios por ser mi fuerza, mi luz y por no permitirme bajar los brazos. A mami y a toda mi familia quiénes estuvieron presentes cuando más los necesité. A mi tutor, por todo el apoyo y tiempo dedicado en este proyecto de titulación. A mis amigos y compañeros de trabajo por toda la confianza que depositaron en mí. A mis maestros por compartir sus conocimientos y sobretodo las experiencias de vida.

A todos ustedes…
¡Gracias infinitas!

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, MSc.
DECANO DE LA FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

Ing. Roberto Crespo Mendoza, Mgs.
DIRECTOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

Ing. Ismelis Castellanos López, MSc.
PROFESOR TUTOR DEL PROYECTO DE TITULACIÓN

Lcda. Jenny Ortiz Zambrano, Mgs.
PROFESOR REVISOR DEL ÁREA-TRIBUNAL

Ing. Jéssica Yépez Holguín, Mgs.
PROFESOR REVISOR DEL ÁREA-TRIBUNAL

Ab. Juan Chávez Atocha, Esp.
SECRETARIO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL"

Autora: Carolina Estefanía Morocho Crespo

.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL

Proyecto de Titulación que se presenta como requisito para optar por el título de

INGENIERO EN SISTEMAS COMPUTACIONALES

Autora: Carolina Estefanía Morocho Crespo

C.I. 092730584-7

Tutor: Ing. Ismelis Castellanos López, MSc.

Guayaquil, agosto de 2016

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por la estudiante Carolina Estefanía Morocho Crespo, como requisito previo para optar por el título de Ingeniero en Sistemas Computacionales cuyo problema es:

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL.

Considero aprobado el trabajo en su totalidad.

Presentado por:

Morocho Crespo Carolina Estefanía Cédula de ciudadanía N° 092730584-7

Tutor: Ing. Ismelis Castellanos López, MSc.

Guayaquil, agosto de 2016

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

Nombre Alumno: CAROLINA ESTEFANÍA MOROCHO CRESPO	
Dirección: SAMANES 5 MANZANA 941 VILLA 26	
Teléfono: 2840104	**E-mail:** carolina.morochoc@ug.edu.ec

Facultad: CIENCIAS MATEMÁTICAS Y FÍSICAS
Carrera: INGENIERÍA EN SISTEMAS COMPUTACIONALES
Proyecto de titulación al que opta: INGENIERÍA EN SISTEMAS COMPUTACIONALES
Profesor tutor: ING. ISMELIS CASTELLANOS LÓPEZ, MSc.

Título del Proyecto de titulación: DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL.

Tema del Proyecto de Titulación: HERRAMIENTA DE SOFTWARE PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica:

Inmediata	**X**	Después de 1 año	

Firma Alumna:

3. Forma de envío:

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM [ ] CDROM [**X**]

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL

Autor: Carolina Estefanía Morocho Crespo
Tutor: Ing. Ismelis Castellanos López, MSc

RESUMEN

Cuando hablamos de temas de control interno hay que tener claro que toda la organización debe estar involucrada para alcanzar los objetivos propuestos por las autoridades. Considerando los constantes ataques a los que se ven expuestos los sistemas de información se ha planteado como objetivo principal de este proyecto de titulación el desarrollo de una herramienta de software que permita ejecutar la evaluación del control interno de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con la finalidad de que se conozcan las deficiencias de control y poder efectuar planes de acción para mitigar dichas deficiencias que a la larga podrían convertirse en riesgos materializados. Para el análisis de factibilidad de la herramienta de software, se han efectuado entrevistas y encuestas considerando como población de estudio a los docentes de la carrera que son aquellos que nos pueden dar información relevante sobre el control interno y seguridad en la institución, así mismo para la obtención del tamaño de la muestra se consideró el muestreo aleatorio simple que es un método sencillo y que permite el cálculo rápido de medias. Asimismo, se ha considerado trabajar con la metodología de desarrollo de software en cascada, el cual fue estudiado y analizado, llegando a la conclusión de que se adaptaba al proyecto. Finalmente, se puede expresar que la herramienta de software desarrollada ofrece una solución amigable a la carrera permitiéndole ejecutar la evaluación del control interno sin necesidad de contratar costosas consultorías o requerir personal especializado en este campo.

PALABRAS CLAVES: Herramienta de Software. Control Interno. Desarrollo de Sistema. Auditoría de Sistemas. Seguridad de la Información.

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL

Autor: Carolina Estefanía Morocho Crespo
Tutor: Ing. Ismelis Castellanos López, MSc

ABSTRACT

When we talk about issues of internal control it must be clear that the entire organization should be involved to achieve the goals set by the authorities. Considering the constant attacks to which they are exposed information systems it has emerged as the main objective of this project titling the development of a software tool that allows to run the evaluation of internal control Engineering Degree in Computer Systems University of Guayaquil in order that control deficiencies are known and able to carry out action plans to mitigate these shortcomings that eventually could become risks materialized. For feasibility analysis software tool, have been carried out interviews and surveys considered as study population teachers of the race are those who can give us relevant information on internal control and security in the institution, also for obtaining sample size simple random sampling is a simple method that allows rapid calculation of averages was considered. It also has considered working with software development methodology cascade, which was studied and analyzed, concluding that suited the project. Finally, we can say that the developed software tool offers a friendly solution to the race allowing you to run the evaluation of internal control without hiring expensive consultants or require specialized personnel in this field.

KEYWORDS: Software Tool. Internal control. System Development. Systems Audit. Security of the information.

INTRODUCCIÓN

La seguridad y protección de la información en tiempos de Internet constituye un desafío de alta complejidad al que se enfrentan hoy las organizaciones que abren sus puertas al mundo a través de la red.

Asimismo, la necesidad de que los recursos informáticos que soportan los procesos de negocio críticos funcionen adecuadamente y con disponibilidad casi permanente, determina que el aseguramiento del funcionamiento de la red, de las aplicaciones y de los servicios brindados a los clientes externos e internos constituya hoy un elemento crítico para las instituciones.

Debido a ello, hoy en día la seguridad de la información se ha convertido en un tema dominante y es objeto de un enfoque renovado para todo tipo de negocio. A medida que las organizaciones siguen haciendo frente a los desafíos que plantean la seguridad y privacidad de la información, incluyendo el robo de identidad, fugas de datos, fraudes, phishing, y una gran cantidad de otros ataques internos y externos, siguen preguntándose:

- ¿Podemos demostrar que estamos cumpliendo con las reglamentaciones mundiales y con las buenas prácticas internacionales actuales en la seguridad de la información, gestión de riesgos y control interno?
- ¿Nos hemos protegido sistemáticamente de las amenazas y los costos relacionados con TI?
- ¿Cómo podemos asegurar que nuestros activos críticos han sido identificados y se encuentran debidamente protegidos?
- ¿Los colaboradores y estudiantes confían en nosotros y estamos haciendo todo lo referente para mantener esta confianza?

Desde el punto de vista de la Ley Orgánica de Protección de Datos, las medidas de seguridad LOPD van destinadas a todas las organizaciones, empresas e instituciones que almacenan y tratan datos de carácter personal en sus sistemas de información, cuya finalidad principal es proteger, los datos de carácter personal

tratados, de posibles incidencias que puedan provocar su pérdida, alteración u acceso no autorizado, tanto interno como externo. (Consulting Integral, 2015)

Ninguna organización puede funcionar hoy sin una efectiva gestión de seguridad de la información y una adecuada implementación del control interno, ni mucho menos podría hacerle frente a los constantes ataques informáticos a los que actualmente se ven expuestas.

La información se ha convertido en un elemento vital para las organizaciones y necesita protegerse. Empresas de todos los tamaños y segmentos han aumentado sus necesidades de almacenamiento y, como estas siguen creciendo año a año, los desafíos son cada vez mayores.

Al multiplicarse los volúmenes de datos, su administración es un cargo muy costoso en algunas ocasiones, lo que está obligando a las instituciones a tomar decisiones sobre qué hacer con la información, cómo almacenarla y/o en manos de quién dejarla.

Es por esto, que una correcta y oportuna evaluación del control interno permitiría a las autoridades y directivos de las instituciones reforzar sus puntos débiles en el tratamiento de la seguridad de la información.

La norma internacional UNE-ISO/IEC 27001:2013 está conformada por catorce dominios que a su vez se encuentran desglosados en una serie de controles que permitirán a las organizaciones utilizarlos como directrices para una correcta gestión de seguridad de la información.

De acuerdo a lo antes expresado nace el presente proyecto de titulación titulado: "*Desarrollo de una herramienta de software como asistente metodológico para la Evaluación del Control Interno Informático en la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil*"

El presente proyecto de titulación ha sido organizado en varios capítulos, los cuáles se describen a continuación:

En el *Capítulo I*, se formula el problema de investigación al cual se le dará solución considerando sus causas y consecuencias, la formulación del problema y los objetivos del proyecto (general y específicos). Asimismo se ha delimitado el problema, en este caso la investigación se centrará en la situación actual del control interno de la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil.

En el *Capítulo II*, se encuentra la descripción del marco teórico y contendrá los conceptos claves para el desarrollo de este proyecto de titulación, así como también encontrarán definiciones de autores y de la norma ISO 27001, para que el lector pueda familiarizarse con los temas y tenga una mayor comprensión.

En el *Capítulo III*, se incluye la metodología, entregables y criterios de evaluación de la herramienta de software, así como también se ha realizado un análisis de factibilidad para comprobar que el desarrollo del proyecto de titulación es operativo, técnico, legal y económicamente factible.

Finalmente, en el *Capítulo IV*, se detallan los criterios de aceptación, aprobación de la herramienta de software, conclusiones y recomendaciones.

CAPÍTULO I

1. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

1.1.1. UBICACIÓN DEL PROBLEMA EN UN CONTEXTO

Hoy en día existe un gran crecimiento tanto en la educación como en la economía de información y telecomunicaciones, los sistemas de información son una de las soluciones que las instituciones educativas fueron adoptando para su trabajo diario, lo que les permitió mejorar su administración y rapidez en cada uno de sus procesos.

Para la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil es vital focalizarse en sus fortalezas para lograr el cumplimiento de sus objetivos para así convertirse en una carrera líder en la formación de profesionales de excelencia, líderes, emprendedores con sólidos valores morales y éticos comprometidos con la sociedad y que contribuyan al desarrollo del país, para mejorarlo en lo social, económico, ambiental y político. Hacer investigación, transferencia de tecnología, extensión de calidad e innovación para dar soluciones a los problemas y necesidades presentes y futuras del país.

Si bien con el uso de la tecnología en las instituciones de educación superior se han logrado automatizar los procesos que antes eran llevados de forma manual, es importante considerar que en un mundo donde existen continuos cambios tecnológicos, el incremento de la demanda de los jóvenes para ingresar a las universidades conllevan también a considerar que existen mayores riesgos tecnológicos para las instituciones educativas.

En enero de 2016, una red de hackers accedió a los sistemas informáticos de universidades privadas del Ecuador para registrar como alumnos a personas que nunca cursaron estudios superiores. Este delito incluyó a una lista de 366

personas que habrían inscrito ilegalmente sus títulos falsos en la base de datos de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt). Este hecho ha permitido constatar las vulnerabilidades que presenta la red y la importancia que implica para las universidades el protegerse de manera adecuada ante la inminente amenaza de ataques avanzados. (GMS, 2016)

A causa del reciente ataque informático presentado en la Senescyt, en el Ecuador es cada vez más frecuente que las instituciones educativas contraten servicios de consultoría para la evaluación del control interno de sus procesos, seguridades de acceso, cambios en sus sistemas de aplicación, seguridades en sus centros de datos, entre otros. Y es que la alta dirección de las instituciones de educación superior tanto pública como privada, presenta mayor interés en conocer la situación actual de sus instituciones y poder actuar a través de la optimización de su control interno.

De acuerdo al Estudio Global sobre las Prácticas de Seguridad de la Información en Tecnología, Medios y Telecomunicaciones (TMT) publicado en 2013 por la firma Deloitte se determinó que las organizaciones, actualmente se centran en la seguridad de la información debido a que sus clientes y el mercado así lo exigen y no sólo porque las regulaciones lo requieren. (Deloitte, 2013)

Asimismo, la firma Ernst and Young publicó la Encuesta Global de Seguridad de la Información en donde se evidenció que el 56% de los encuestados clasificó la prevención de fuga o pérdida de datos como un tema de alta prioridad para sus compañías en los próximos 12 meses mientras que el 49% de los encuestados catalogó los riesgos y las amenazas de personas con información privilegiada como de prioridad media, a pesar de que 56% considera que los empleados son una de las fuentes más probables de un ataque, y 36% señala a los contratistas externos como una fuente factible. (Ernst & Young, 2015)

Considerando que la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil cuenta con información y recursos tecnológicos que pueden verse afectados por controles ineficientes resulta conveniente contar con

una herramienta de software que les permita a las autoridades poder realizar una evaluación de sus controles internos implementados.

Tal como lo expresa la Consultora de Sistemas de Gestión y Normas ISO – SBQ; en los últimos años, las noticias de los incidentes de seguridad son cada vez mayores y también son mayores la diversidad de formas en las que estos se llevan a cabo. Antes las empresas sólo debían preocuparse de que las oficinas estuvieran protegidas por los robos, los incendios, las inundaciones, etc., pero ahora las amenazas de las que deben protegerse son mayores y vienen de forma menos visible. Ya no sólo deben de implantar sistemas para protegerse contra los incendios o las inundaciones, sino que también hay que establecer políticas y sistemas de protección de los datos en los sistemas informáticos, como ordenadores, discos duros, etc. Y el aumento cada vez mayor de las empresas en el uso de los dispositivos móviles y las aplicaciones de estos hace que las amenazas sean aún mayores. (SBQ Consultores, 2016)

A través de una correcta implementación de controles internos, la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil incrementará la confiabilidad de los mismos, identificando de manera oportuna los posibles incidentes y riesgos de tecnología de la información que podrían materializarse, todo esto considerando los controles y buenas prácticas definidas en la norma internacional de seguridad de la información, ISO 27001.

1.1.2. SITUACIÓN CONFLICTO NUDOS CRÍTICOS

Este problema se origina principalmente en las instituciones educativas por la falta de revisiones del ambiente de tecnología de la información, no ejecutar auditorías internas y la falta de asesoramiento continúo por parte de personal especializado han hecho que se deje de lado una eficaz evaluación del control interno.

Adicional, el problema radica en la falta de una herramienta gratuita que permita realizar la evaluación del control interno informático utilizando un mínimo de tiempo en dicha tarea pero que proporcionará a las autoridades y directivos; información relevante, suficiente y precisa sobre la situación actual de la carrera.

Para el caso de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil, la inexistencia de la evaluación del control interno informático se podría convertir en una problemática para las autoridades de esta institución impactando a la información, considerada como el principal activo de toda organización.

La información debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la institución. La norma/estándar UNE ISO/IEC 27001 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos y lógicos y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. (Fernández, 2012)

Asimismo, McAfee investigó 386 incidentes estadounidenses de pérdida de datos registrados durante el período de enero de 2009 a abril de 2011 que afectaron a 23 millones de registros. Los incidentes fueron divididos en tres categorías: ataques externos, violaciones de seguridad internas, tanto accidentales como de intencionalidad maliciosa, y eventos de naturaleza desconocida. (McAfee, 2012)

Los ataques externos correspondieron al 52% de los incidentes y afectaron al 60% de los registros comprometidos. En cuanto a los ataques internos maliciosos: el robo intencional de datos por parte de personal de la propia empresa, correspondió al 16% de los incidentes, con el 20% de los registros comprometidos. Si bien un 44% de los incidentes se debió a fuentes internas, la gran mayoría se debió a casos accidentales. Sin embargo, en el caso de los ataques maliciosos de origen interno, el número promedio de registros afectado por incidente fue mucho mayor, debido a la mayor facilidad en la preparación de estos ataques.

Una evaluación oportuna de los controles internos informáticos permitirá minimizar los incidentes de seguridad presentados en la investigación realizada por McAfee y también con dicha evaluación se podrá estimar el nivel de madurez de la

situación actual de la institución, y les permitirá a las autoridades intervenir para corregir las posibles deficiencias identificadas en los controles.

1.1.3. CAUSAS Y CONSECUENCIAS DEL PROBLEMA

Las instituciones educativas no cuentan con evaluaciones del control interno informático por las siguientes causas:

- Costos elevados de consultorías.
- Falta de presupuesto.
- Poco interés en temas de auditoría de sistemas y control interno.
- Inexistencia de herramientas de software open source para la evaluación del control interno.
- Falta de conocimiento de estándares para las auditorías de sistemas.

De acuerdo a las causas del problema anteriormente expuestas, se derivan las siguientes consecuencias:

- Pérdida de información importante.
- Retrasos en las tareas y operaciones de las instituciones educativas.
- Manipulación de información por parte de terceros.
- Accesos no autorizados y errores en la segregación de funciones.
- Riesgos de tecnología de la información no identificados.

1.1.4. DELIMITACIÓN DEL PROBLEMA

Campo: Educación Superior, en la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil, ubicada en las calles Víctor Manuel Rendón 429 entre Baquerizo Moreno y Córdova, Ciudad de Guayaquil, Provincia del Guayas, Ecuador

Área: Proceso de evaluación del control interno por parte de las autoridades en la Carrera de Ingeniería de Sistemas Computacionales.

Aspectos: Delimitado, claro, evidente, original, factible e identifica los productos esperados.

Tema: DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL.

1.1.5. FORMULACIÓN DEL PROBLEMA

¿DE QUÉ MANERA BENEFICIA A LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL LA IMPLEMENTACIÓN DE UNA HERRAMIENTA DE SOFTWARE QUE PERMITA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO A TRAVÉS DE LA NORMA ISO 27001?

1.1.6. EVALUACIÓN DEL PROBLEMA

Entre los aspectos para la evaluación del problema que se encuentran presentes en este proyecto de tesis tenemos los siguientes:

Delimitado: El presente proyecto se enfocará en la evaluación de la situación actual de los controles implementados en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil considerando la norma ISO/IEC 27001 como marco de referencia de las buenas prácticas de seguridad de la información.
La herramienta de software que permitirá ejecutar la evaluación del control interno se desarrollará en un período de tres meses, comprendido entre junio y agosto de 2016.

Claro: Para el desarrollo de este proyecto no es necesario la utilización de términos complejos, más bien proporcionará expresiones y resultados claros y precisos sobre el análisis de los controles internos y permitirá a las autoridades de

la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil tomar decisiones oportunas y de ser el caso, minimizar o asumir los posibles riesgos tecnológicos existentes.

Evidente: En la actualidad, las autoridades de la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil desconocen su posicionamiento con respecto al cumplimiento de los controles de seguridad de la información versus las buenas prácticas de tecnología, esta situación podría dificultar el manejo adecuado de sus controles internos.

Original: Es totalmente novedoso por desarrollar una herramienta de software que funcione como asistente metodológico para la evaluación del control interno informático de la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil.

Factible: El sistema de información que será desarrollado para una necesidad identificada en la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil resulta factible ya que utilizando un conjunto mínimo de recursos proporcionará información suficiente para que las autoridades tomen decisiones oportunas.

Identifica los productos esperados: Herramienta de software Open Source con una interfaz amigable para las autoridades de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil, que permita realizar en pocos minutos la evaluación de los controles informáticos basándose a la norma internacional ISO/IEC 27001.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

- Desarrollar un sistema de aplicación utilizando herramientas reconocidas en el mercado, de fácil comprensión y utilización con la finalidad de

simplificar la ejecución de tareas de evaluación del control interno informático en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil permitiéndole acoplarse a la norma ISO/IEC 27001 para optimizar su control interno y tomar decisiones oportunamente.

1.2.2. OBJETIVOS ESPECÍFICOS

- Explicar los beneficios de la evaluación del control interno para que las autoridades de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil puedan trabajar con la optimización de los controles existentes.
- Orientar a las autoridades de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil para que se ejecute oportunamente la evaluación del control interno de la institución.
- Facilitar una herramienta de software para la obtención de información relevante, suficiente y oportuna con la finalidad de lograr la implementación de controles para la minimización de los riesgos tecnológicos.
- Conocer la situación actual del control interno de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil para que las autoridades puedan actuar en sus brechas de seguridad.
- Comparar el estado actual en la que se encuentra la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con los requerimientos del estándar de buenas prácticas ISO/IEC 27001 para que las autoridades conozcan su situación frente a las buenas prácticas de seguridad.

1.3. ALCANCES DEL PROBLEMA

El presente proyecto tendrá como alcance el desarrollo de un sistema de aplicación que les permita a las autoridades de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil realizar una evaluación de su control interno tomando como base los controles y requisitos definidos en la norma internacional UNE-ISO/IEC 27001 que se enfoca en las buenas prácticas de la seguridad de la información.

Los dominios que podrán ser evaluados desde el sistema de aplicación a desarrollarse serán los siguientes:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad relativa a los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relación con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- Cumplimiento

Dentro de los catorce dominios antes mencionados, se evaluarán treinta y cinco objetivos de control y ciento catorce controles. (Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)

Al concluir este proyecto de titulación se entregará una aplicación que se enfocará en el estudio de la situación actual de la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil versus los controles definidos en la norma ISO/IEC 27001, para dar como resultado un análisis de brecha de alto nivel que contendrá la evaluación de los controles de la institución.

El sistema de aplicación permitirá generar y descargar gráficas estadísticas con el nivel de madurez de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil basado en el cumplimiento de los controles informáticos descritos en la norma ISO/IEC 27001 y además el sistema de aplicación permitirá la generación de un informe con los resultados del análisis gap de la institución.

Dentro de este proyecto de titulación no se están considerando modificaciones o cambios solicitados posteriormente a la aprobación de esta herramienta de software. Los controles que se incorporarán en el sistema de aplicación a desarrollarse corresponderán a los definidos en la versión actual de la norma UNE-ISO/IEC 27001:2013.

1.4. JUSTIFICACIÓN E IMPORTANCIA

Según una publicación del diario El Comercio, el Ecuador ocupa el octavo lugar entre los países de la región que más ataques informáticos registró en el 2014. Brasil y Perú lideran la lista con un 32% y 28% respectivamente. (Diario EL COMERCIO, 2015)

Tomando en consideración los continuos delitos informáticos, robo de información, suplantación de identidades; en la actualidad, es cada vez más recurrente escuchar a la alta administración de las empresas y/o instituciones preocuparse por la evaluación de su control interno, a través de la contratación de firmas consultoras especializadas en efectuar esta tarea. Y es que, la evaluación de controles internos les permite a los directivos de las instituciones identificar sus debilidades potenciales y hacer énfasis en el mejoramiento de sus controles existentes.

En este contexto, es fundamental que las instituciones educativas inviertan en seguridad de la información, pues deben considerar que cuando un ataque cibernético es exitoso, recuperarse del mismo requiere gastos no contemplados y excesivamente mayores de lo que representa una inversión previa. Las instituciones educativas guardan información de contactos, direcciones, datos socioeconómicos, cuentas bancarias, etc.; todos estos registros son sensibles y por tanto su pérdida puede implicar gastos y daños, no solamente económicos. (GMS, 2016)

Considerando el uso de la tecnología en la automatización de los procesos, para la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de

Guayaquil es sumamente importante enfocarse en sus debilidades de control pero por la situación económica del país, es cada vez más complicado la asignación de presupuesto para la contratación de personal especializado en evaluación del control interno. Por esta razón, el disponer de una herramienta de software para efectuar una autoevaluación de sus controles les permitirá actuar oportunamente para prevenir, detectar y corregir errores, así como identificar la deficiencia o ineficacia de los controles implementados en la institución.

Todas las instituciones educativas deberían ser conscientes de que los delincuentes cibernéticos ganan dinero al robar información personal y luego venderla en el mercado negro a otros criminales, que a su vez convierten los datos en efectivo mediante una serie de tácticas fraudulentas. (Burrel, 2014)

Los delincuentes informáticos están apuntando a las brechas de seguridad existentes en las instituciones educativas, a continuación mencionamos tres ataques a la seguridad de la información que fueron ocasionados a universidades en los Estados Unidos:

El 18 de febrero de 2014, la Universidad de Maryland resultó víctima de un ataque de seguridad informática que dejó al descubierto registros con información personal identificable.
Una semana más tarde, la Universidad de Indiana anunció que un error del personal había dejado expuesta información sobre 146.000 estudiantes por un lapso de 11 meses.
Otra semana después, el Sistema de Universidades de Dakota del Norte informó que habían atacado un servidor con los nombres y números de Seguro Social de más de 290.000 alumnos y ex alumnos, y alrededor de 780 profesores y empleados. (Burrel, 2014).

Para la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil, el disponer de una herramienta de software propia que más que nada actúe como un asistente metodológico sobre el control interno informático será de gran utilidad para conocer el estado actual de la institución, ya que mostrará información relevante que podrá ser vista y evaluada a tiempo por los directivos,

antes que ocurra la materialización de algún tipo de riesgo informático.

El desarrollo de este proyecto de tesis resulta realmente importante y se encuentra justificada su investigación ya que le permitirá a la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil ser pionera en la utilización de una herramienta de software que le permite automatizar la evaluación de su control interno, generando documentación necesaria y suficiente para que los directivos de la institución educativa actúen oportunamente tomando decisiones que minimicen y corrija las debilidades o deficiencias de control identificadas en el análisis.

En uno de los informes de seguridad cibernética, la Organización de Estados Americanos (OEA) hace un balance sobre la situación del continente en cuanto a delitos informáticos e indica que “los ataques se están volviendo más prevalentes y sofisticados”. Tras una encuesta en cada nación se concluyó que en Ecuador hay la percepción de que el país no está preparado para afrontar un ataque cibernético. En otro punto, el documento de 60 páginas refiere que en el país no se ha incrementado el presupuesto para ciberseguridad. (Diario EL COMERCIO, 2015)

Para hacerle frente a la falta de presupuesto asignado a la ciberseguridad, el sistema de aplicación a desarrollarse resulta también relevante y significativo en la práctica puesto que con un mínimo de conocimientos de auditoría y consultoría, se podrá realizar una evaluación de controles internos de la institución obtenido un análisis de brecha de seguridad de alto nivel en donde las autoridades la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil podrán verificar el cumplimiento de los mismos por parte del personal de la institución; todo esto, sin la necesidad de llegar a la contratación de costosas consultorías.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ANTECEDENTES DEL ESTUDIO

Desde épocas primitivas, el ser humano se ha visto en la necesidad de implementar mecanismos de control para salvaguardar sus activos y de esta forma no ser víctimas de desfalcos o robos.

Como parte de la historia se puede mencionar que desde el segundo viaje de Colón a América, se evidenció la existencia de controles aplicados por los reyes al asignar a un empleado la tarea de controlar el manejo de los fondos de los barcos.

Y es que la necesidad de ejercer un control dentro de las organizaciones fue constatada por los primeros gobernantes, jefes religiosos y dirigentes empresariales. Dada la necesidad de dirigir y supervisar las actividades de la organización, se establecieron controles para asegurar la consecución de objetivos. (Cooper & Lybrand, 1997)

Los intentos iniciales por querer aplicar a las computadoras en el área de los negocios se enfocaron hacia los datos, luego se trató de hacer hincapié en la información y el apoyo a las decisiones. A su vez las primeras compañías que usaron computadoras reconocieron la gran necesidad de establecer unidades organizacionales autónomas de especialistas que se encargarían de implementar los sistemas. (Mcleod, 2000)

La rápida evolución de las organizaciones y los continuos avances tecnológicos, han contribuido en que diariamente exploten nuevas amenazas y vulnerabilidades informáticas, así como también la información se vea expuesta por las brechas de seguridad existentes en las instituciones. Tomando esto en consideración, los directivos muestran especial interés en detectar, conocer, minimizar o asumir los

riesgos tecnológicos a través de una buena gestión del control interno y de seguridad de la información.

Se han presentado muchos casos de delitos informáticos ejecutados a universidades y es que al hablar de un eficiente control interno, no podemos dejar de lado la seguridad de la información, que hoy en día sin duda cumple una función importante dentro de cualquier institución. Asegurar la confidencialidad, integridad y disponibilidad de la información se ha convertido en una necesidad, que puede ser tratada a través de una buena gestión de seguridad.

Un estándar internacionalmente utilizado para gestionar la seguridad de la información es ISO 27001, que representa la experiencia acumulada de expertos en el tema. Y aunque su implementación debe realizarse en función de las características, necesidades y condiciones de cada organización, uno de los primeros pasos para su aplicación está relacionado con conocer el documento y sus propósitos.

Es muy difícil de mostrar el valor económico de una aplicación de computadora, por lo que se realizan análisis extensos para justificar cada proyecto potencial. Lo que sí es claro es que los gerentes toman decisiones para resolver problemas, y usan información para tomar estas decisiones. (Mcleod, 2000)

A lo largo de nuestras vidas, hemos leído en periódicos o escuchado en noticias que los sistemas de información de las instituciones educativas son atacados y vulnerados por estudiantes para modificar sus calificaciones.

En febrero del 2013, los sistemas informáticos de la Universidad de Especialidades Espíritu Santo sufrieron un ataque de hackers, el objetivo de la fallida intervención fue violentar la seguridad del registro de calificaciones de los alumnos de la institución. La intromisión fue detectada a tiempo por el sistema informático y por docentes. (Diario Expreso, 2013)

Asimismo, uno de los últimos casos reportados de ataques a los sistemas de las universidades fue el presentado en el mes de mayo del 2016, donde se dio a

conocer que un joven estudiante ingresó en el sistema informático de la Universidad Argentina de la Empresa (UADE) y tuvo acceso a las bases de datos de los alumnos, profesores y usuarios administradores de la red, donde "varias veces" cambió las notas de exámenes y trabajos. El joven hacker ya está a disposición de la Justicia. (Diario Argentino Ámbito, 2016)

Con el crecimiento acelerado de la tecnología y comunicaciones, las autoridades y directivos deben enfocarse en conocer la situación actual de los controles internos de una organización, y el hecho de no contar con un sistema informático que permita ejecutar esta tarea es una limitante que afecta la Carrera de Ingeniería en Sistemas Computaciones de la Universidad de Guayaquil, porque si bien en el mercado existen herramientas de software que se encargan de la gestión de seguridad de la información resultan ser soluciones no adaptables a instituciones educativas y además los precios resultan demasiado elevados haciendo que la implementación de estos sistemas se escape de las manos de las autoridades.

Cada vez es más frecuente la preocupación de los directivos de las universidades por conocer sus brechas de seguridad de la información, tanto es el interés que las universidades están optando por alinear sus controles internos a normas, estándares y marcos de trabajo de seguridad de la información. Al referirnos a la gestión de seguridad de la información en las instituciones educativas, no podemos dejar de mencionar la certificación ISO 27001 que logró la Universidad Warnborough del Reino Unido, y es que esta acreditación los ha favorecido en la lucha contra el acceso ilegal a sus datos confidenciales.

Muchos sistemas de información no han sido diseñados para ser seguros en el sentido de la Norma ISO/IEC 27001. La seguridad que se puede lograr a través de medios técnicos es limitada y debería ser apoyada por la gestión y los procedimientos apropiados. La identificación de los controles que deberían implantarse requiere una planificación cuidadosa y una atención al detalle. (Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)

Al hablar del activo más importante de cualquier organización, debemos considerar el posicionamiento en el que está la Carrera de Ingeniería en Sistemas

Computacionales de la Universidad de Guayaquil con respecto al control interno existente y que permitirá que las autoridades de la carrera puedan actuar y tomar decisiones oportunas y de ser el caso, minimizar los posibles riesgos tecnológicos existentes.

La información nos permite ser eficiente todos los procesos internos de nuestra organización, nos permite también conocer mejor a nuestra competencia así como el mercado por el que se compite. En general podemos conocer mejor el medio tanto interno como externo de nuestro negocio, para así detectar nuestras debilidades y potencialidades, atacarlas, y lograr una ventaja competitiva con respecto a las demás empresas del ramo. (Navarrete, 2002)

El tema de seguridad de la información está causando un gran interés y es que las empresas al sufrir alguna brecha de seguridad no solo están perdiendo información confidencial sino que también dicha brecha repercute en la imagen de la organización y en muchas ocasiones, grandes pérdida de dinero.

Las Tecnologías de Información en los procesos de entrada, conversión y salida dan a las instituciones una importante ventaja competitiva. ¿Por qué Microsoft es la más grande compañía de software? ¿Por qué Toyota es la manufacturera automotriz más eficiente? ¿Por qué McDonald's es la más eficiente compañía de comida rápida? Cada una de estas organizaciones sobresale en el desarrollo, administración y uso de Tecnologías de Información para administrar el entorno organizacional y crear valor para toda la institución. (Navarrete, 2002)

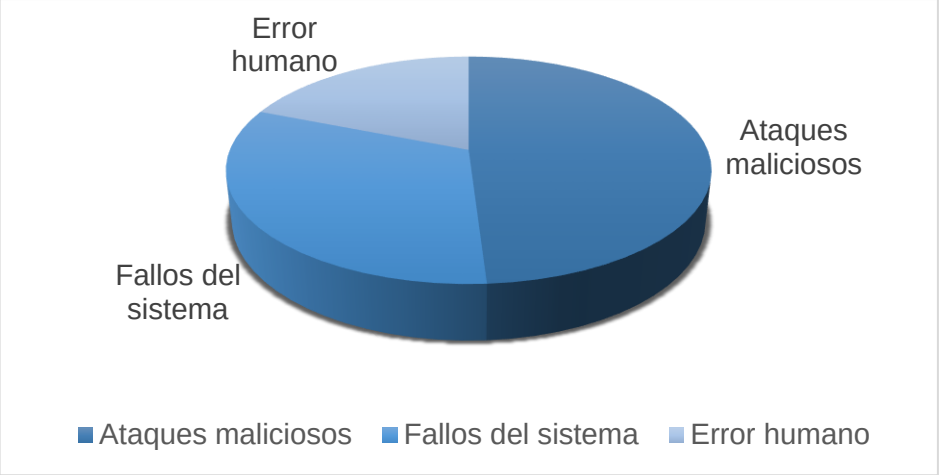
Compañías de seguridad informática y consultoras de seguridad de la información como ESET, McAfee, Kaspersky, Level 3, Deloitte, Ponemon, entre otras; realizan de manera periódica estudios y encuestas focalizadas en conocer los principales inconvenientes, amenazas y vulnerabilidades a las que se ven expuestas y que enfrentan hoy en día las organizaciones.

De acuerdo a un estudio efectuado por el Instituto Ponemon, las brechas de datos se focalizan principalmente en tres incidentes:

- 49% se deben a ataques maliciosos o criminales.

- 32% debido a procesar fallos y/o problemas técnicos del sistema.
- 19% debido a un error humano (empleados negligentes).

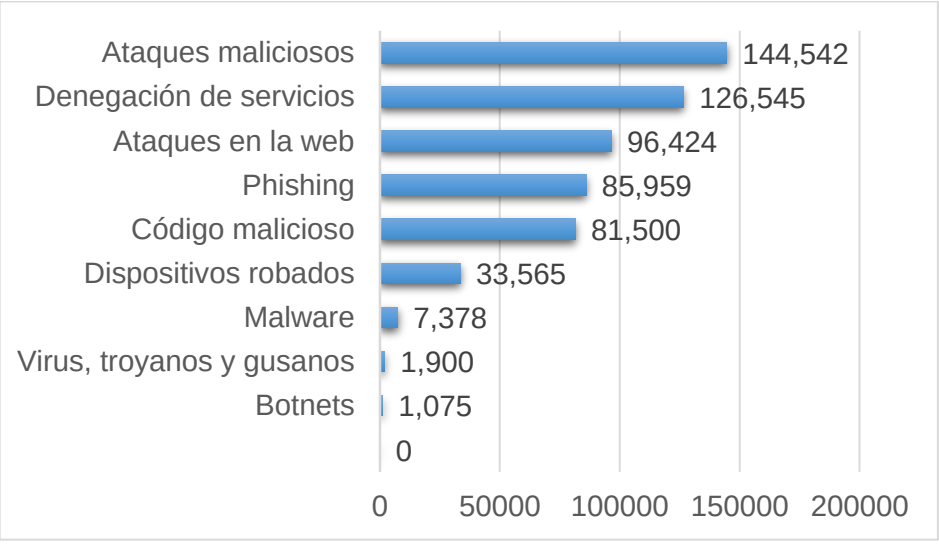
Figura 1. Incidentes de seguridad



Elaboración: Carolina Morocho Crespo
Fuente: Adaptado de (Ponemon Institute, 2015)

Ponemon atribuye los crecientes costos de los delitos informáticos a varios factores, incluyendo el tamaño de la organización, la industria, la línea de tiempo para la resolución y el tipo de ataque. (Ponemon Institute, 2015)

Figura 2. Costos por brechas de seguridad

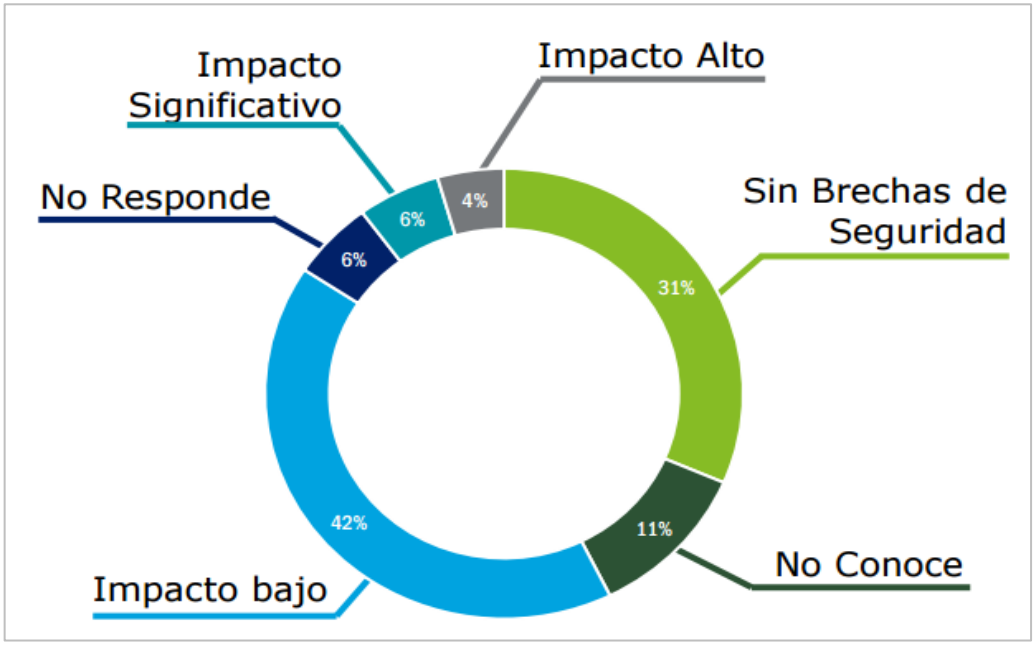


Elaboración: Ponemon Institute
Fuente: Estudio Costos del cibercrimen

Las organizaciones sea cual sea su giro de negocio presentan constantes desafíos a la hora de gestionar su seguridad de la información, entre estos desafíos se destaca el monitoreo de riesgos, respuesta ante incidentes y brechas de seguridad de la información.

De acuerdo a la Encuesta sobre Tendencias de Cyber Riesgos y Seguridad de la Información publicada en Junio del 2016 por la firma Deloitte, dentro de los aspectos que presentan mayores desafíos para las organizaciones en Latinoamérica se destaca la implementación de capacidades de monitoreo de riesgos y de respuesta ante incidentes y brechas de seguridad de la información. Esto resulta de relevancia considerando que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses, con pérdidas económicas superiores a U$S 250.000, más las pérdidas reputacionales o por daño de imagen. (Deloitte, 2016)

Figura 3. Impacto de las brechas de seguridad



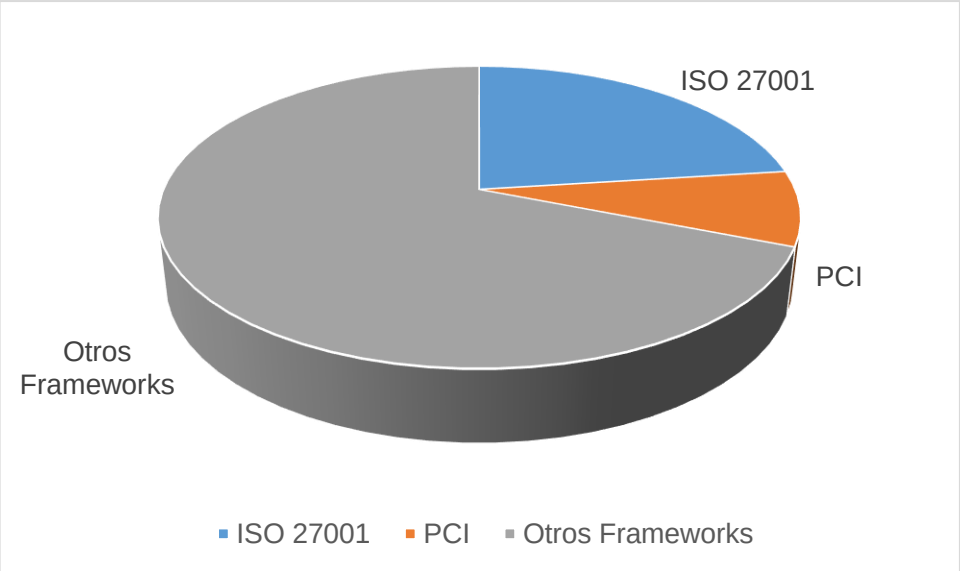
Elaboración: Deloitte & Touche
Fuente: Encuesta sobre Tendencias de Cyber Riesgos y Seguridad de la Información

De acuerdo con el informe de ESET Security Report Latinoamérica, casi el 42% de los encuestados afirmó que debe cumplir con algún estándar o marco de

trabajo, como ISO 27001 o PCI. Si bien estas obligaciones no determinan la ausencia de incidentes de seguridad, dejan ver que en la mayoría de los casos efectivamente se gestiona la Seguridad de la Información, además de que continuamente se revisan y actualizan los controles. (ESET Security, 2016)

El cumplimiento de normas y prácticas es esencial para lograr una correcta gestión de la Seguridad de la Información en las organizaciones. Estas actividades están relacionadas ciertos estándares previamente establecidos y que son aplicables a las empresas de acuerdo a sus funciones y características. En el mismo sentido, las empresas comprometidas con la protección de la información propia o de terceros, cumplen con estándares o normas de seguridad que se pueden adoptar voluntariamente. (ESET Security, 2016)

Figura 4. Marcos de trabajo que cumplen las empresas en Latinoamérica



Elaboración: ESET Security
Fuente: ESET Security Report Latinoamérica 2016

Tomando en consideración todos los puntos expuestos, las estadísticas presentadas por compañías expertas en seguridad de la información y considerando además la importancia y beneficios que conlleva una evaluación oportuna de los controles internos en cualquier organización, la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil no debería ser la excepción en focalizarse en la evaluación de su control interno, tal

como lo expresa la Contraloría General del Estado, el control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos.

Es por esto que a través de la ejecución de un análisis de brecha de seguridad en donde se consideren los controles de la norma ISO/IEC 27001 como marco de referencia, se podría obtener el “estado de la situación actual” de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil comparado con el “estado ideal o esperado” y de esta forma les permitirá a las autoridades trabajar en el fortalecimiento de los controles de seguridad de la información.

2.2. FUNDAMENTACIÓN TEÓRICA

La tecnología de la información en la actualidad se considera con un elemento primordial para el desarrollo y emprendimiento de las empresas y podemos referir a la información como el activo más valioso de la entidad, es decir como un recurso del cual la organización espera obtener un beneficio en el futuro. (Aumatell, 2003)

2.2.1. CONTROL INTERNO

Así como la opinión del auditor sobre los estados financieros se refiere si los mismos son razonables en sus cifras con respecto a un marco contable, llámese IFRS, NIF o USGAAP, para opinar sobre la efectividad de un sistema de control interno, es necesario partir de un marco de referencia sobre el mismo. La SEC y el PCAOB reconocieron como un marco de referencia adecuado sobre el control interno el emitido por COSO en 1992. (PricewaterhouseCoopers S.C., 2014)

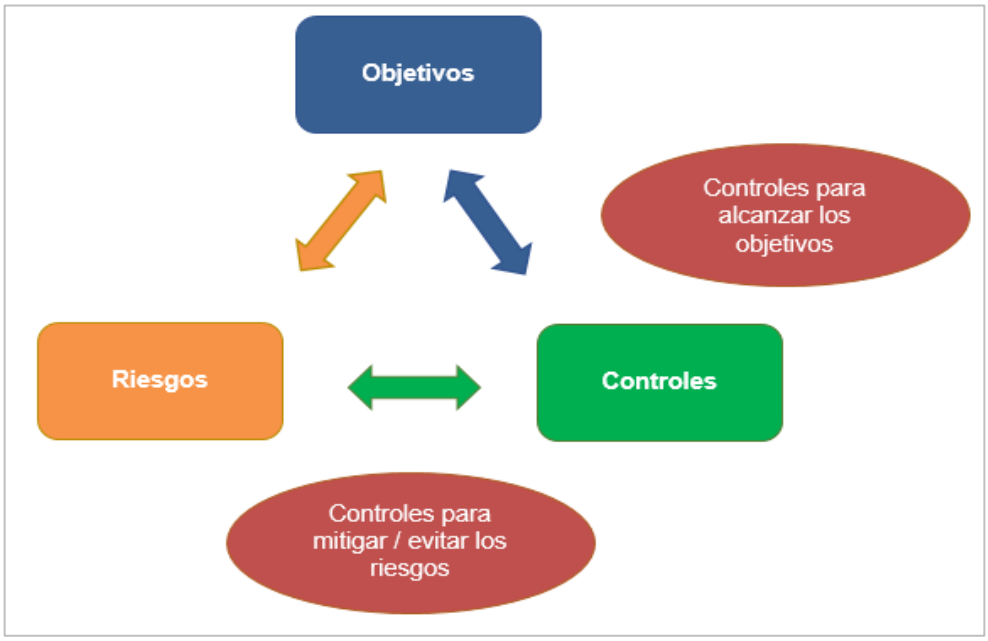
Si bien, reconocen la posibilidad de aplicar otro marco de control interno, el marco de COSO 1992 ha sido el más reconocido y aplicado. Bajo las circunstancias del ambiente de negocios que siguió a los escándalos financieros de 2002, COSO 1992 cubrió cabalmente las necesidades de ese momento. (PricewaterhouseCoopers S.C., 2014)

MODELO COSO

El control interno se define como un proceso efectuado por el consejo de administración, la dirección y el resto de personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento regulatorio. (Committee of Sponsoring Organizations, 2013)

El control interno ayuda a las entidades a lograr importantes objetivos y a mantener y mejorar su rendimiento. El control interno según el Modelo de COSO permite a las organizaciones desarrollar, de manera eficiente y efectiva, sistemas de control interno que se adapten a los cambios del entorno operativo y de negocio, mitigando riesgos hasta niveles aceptables y apoyando a la toma de decisiones y el gobierno corporativo de la organización. (Committee of Sponsoring Organizations, 2013)

Figura 5. Aspectos claves del control interno



Elaboración: Jorge Badillo Ayala
Fuente: Informe COSO (Committee of Sponsoring Organizations, 2013)

El modelo COSO proporciona tres categorías de objetivos para ofrecer seguridad razonable en la gestión de un sistema de control interno.

Tabla I. Objetivos del control interno

Objetivos	Descripción del Objetivo
Operaciones	Hacen referencia a la efectividad y eficiencia de las operaciones de la entidad, incluidos sus objetivos de rendimiento financiero y operacional, y la protección de los activos frente a posibles pérdidas.
Información	Hacen referencia a la información financiera y no financiera interna y externa y pueden abarcar aspectos de confiabilidad, oportunidad, transparencia, u otros conceptos establecidos por los reguladores, organismos reconocidos o políticas de la propia entidad.
Cumplimiento	Hacen referencia al cumplimiento de las leyes y regulaciones a las que está sujeta la entidad.

Elaboración: Carolina Morocho Crespo
Fuente: Informe COSO (Committee of Sponsoring Organizations, 2013)

Asimismo, en el modelo COSO se ha definido que en un sistema de control interno intervienen cinco componentes que se relacionan entre sí:

Tabla II. Componentes del control interno

Componente	Descripción del Componente
Ambiente de Control	Conjunto de normas, procesos y estructuras que constituyen la base sobre la que se desarrolla el control interno de una organización. El ambiente de control incluye: la integridad, los valores éticos, filosofía de la Dirección, la asignación de la autoridad, las responsabilidades, la organización, el desarrollo de los empleados y la orientación de la Dirección.
Evaluación de riesgos	Primero deben identificarse los objetivos organizacionales, vinculados y coherentes, luego deben identificarse y evaluarse los riesgos relevantes que pueden afectar el alcanzar esos objetivos.

Componente	Descripción del Componente
Actividad de Control	Son las políticas y procedimientos que ayudan a asegurar que se toman las medidas para limitar los riesgos que pueden afectar que se alcancen los objetivos organizacionales.
Información y Comunicación	Se debe identificar, ordenar y comunicar en forma oportuna la información necesaria para que los empleados puedan cumplir con sus obligaciones.
Supervisión o Monitoreo	Debe existir un proceso que compruebe que el sistema de control interno se mantiene en funcionamiento a través del tiempo, tiene tareas permanentes y revisiones periódicas. Estas últimas dependerán en cuanto a su frecuencia de la evaluación de la importancia de los riesgos en juego.

Elaboración: Carolina Morocho Crespo
Fuente: Informe COSO (Committee of Sponsoring Organizations, 2013)

Tanto los objetivos como los componentes del control interno se interrelacionan entre sí. La organización debe alcanzar las tres categorías de objetivos y para conseguirlo debe seguir las acciones de los componentes del control interno

Figura 6. Relación entre Objetivos y Componentes del control interno

Elaboración: Informe COSO
Fuente: (Committee of Sponsoring Organizations, 2013)

Existen otros modelos que han propuesto definiciones para el control interno, a continuación las revisaremos:

Definición según COCO:

La Guía de Control COCO define al control como el conjunto de elementos que incluyen: recursos, sistemas, procesos, cultura, estructura y tareas, que se adoptan para respaldar a las personas en el logro de los objetivos de una entidad. COCO establece que los objetivos del control interno deben recaer en las categorías relacionadas con la efectividad y eficiencia de las operaciones, confiabilidad de la información interna y externa, y cumplimiento de las leyes, reglamentos y políticas internas aplicables. (Instituto Canadiense de Contadores Autorizados, 1995)

Definición según INTOSAI:

Según la definición otorgada por la INTOSAI (International Organisation of Supreme Audit Institutions), el control interno representa el conjunto de los planes, métodos, procedimientos y otras medidas, incluyendo la actitud de la dirección, para ofrecer una garantía razonable de que se han cumplido los objetivos generales siguientes:

- Promover las operaciones metódicas, económicas, eficientes y eficaces y los productos y servicios de calidad, acorde con la misión que la institución debe cumplir;
- Preservar los recursos frente a cualquier pérdida por despilfarro, abuso, mala gestión, errores, fraude e irregularidades;
- Respetar las leyes, reglamentaciones y directivas de la dirección; y
- Elaborar y mantener datos financieros y de gestión fiables y presentarlos correctamente en los informes oportunos. (INTOSAI, 2001)

Definición según COBIT:

El control interno, según la metodología COBIT, se define como: Las políticas, procedimientos, prácticas y estructura organizacional, diseñadas para proveer una garantía razonable de que los objetivos de la empresa van a conseguirse y de que los eventos no deseados serán evitados o detectados y subsanados. (ISACA, 2012)

2.2.2. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se consigue mediante la implantación de un conjunto adecuado de controles, lo que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles se deberían establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización. (Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)

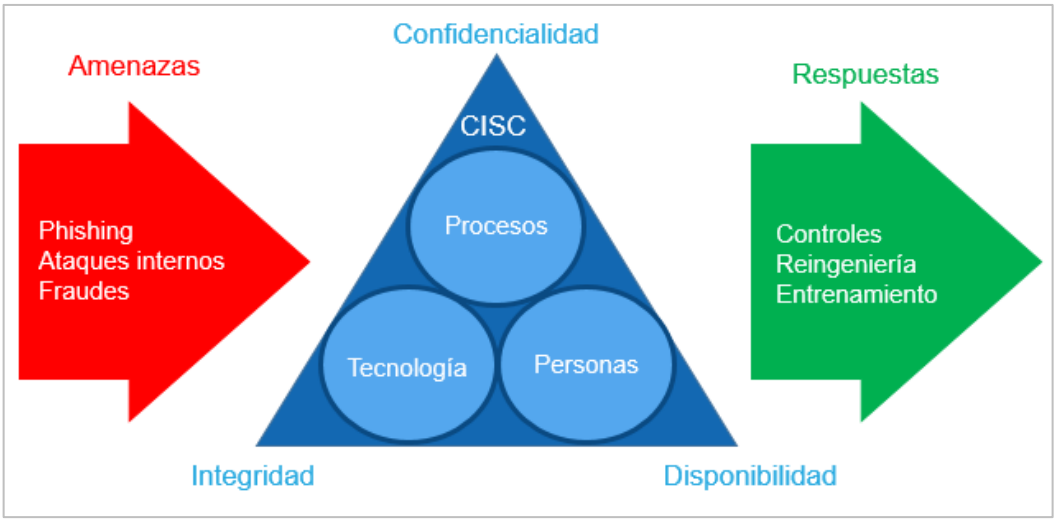
Al hablar de gestión de seguridad de la información no solo debemos enfocarnos en la seguridad del ambiente de tecnología de la información, sino también en gestionar la seguridad en la parte de talento humano, de procesos, protección física y jurídica, etc.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (ISO27000es, 2012)

Existen varios modelos para estimar la seguridad de información pero el modelo basado en los tres principios básicos: confidencialidad, integridad y disponibilidad es considerado como el más extendido en el tema de gestión de seguridad de la información. Las instituciones mantienen gran interés en proteger el activo más importante que poseen, la información.

En el manual de preparación del CISSP (Certified Informations Systems Security Professional candidate), se concibe la confidencialidad, la integridad y la disponibilidad como los tres principios básicos de la seguridad de los sistemas de información. Todos los controles, salvaguardas, amenazas, vulnerabilidades y procedimientos relacionados con la seguridad de la información se basan en estos tres principios. (Belt Ibérica S.A., 2004)

Figura 7. Principios básicos de seguridad de la información



Elaboración: Carolina Morocho Crespo
Fuente: Norma ISO/IEC 27001:2013

Asimismo, el manual de preparación del CISSP define por separado cada uno de los conceptos de los tres principios de seguridad de la información: (Belt Ibérica S.A., 2004)

- **Confidencialidad.** Intenta prevenir la revelación no autorizada, intencional o no, del contenido de un mensaje o de información en general. La pérdida de información puede producirse de muchas maneras, por ejemplo, por medio de la publicación intencional de información confidencial de una organización o por medio de un mal uso de los derechos de acceso en un sistema.

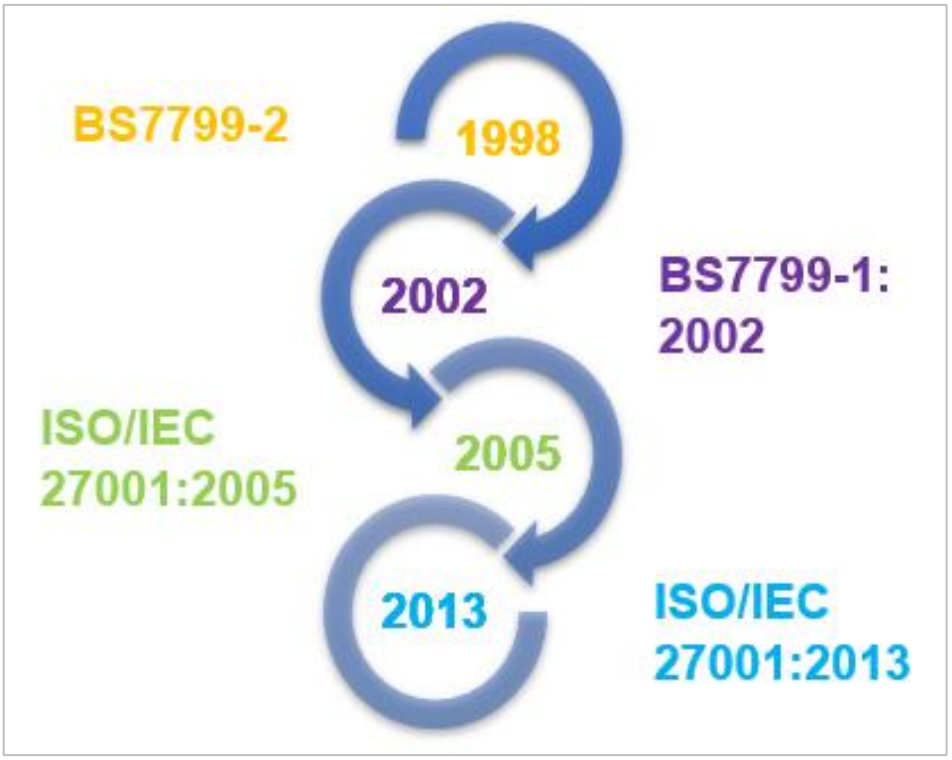
- **Integridad.** Asegura que:
  - No se realizan modificaciones de datos en un sistema por personal o procesos no autorizados.
  - No se realizan modificaciones no autorizadas de datos por personal o procesos autorizados.

- **Disponibilidad.** Asegura que el acceso a los datos o a los recursos de información por personal autorizado se produce correctamente garantizando que los sistemas funcionen cuando se los necesita.

2.2.3. ISO/IEC 27001:2013 SEGURIDAD DE LA INFORMACIÓN

El origen de la Norma ISO27001 está en el estándar británico BSI (British Standards Institution) BS7799-Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005.

Figura 8. Cronología Norma ISO 27001



Elaboración: Carolina Morocho Crespo
Fuente: Magazcitum

En la actualidad las empresas se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes que pueden dañar de forma importante sus sistemas de información y pueden poner en peligro la continuidad del negocio. (Aenor Ecuador, 2014)

Ante estas circunstancias es imprescindible que las empresas evalúen los riesgos asociados y establezcan las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. (Aenor Ecuador, 2014)

La estructura de la norma ISO 27001 se reduce a dos elementos básicos: las cláusulas de requisitos para que una organización funcione alineada con un sistema de gestión, junto con los objetivos de control y los controles de seguridad, que consideran distintos enfoques de protección. (Mendoza, 2015)

Figura 9. Estructura de la ISO 27001

Elaboración: Miguel Ángel Mendoza
Fuente: Seguridad ESET

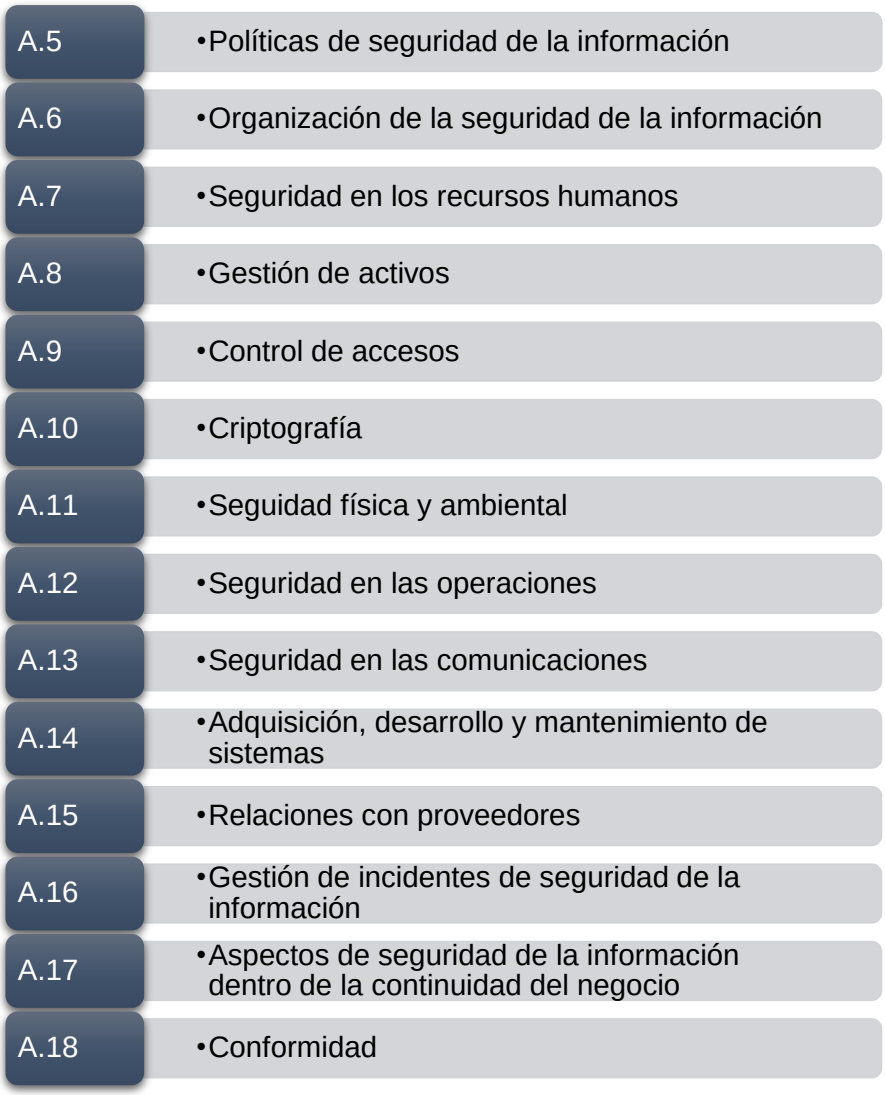
La Gestión de la Seguridad de la Información debe pasar por varios niveles o escalones, cada uno con su coste asociado y contexto de aplicabilidad. Se comienza a perfilar una escala de progresión en lo que ahora conocemos como Sistemas de Gestión de Seguridad de la Información basados en la norma ISO 27001. (ISO27000es, 2012)

La norma ISO 27001 puede ser implementada en cualquier tipo de organización, sea esta grande o pequeña, con o sin fines de lucro, pública o privada. Y es que el principal objetivo de la norma es proporcionar una base para desarrollar políticas de seguridad dentro de las instituciones y ser una práctica para su gestión.
De la misma forma, en la norma ISO 27001 se han definido catorce dominios de controles que cubren la gestión de la seguridad de la información.

Cada categoría principal de controles de seguridad contiene:

- Un objetivo del control qué establece que es lo que se quiere conseguir.
- Uno o más controles que pueden ser aplicados para conseguir el objetivo de control. (Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)

Figura 10. Dominios de seguridad de ISO/IEC 27001:2013



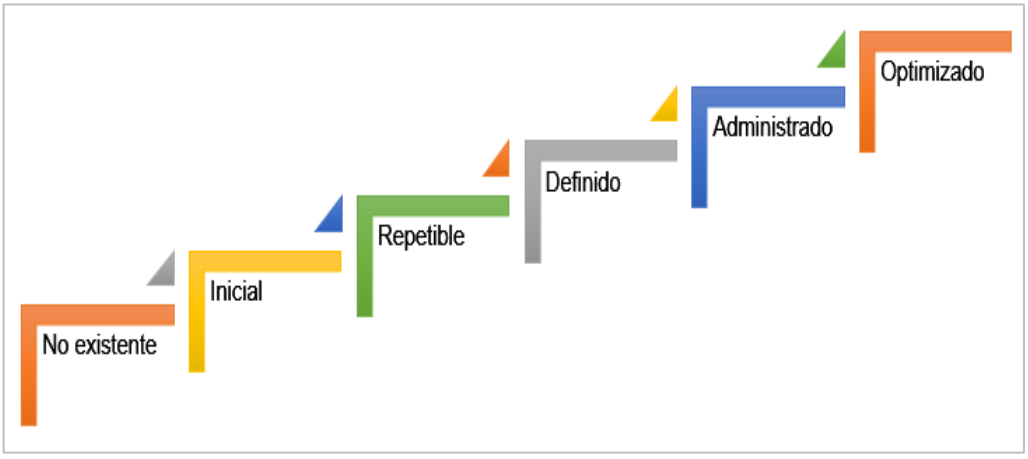
Elaboración: Carolina Morocho Crespo
Fuente: Norma ISO/IEC 27001:2013

Para la evaluación de los controles de la norma ISO/IEC 27001:2013, se considerarán los siguientes niveles de madurez con su respectiva puntuación para el análisis de brecha de seguridad de la información.

- **10 – Optimizado:** La organización ha refinado su cumplimiento a un nivel de buena práctica.
- **8 – Administrado:** La organización regularmente mide su cumplimiento y hace mejoras al proceso de forma regular.

- **6 – Definido:** La organización aplica un enfoque detallado, documentado. Pero no existe medición, ni reforzamiento periódico del mismo.
- **4 – Repetible:** La organización tiene un enfoque consistente, pero en su mayoría no está documentado.
- **2 – Inicial:** La organización tiene un enfoque ad-hoc o desestructurado en esta práctica o estándar.
- **0 – No existente:** No hay evidencia de este estándar o práctica en la organización.

Figura 11. Niveles de madurez de seguridad de la información



Elaboración: Carolina Morocho Crespo
Fuente: Norma ISO/IEC 27001:2013

El análisis de brecha entre el estado actual y el estado deseado para cada métrica definida identifica los requerimientos y prioridades para un plan general u hoja de ruta para asegurar los objetivos y cerrar las brechas. (ISACA, 2016)

De acuerdo a lo expresado por ISACA en el Manual de de Preparación al Examen CISM, el estado deseado al que las organizaciones desean llegar incluye:

- La estrategia de seguridad cuente con la aceptación y respaldo de la alta dirección.
- Las políticas de seguridad estén completas y sean congruentes con la estrategia.
- Se mantengan de manera consistente estándares completos para todas las políticas aplicables.

- Se tengan procedimientos completos y precisos para todas las operaciones importantes.
- Asignación clara de roles y responsabilidades
- Se cuente con una estructura organizacional que otorgue una autoridad apropiada a la gestión de seguridad de la información sin que existan conflictos de interés inherentes
- Controles efectivos han sido diseñados, implementados y mantenidos.
- Métricas de seguridad y procesos de monitoreo efectivos se encuentran en operación.
- Aprobaciones de seguridad apropiadas en los procesos de gestión de cambios.
- Los riesgos son apropiadamente identificados, evaluados, comunicados y gestionados.
- Aspectos regulatorios y legales son conocidos y abordados.
- Procesos de cumplimiento y ejecución efectivos.
- Capacidades de respuesta a incidentes y emergencias probadas y funcionales.
- Capacitación y entrenamiento en seguridad apropiado para todos los usuarios.
- Los activos de información han sido identificados y clasificados según su criticidad y sensibilidad. (ISACA, 2016)

2.2.4. APLICACIONES WEB

El concepto de aplicación Web no es nueva. Uno de los primeros lenguajes de programación para el desarrollo de aplicaciones Web fue el "Perl". Fue inventado por Larry Wall en 1987 antes de que Internet se convirtiera en accesible para el público en general. Pero fue en 1995, cuando el programador Rasmus Lerdorf hizo el PHP a disposición de todo el desarrollo de aplicaciones web realmente despegó. Hoy en día, sin embargo, muchas de estas aplicaciones son desarrolladas en PHP incluyendo Google, Facebook y Wikipedia. (Luján, 2002)

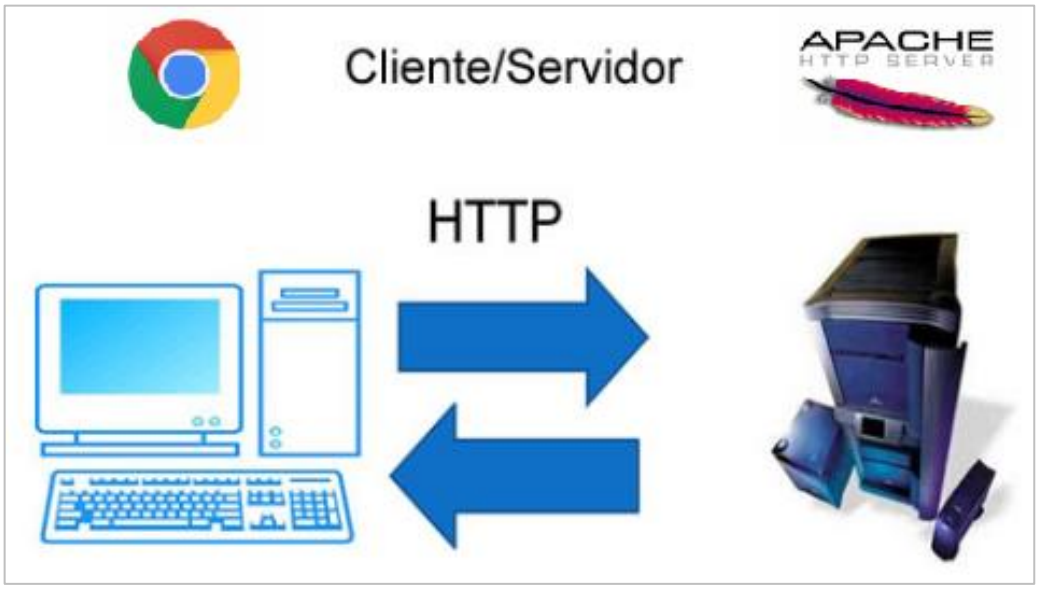
El desarrollo de las aplicaciones web ha tomado un gran impulso en el campo de la ingeniería de software y es que una aplicación web a diferencia de las

tradicionales aplicaciones de escritorio son independientes del sistema operativo, es decir funcionan a través de un navegador web y conexión a internet por lo que no se necesita la instalación o actualización del sistema en los equipos de usuarios de la organización.

Según el autor Pressman, las webapps son poco más que un conjunto de archivos de hipertexto vinculados que presentan información con uso de texto y gráficas limitadas. Sin embargo, desde que surgió web 2.0, las webapps están evolucionando hacia ambientes de cómputo sofisticados que sólo proveen características aisladas, funciones de cómputo y contenido para el usuario final, sino que también están integradas con bases de datos corporativas y aplicaciones de negocio. (Pressman, 2010)

Asimismo el autor Sergio Luján en su libro Programación de aplicaciones web: historia, principios básicos y clientes web expresa que una aplicación web es un tipo especial de aplicación cliente/servidor, donde tanto el cliente (navegador, explorador o visualizados) como el servidor (servidor web) y el protocolo mediante el cual se comunica (HTTP) están estandarizados y no han de ser creados por el programador de aplicaciones. (Luján, 2002)

Figura 12. Arquitectura de aplicaciones web



Elaboración: Denys Tovar
Fuente: (Pressman, 2010)

Entre las principales ventajas que ofrece la utilización de las aplicaciones web se menciona lo siguiente:

- Compatibilidad con diferentes plataformas.
- No requieren de instalación ni actualización en las computadoras.
- Disponibilidad de la aplicación 24/7/365.
- Son aplicaciones generalmente livianas.
- No requieren grandes cantidades de recursos.
- Son portables, para su funcionamiento solo se necesita conexión a internet.
- Múltiples usuarios pueden acceder al mismo tiempo a la aplicación.
- Son aplicaciones autónomas.

2.2.5. HERRAMIENTAS PARA EL DESARROLLO DEL SOFTWARE

Actualmente en el mercado existen una serie de herramientas tecnológicas destinadas al desarrollo de sistemas de aplicación, lo que es de gran ayuda ya que se podrán emplear herramientas que se adapten al proyecto de titulación: "*Desarrollo de una herramienta de software como asistente metodológico para la Evaluación del Control Interno Informático en la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil*"

A continuación se describen las herramientas seleccionadas para el desarrollo del sistema de aplicación antes mencionado:

Framework ZK

Considerando el desarrollo de una aplicación web, se necesita un framework de apoyo para mantener las características de un sitio web estructurado, organizado y dinámico, por lo cual se ha considerado el framework ZK.

ZK es un framework de aplicaciones web diseñado en AJAX, salió al mercado como un software de código libre que permite tener una interfaz de usuario completa desarrollada para aplicaciones web sin usar JavaScript y con poca programación. (ZKOSS, 2016)

Figura 13. Logo ZK Framework

Elaboración: ZKOSS
Fuente: (ZKOSS, 2016)

ZK ofrece un entorno de desarrollo ágil, intuitivo al codificar, fácil de estudiar y aprender, y por permitir una correcta gestión de cambios. Adicional, soporta los principales patrones de desarrollo, MVC o MVVM.

Entre las principales características de ZK podemos mencionar:

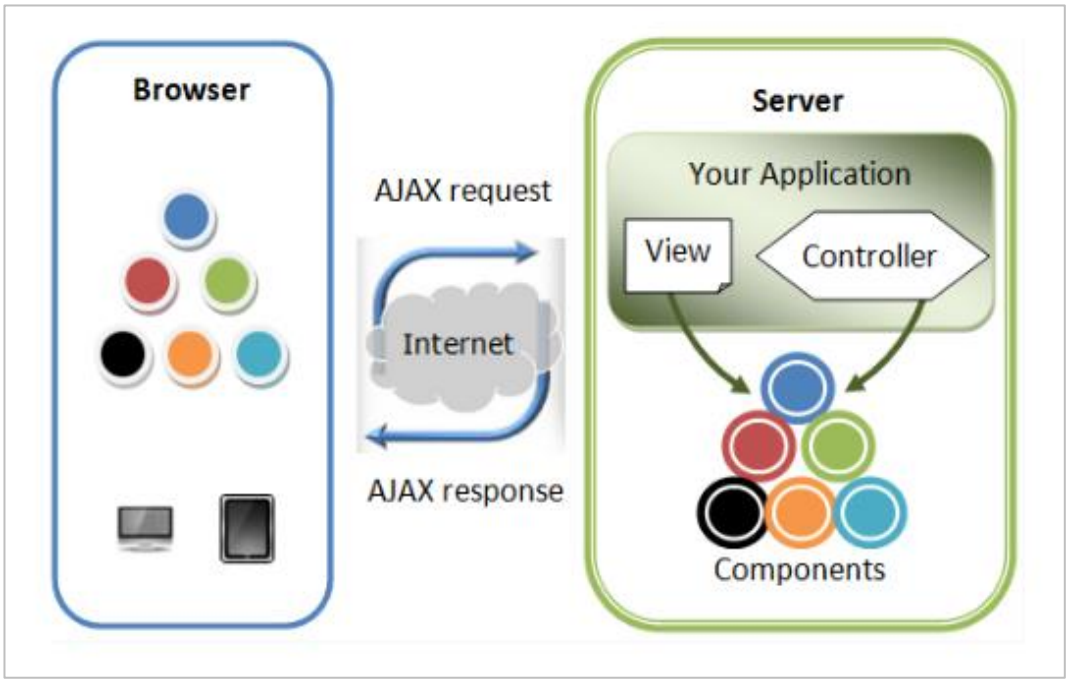
- ZK es un proyecto libre creado por la empresa Potix que nació con el objetivo de simplificar radicalmente el desarrollo de aplicaciones web.
- ZK es un framework de componentes dirigido a través de eventos (EventDriven).
- Con él podemos desarrollar interfaces de usuarios de un modo profesional y extremadamente fácil.
- Está basado en tecnologías abiertas, con una curva de aprendizaje casi plana: HTML y XUL.
- ZK está disponible para ser descargado en www.ZKoss.org en varias modalidades de licencia http://www.zkoss.org/license/.
- Es una plataforma perfecta para montar prototipos y probar código.
- Diseñado para ser Direct RIA (Direct Rich Internet Applications).
- Funciona también con JSP, JSF, Portlet, tecnologías Java EE y se integra con los IDE's más comunes. En el caso de Eclipse por ejemplo con ZK Studio.
- Es completamente factible utilizarlo en entornos altamente explotados por los usuarios.

- Podemos crear simples Richlets web, que son componentes con todo lo necesario para funcionar dentro de otras páginas hechas en cualquier tecnología, respondiendo a una simple URL.
- Es una tecnología completamente madura, que existe como tal desde el año 2005 y ha tenido una comunidad que no ha parado de crecer de una forma increíble.
- Dispone de una empresa por detrás que respalda y coordina todo su desarrollo. (Fundación AtixLibre, 2013)

Con respecto a la arquitectura de ZK tenemos:

- Cuando un navegador visita una página de una aplicación hecha con ZK, ZK crea los componentes que defina el fichero ZUL y los renderiza en el navegador. Puedes manipular los componentes directamente desde el controlador para implementar la lógica de la vista. Todos los cambios que hagas en los componentes será automáticamente reflejado en el navegador del usuario y ZK se encarga de abstraerte de la comunicación.

Figura 14. Arquitectura de ZK



Elaboración: ZKOSS
Fuente: (ZKOSS, 2016)

Entre los clientes y usuarios de ZK se puede mencionar a las principales compañías del mundo: Sony, Oracle, Toyota, eBay, Samsung, TATA Consultancy Services, Huawei, Alcatel, entre otras.

IDE MyEclipse

El IDE que se utilizará en la aplicación web a desarrollarse será MyEclipse en su versión 8.5.

MyEclipse es la solución lógica, basada en complementos Eclipse para la totalidad de su entorno de desarrollo integrado J2EE (IDE) y está disponible para las principales plataformas, incluyendo Windows, Linux y Mac.

Figura 15. Logo MyEclipse

Elaboración: Genuitec
Fuente: (Genuitec, 2016)

MyEclipse integra hoy las tecnologías más innovadoras open-standards para ofrecer un ambiente de desarrollo Web J2EE, XML, UML y bases de datos con una variedad de conectores de servidor para acelerar el desarrollo, implementación, pruebas y portabilidad. MyEclipse ofrece la flexibilidad de elegir la tecnología que necesita en cada capa de aplicación, seleccione los paquetes de tecnología opcional, "off" características que no sean necesarios, accesar modelos Velocity para generar códigos y añadir herramientas comerciales y open-source de terceros para mejorar su experiencia de desarrollo. (Genuitec, 2016)

Base de datos Oracle

Como almacén de los datos para este proyecto, se utilizará la base de datos Oracle 11g Standard Edition R2, conocida por ser una potente herramienta cliente/servidor para la gestión de la base de datos de cualquier proyecto de desarrollo de aplicaciones.

La base de datos Oracle 11g Standard Edition R2 está disponible para una variedad de sistemas operativos e incluyen una serie de herramientas en común para el desarrollo de aplicaciones e interfaces de programación. Uno de los beneficios de Oracle es la facilidad de actualización: solo debe instalar el software de la próxima edición, sin hacer cambios en la base de datos ni en las aplicaciones, y podrá obtener el rendimiento, la escalabilidad, la confiabilidad y la seguridad por las que Oracle es reconocido en un entorno fácil de administrar. (Oracle, 2010)

Figura 16. Logo Oracle

Elaboración: Oracle
Fuente: (Oracle, 2010)

Desarrollado sobre Oracle Database, Oracle Content Database ha sido diseñada para que las organizaciones puedan controlar y gestionar grandes volúmenes de contenidos no estructurados en un único repositorio con el objetivo de reducir los costes y los riesgos asociados a la pérdida de información.

Una Base de datos Oracle tiene una estructura física y una estructura lógica:

- La estructura física se corresponde a los ficheros del sistema operativo.
- La estructura lógica está formada por los tablespace y los objetos de un esquema de Base de datos.

Oracle 11 es una base de datos de características completas para pequeñas y medianas empresas que requieren el desempeño, la disponibilidad y la seguridad de la base de datos #1 del mundo a un bajo costo. Disponible en un solo servidor

o en servidores en clúster con hasta cuatro procesadores, es la opción segura para desarrollar e implementar de manera económica las aplicaciones de la base de datos.

JasperReports
Para la creación de informes se utilizará la herramienta JasperReports.

La biblioteca JasperReports es un motor de informes de código abierto más popular del mundo. Está escrito completamente en Java y es capaz de utilizar los datos procedentes de cualquier tipo de fuente de datos y producir documentos que se pueden ver, imprimir o exportar en una variedad de formatos de documentos incluyendo HTML, PDF, Excel, OpenOffice y Word. (Jaspersoft, 2002)

Figura 17. Logo JasperReports

Elaboración: Jaspersoft
Fuente: (Jaspersoft, 2002)

JasperReports ofrece las características necesarias para generar informes dinámicos, incluyendo la recuperación de datos mediante JDBC (Java Database Connectivity), así como el apoyo a los parámetros, expresiones, variables y grupos. JasperReports también incluye características avanzadas, tales como fuentes de datos personalizadas, scriptles y subinformes. (Jaspersoft, 2002)
Para comenzar a utilizar JasperReports, primero hay que entender qué objetos usa JasperReports para representar el proceso de información a medida que avanza desde el diseño del informe de la redacción del informe:

- **JasperDesign:** Representa la definición de un informe. En la mayoría de los casos, se crea un JasperDesign de una plantilla de informe XML, aunque también se pueden crear mediante programación.

- **JasperReport:** Representa un JasperDesign compilado. El proceso de compilación verifica el diseño de informes y compila el diseño en un objeto JasperReport.
- **JasperPrint:** Representa un informe generado. Se crea un JasperPrint de un JasperReport a través del proceso de llenado en el que un informe se rellena con datos de una fuente de datos. (Jaspersoft, 2002)

2.3. FUNDAMENTACIÓN LEGAL

En la legislación del Ecuador se han establecido leyes, normas, decretos y regulaciones que sirven de amparo o resguardo ante ataques informáticos, ingeniería social, entre otros; así como también, se han especificado artículos que mencionan la importancia de la información y el uso de la tecnología.

A continuación citamos las principales leyes, regulaciones y decretos:

2.3.1. CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

El Código Orgánico Integral Penal (COIP) publicado en el Registro Oficial Suplemento N° 180 del 10 de febrero de 2014 con una última modificación el 14 de marzo del 2016, penaliza las acciones de perjuicio, daño y dolo a través de los artículos de los capítulos segundo y tercero:

Capítulo Segundo Delitos contra los Derechos de Libertad

Sección Sexta

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

Sección Novena

Artículo 185.- Extorsión.- La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia Ministerio de Justicia, Derechos Humanos y Cultos 82 o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 186.- Estafa.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

Artículo 187.- Abuso de confianza.- La persona que disponga, para sí o una tercera, de dinero, bienes o activos patrimoniales entregados con la condición de restituirlos o usarlos de un modo determinado, será sancionada con pena privativa de libertad de uno a tres años.

Artículo 189.- Robo.- La persona que mediante amenazas o violencias sustraiga o se apodere de cosa mueble ajena, sea que la violencia tenga lugar antes del acto para facilitarlo, en el momento de cometerlo o después de cometido para procurar impunidad, será sancionada con pena privativa de libertad de cinco a siete años.

Capítulo Tercero Delitos contra los Derechos del Buen Vivir

Sección Tercera

Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Art. 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

2.3.2. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS

Ley No. 67. R.O. Suplemento 557 del 17 de abril del 2002.

CONGRESO NACIONAL

Considerando:

Que el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.

Que se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

Que a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia.

Que es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio

electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales.

En uso de sus atribuciones, expide la siguiente: **"LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS"**

TÍTULO PRELIMINAR

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Título I
DE LOS MENSAJES DE DATOS
Capítulo I
PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma,

medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 6.- Información escrita.- Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Art. 8.- Conservación de los mensajes de datos.- Toda información sometida a esta Ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:
a. Que la información que contenga sea accesible para su posterior consulta.

b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

2.3.3. LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Capítulo III
NORMAS GENERALES APLICABLES A LOS REGISTROS PÚBLICOS

Art. 23.- Sistema Informático.- El sistema informático tiene como objetivo la tecnificación y modernización de los registros, empleando tecnologías de información, bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive, codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados.

El sistema informático utilizado para el funcionamiento e interconexión de los registros y entidades, es de propiedad estatal y del mismo se podrán conceder licencias de uso limitadas a las entidades públicas y privadas que correspondan, con las limitaciones previstas en la Ley y el Reglamento.

Art. 26.- Seguridad.- Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública.

2.3.4. LEY ORGÁNICA DE EDUCACIÓN SUPERIOR

Art. 32.- Programas informáticos.- Las empresas que distribuyan programas informáticos tienen la obligación de conceder tarifas preferenciales para el uso de las licencias obligatorias de los respectivos programas, a favor de las instituciones de educación superior, para fines académicos.

Las instituciones de educación superior obligatoriamente incorporarán el uso de programas informáticos con software libre.

2.3.5. NORMAS PARA EL CONTROL INTERNO DEL SECTOR PÚBLICO

CÓDIGO 110
NORMAS GENERALES DEL CONTROL INTERNO

110-07 Evaluación del control interno.- La máxima autoridad de cada entidad dispondrá por escrito que cualquier funcionario que tenga a su cargo un programa, proceso o actividad, periódicamente evalúe la eficiencia del control interno y comunicará los resultados ante quien es responsable.

Un análisis periódico de la forma en que ese sistema está operando le proporcionará al responsable la tranquilidad de un adecuado funcionamiento, o la oportunidad de su corrección y fortalecimiento. Si bien la Unidad de Auditoría Interna lleva a cabo revisiones sobre la eficacia del sistema, son fundamentales

los controles efectuados por los funcionarios que tienen bajo su responsabilidad un segmento organizacional, programa, proceso o actividad, los que deben efectuar auto evaluaciones periódicas al sistema de control interno.

2.4. PREGUNTAS CIENTÍFICAS A CONTESTARSE

El presente proyecto de titulación contestará las siguientes preguntas científicas:

- ¿Cuáles son los beneficios que produce una correcta gestión de seguridad de la información en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil?
- ¿Cuáles son los beneficios que tendrán la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil al efectuar la evaluación de su control interno?
- ¿Cómo facilitaría a la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil contar con una herramienta de software que permita ejecutar un análisis de brecha de seguridad de la información?
- ¿Qué daño provocaría no evaluar oportunamente los controles para la gestión de la seguridad de la información en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil?
- ¿Qué impacto tendría en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil la pérdida o robo de información confidencial de docentes y estudiantes?

2.5. DEFINICIONES CONCEPTUALES

Análisis de Brecha: Herramienta de análisis para contrastar el “estado de la situación actual” y el “estado esperado o ideal”. Las diferencias entre ambas situaciones suponen las brechas que se desea eliminar. (Norma ITIL, 2016)

El análisis Gap o análisis de brecha es una herramienta o una técnica que permite una organización de comparar su rendimiento real contra las normas. El análisis

de brecha evalúa la respuesta de la pregunta "¿Dónde estamos?" y se mide contra "¿Dónde queremos estar?" (Al-Mayahi & Mansoor, 2006)

Seguridad de la Información: Consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información y de los sistemas implicados en su tratamiento dentro de una organización. (ISO27000es, 2012)

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (ISACA, 2012)

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable. (ISO27000es, 2012)
Los controles pueden elegirse de los controles de la norma ISO 27001 o de otros conjuntos de controles, o bien se pueden diseñar nuevos controles para cubrir adecuadamente las necesidades específicas. (Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)

Control Interno: Según el modelo COSO, el control interno se define como un proceso efectuado por el consejo de administración, la dirección y el resto de personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento regulatorio. (Committee of Sponsoring Organizations, 2013)

Estándares: Es una publicación que recoge el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología. Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productores,

vendedores, compradores, usuarios y reguladores). En principio, son de uso voluntario, aunque la legislación y las reglamentaciones nacionales pueden hacer referencia a ellos. (ISO27000es, 2012)

De la conceptualización antes descrita, se puede decir que los estándares son modelos o normas estudiadas, revisadas y documentadas que establecen para garantizar el acoplamiento y calidad de elementos construidos independientemente.

Norma ISO 27001: Es un estándar emitido por la Organización Internacional de Normalización (ISO) que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su implementación puede ser en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001. (ISO27000es, 2012)

Información: Es un activo valioso que puede impulsar o destruir su empresa. Si se gestiona de forma adecuada, le permite trabajar con confianza. (Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)

Confidencialidad: La información se divulga sólo a aquellos que tengan derecho a conocerla y sólo puede ser observada por ellos. (ISACA, 2016)

De acuerdo a lo expuesto por ISACA como definición de confidencialidad se puede concluir que la información no debe ni será conocida por personas no autorizadas.

Integridad: La información está protegida contra modificaciones no autorizadas. (ISACA, 2016)
La información no es íntegra cuando no refleja la realidad de las instituciones, lo que podría generar errores en el procesamiento de la información y provocar la toma errónea de decisiones.

Disponibilidad: La información está disponible y se puede utilizar cuando se le requiere, y los sistemas que la proporcionan pueden resistir ataques en forma apropiada. (ISACA, 2016)

En otras palabras, la información no está disponible para poder desarrollar las actividades o es imposible generar la información oportunamente.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO27000es, 2012)

De acuerdo a lo expresado por ISACA, se define al riesgo como la combinación de la probabilidad de un evento y sus consecuencias. (ISACA, 2012)

Incidentes de seguridad de la Información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO27000es, 2012)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO27000es, 2012)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO27000es, 2012)

Fuga de información: Incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma (tanto todos como un grupo reducido).

Herramienta de Software: Programas diseñados para o por los usuarios para facilitar la realización de tareas específicas en la computadora, como pueden ser las aplicaciones ofimáticas (procesador de texto, hoja de cálculo, programa de presentación, sistema de gestión de base de datos...), u otros tipos de software especializados como software médico, educativo, programas de contabilidad, etc.

Análisis: El análisis es una de las etapas del ciclo de vida de un sistema informático. En esta etapa los analistas se encargan de analizar los requerimientos del sistema. Esta etapa centra su atención en la interacción de los usuarios con el sistema. (Alegsa, 2016)

Colección de requerimientos funcionales y no funcionales, con los cuales el desarrollador o desarrolladores del software comprenden completamente la naturaleza de los programas que deben construirse para desarrollar la aplicación, la función requerida, comportamiento, rendimiento e interconexión. (Pressman, 2010)

Diseño: El diseño del software es realmente un proceso de muchos pasos pero que se clasifican dentro de uno mismo. En general, las actividades del diseño se refieren al establecimiento de las estructuras de datos, la arquitectura general del software, representaciones de interfaz y algoritmos. El proceso de diseño traduce requisitos en una representación del software. (Pressman, 2010)

Establecimiento de la estructura y arquitectura para el desarrollo de la herramienta de software.

Desarrollo: Esta actividad consiste en traducir el diseño, en una forma legible por la máquina. La generación de código se refiere tanto a la parte de generación de los ambientes virtuales, como a la parte en la cual se añadirá comportamiento a estos ambientes. Por ejemplo, el lenguaje de programación VRML 2.0 es un lenguaje de modelado en 3D en el cuál se dibuja por medio de generar código de programación de formato y marcado para especificar las características del objeto u objetos que se van agregando a un mundo o entorno virtual. El comportamiento de las escenas virtuales es decir, su funcionalidad, se puede construir a través de algún otro lenguaje de programación, como clases Java o scripts especificados en JavaScript. Todas estas actividades implican generar código. (Pressman, 2010)

En pocas palabras, el desarrollo de una aplicación consiste en traducir la etapa de diseño en una forma entendible por la máquina a través de la codificación en un lenguaje de programación.

Pruebas: El proceso de pruebas se centra en los procesos lógicos internos del software, asegurando que todas las sentencias se han comprobado, y en los procesos externos funcionales, es decir, la realización de la prueba de detección de errores. (Pressman, 2010)

Consiste en asegurar que la herramienta de software funcione de acuerdo a los requerimientos relevados o levantados con la organización.

Implementación: Consiste en poner en marcha la herramienta de software. Es decir, es colocar en ambiente de producción el sistema o cambio desarrollado.

Usuario: En informática, un usuario es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona. (Alegsa, 2016)

En otras palabras, un usuario es el personal dentro de la institución encargado de la manipulación de la herramienta de software.

Java: Lenguaje de programación orientado a objetos desarrollado por Sun Microsystems. La programación en Java, permite el desarrollo de aplicaciones bajo el esquema de Cliente – Servidor, como de aplicaciones distribuidas, lo que hace capaz de conectar dos o más computadoras u ordenadores, ejecutando tareas simultáneamente, y de esta forma lograr distribuir el trabajo a realizar. (Montoya, 2014)

HTML: Lenguaje de Marcado para Hipertextos (HyperText Markup Language) es el elemento de construcción más básico de una página web y se usa para crear y representar visualmente una página web. Determina el contenido de la página web, pero no su funcionalidad. Su versión más actual es la 5.

Lenguaje desarrollado por el CERN que sirve para modelar texto y agregarle funciones especiales (por ej. hipervínculos). Es la base para la creación de páginas web tradicionales. El texto se modela a partir del uso de etiquetas o tags.

También se pueden agregar scripts al código fuente html (generalmente JavaScript, PHP, etc.). (Alegsa, 2016)

World Wide Web: Mejor conocido como WWW o triple W. Sistema de información y documentos vinculada a través de hipertexto e hipermedios a los que se puede acceder por medio de Internet, más específicamente, con un navegador web.

WWW. Telaraña mundial. Fue desarrollado junto con el HTML, la URL y el HTTP (elementos indispensables de la WWW) en 1990 por Robert Cailliau y Tim Berners-Lee en el CERN en Suiza. Permite incorporar multimedia e hipertextos en internet, dando origen a la Web como la conocemos. El nombre original del prototipo era "Enquire Within Upon Everything". Para poder usar esta tecnología se emplean los navegadores, que son los encargados de interpretar las páginas web y mostrarlas en pantalla. (Alegsa, 2016)

Ajax: Acrónimo de Asynchronous JavaScript And XML (JavaScript asíncrono y XML), es una técnica de desarrollo web para crear aplicaciones interactivas o RIA (Rich Internet Applications). Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano. De esta forma es posible realizar cambios sobre las páginas sin necesidad de recargarlas, lo que significa aumentar la interactividad, velocidad y Usabilidad en las aplicaciones. (Montoya, 2014)

Ajax es una tecnología asíncrona, en el sentido de que los datos adicionales se requieren al servidor y se cargan en segundo plano sin interferir con la visualización ni el comportamiento de la página. JavaScript es el lenguaje interpretado (scripting language) en el que normalmente se efectúan las funciones de llamada de Ajax mientras que el acceso a los datos se realiza mediante XMLHttpRequest, objeto disponible en los navegadores actuales. En cualquier caso, no es necesario que el contenido asíncrono esté formateado en XML.

Ajax es una técnica válida para múltiples plataformas y utilizable en muchos sistemas operativos y navegadores, dado que está basado en estándares abiertos como CSS, JavaScript y Document Object Model (DOM). (EcuRed, 2016)

CSS: Hojas de Estilo en Cascada (Cascading Style Sheets), es un mecanismo simple que describe cómo se va a mostrar un documento en la pantalla, o cómo se va a imprimir, o incluso cómo va a ser pronunciada la información presente en ese documento a través de un dispositivo de lectura. Esta forma de descripción de estilos ofrece a los desarrolladores el control total sobre estilo y formato de sus documentos. (World Wide Web Consortium (W3C), 2016)

Las hojas de estilo (en inglés Style Sheets) son la forma que tienen los diseñadores web para definir el aspecto y diseño de las páginas web. Las hojas de estilo suelen ser escritas en el lenguaje CSS (Cascading Style Sheets) y también en XSLT. El CSS es un estándar de la W3C que es ampliamente aceptado entre los navegadores web actuales. (Alegsa, 2016)

CAPÍTULO III

3. PROPUESTA TECNOLÓGICA

En los capítulos descritos anteriormente se han mencionado los antecedentes, causas y consecuencias que sirvieron como base para la propuesta de este estudio. Los incidentes que afectan la seguridad de la información son cada vez más frecuentes en las organizaciones y la inversión que se le está dando a la gestión de la seguridad de la información ya no es considerada, desde el punto de vista financiero, como un lujo sino más bien como una necesidad de asegurar el activo más importante de la organización.

Este proyecto consiste en el desarrollo de una aplicación web que funcione como un asistente metodológico para la evaluación del control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil a través de la ejecución de un análisis de brecha de seguridad de la información. Para esto la aplicación web a desarrollarse tomará como base los 133 controles de la norma internacional de seguridad de la información ISO/IEC 27001: 2013 (última versión liberada y aprobada) y permitirá realizar la evaluación del control interno, realizando una comparación de la situación actual de la carrera contra el estado ideal propuesto por las buenas prácticas.

La implementación de esta herramienta de software proporcionará los siguientes beneficios:

- Permitirá conocer el nivel de madurez de seguridad de la información en la carrera.
- No se requerirá la contratación de especialistas para que ejecuten la evaluación del control interno.
- Proporcionará información relevante y suficiente que sirva de insumo para las autoridades de tal manera que se puedan identificar riesgos tecnológicos y mejorar los controles internos existentes.
- No se requerirá grandes conocimientos en temas de control interno y auditorías informáticas ya que la herramienta de software será amigable para el usuario.

3.1. ANÁLISIS DE FACTIBILIDAD

El estudio de factibilidad es un instrumento que sirve para orientar la toma de decisiones en la evaluación de un proyecto y corresponde a la última fase de la etapa pre-operativa o de formulación dentro del ciclo del proyecto. Se formula con base en información que tiene la menor incertidumbre posible para medir las posibilidades de éxito o fracaso de un proyecto de inversión, apoyándose en él se tomará la decisión de proceder o no con su implementación. (Gestiopolis, 2001)

Para determinar si el proyecto es factible y pueda ser desarrollado, se deberá aprobar los siguientes estudios:

- Factibilidad Operacional
- Factibilidad Técnica
- Factibilidad Legal
- Factibilidad Económica

3.1.1. FACTIBILIDAD OPERACIONAL

En este apartado se determinará si la herramienta de software a desarrollarse es viable operativamente, para ello se considerarán los siguientes aspectos:

- Solución de la problemática planteada
- Población y Muestra
- Procesamiento y Análisis de Encuestas

3.1.1.1. Solución de la problemática planteada

En la actualidad, en el Ecuador se han presentado muchos casos de ataques informáticos a los sistemas de las universidades, instituciones públicas, entre otras; por lo que analizando esta problemática se vio en la necesidad de proponer una herramienta de software que permita realizar la evaluación del control interno a través de la ejecución de un análisis de brecha considerando las buenas prácticas de seguridad de la información propuestas por la norma internacional ISO 27001. Por medio de la herramienta, las autoridades de la carrera obtendrán la situación actual de su control interno lo que les permitirá trabajar en el mejoramiento de sus prácticas de seguridad de la información.

Con fecha mayo del 2016 se presentó el anteproyecto de tesis donde se propuso el tema de evaluación del control interno informático, el documento con la propuesta fue revisado y evaluado por el Ingeniero Mario Sánchez – Docente de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil. Asimismo del conocimiento mantenido por el Ingeniero Sánchez, en la actualidad no existe un sistema en la carrera que permita ejecutar evaluaciones del control interno.

De acuerdo a las reuniones y conversaciones mantenidas con el ingeniero asignado para la revisión del anteproyecto de tesis se logró mejorar la propuesta, llegando así al tema: *"Desarrollo de una herramienta de software como asistente metodológico para la Evaluación del Control Interno Informático en la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil"*

Se mantuvo una entrevista con el Ingeniero Lorenzo Cevallos – Director Encargado de la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil, en donde logramos evidenciar la necesidad de las autoridades en contar con una herramienta tecnológica que les permita gestionar la seguridad de la información y control interno basándose en las buenas prácticas descritas por un estándar internacional como lo es la ISO 27001.

Las autoridades, profesores y personal administrativo de la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil han demostrado gran interés y apoyo para el desarrollo de los proyectos presentados por los estudiantes de titulación.

3.1.1.2. Marco metodológico

La obtención y recolección de la información para el desarrollo de este proyecto de titulación será la INVESTIGACIÓN TECNOLÓGICA.

La investigación tecnológica en las ciencias de la ingeniería presenta una serie de características que la vinculan en forma natural con la innovación tecnológica, lo cual indica que las instancias de promoción inicial de los proyectos de investigación y la evaluación de la investigación tecnológica pueden ser utilizadas

como un instrumento para fomentar la innovación. Con innovación tecnológica se designa la incorporación del conocimiento científico y tecnológico, propio o ajeno, con el objeto de crear o modificar un proceso productivo, un artefacto, una máquina, para cumplir un fin valioso para una sociedad. (Dean, 2015)

Se llegó a la conclusión de utilizar la investigación tecnológica, ya que resulta conveniente este tipo de investigación debido a que satisface las necesidades del presente proyecto de titulación.

Se considera que los docentes de la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil serían de gran aporte para evaluar la factibilidad operativa del presente proyecto de titulación, ya que sus conocimientos sobre el control interno que actualmente maneja la institución y seguridad de la información permitirán que se obtengan respuestas significativas.

3.1.1.2.1. Población y muestra

La población es un conjunto de todos los elementos que estamos estudiando, acerca de los cuales intentamos sacar conclusiones. (Levin & Rubin, 1996)

La población considerada para este proyecto fueron los docentes de la Carrera de Ingeniería de Sistemas Computacionales de la Universidad de Guayaquil, que como ya se expuso en un párrafo anterior, son los indicados para proporcionar información sobre los controles internos implementados y que maneja actualmente la institución.

Tabla III. Población considerada para factibilidad operativa del proyecto

Población	Docentes
Docentes de Carrera Ingeniería en Sistemas Computacionales	73

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Una muestra es una colección de algunos elementos de la población, pero no de todos. (Levin & Rubin, 1996)

Para poder medir la factibilidad operativa del proyecto se realizó una encuesta, la cual fue dirigida a 61 personas de una población de 73 docentes.

Para la determinación del tamaño de esta muestra se utilizó la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Tabla IV. Tamaño de la muestra para evaluar la factibilidad operativa

Descripción de la fórmula	Valores
N = Tamaño de la población	73
σ = Desviación estándar de la población	0.5
Z = Nivel de confianza	1.96
e = Límite de errores	0.05
n = Tamaño de la muestra	61

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Para mayor detalle de la encuesta/cuestionario utilizada para esta evaluación, referirse al Anexo A adjunto a este documento.

3.1.1.2.2. Técnicas de Recolección de Información

Para el levantamiento de la información para evaluar la factibilidad operativa del proyecto de titulación se emplearán los siguientes métodos de investigación:

- Entrevista
- Encuesta

Se consideraron la entrevista y encuestas como técnicas de recolección de información debido a que son las más conocidas, de fácil aplicación y que permiten al investigador obtener información relevante y suficiente, generalmente la entrevista es un dialogo entre el investigador y la persona sujeto de estudio y las encuestas son cuestionarios manejados de forma anónima.

3.1.1.2.3. Procesamiento y Análisis de Encuestas

Pregunta N° 1

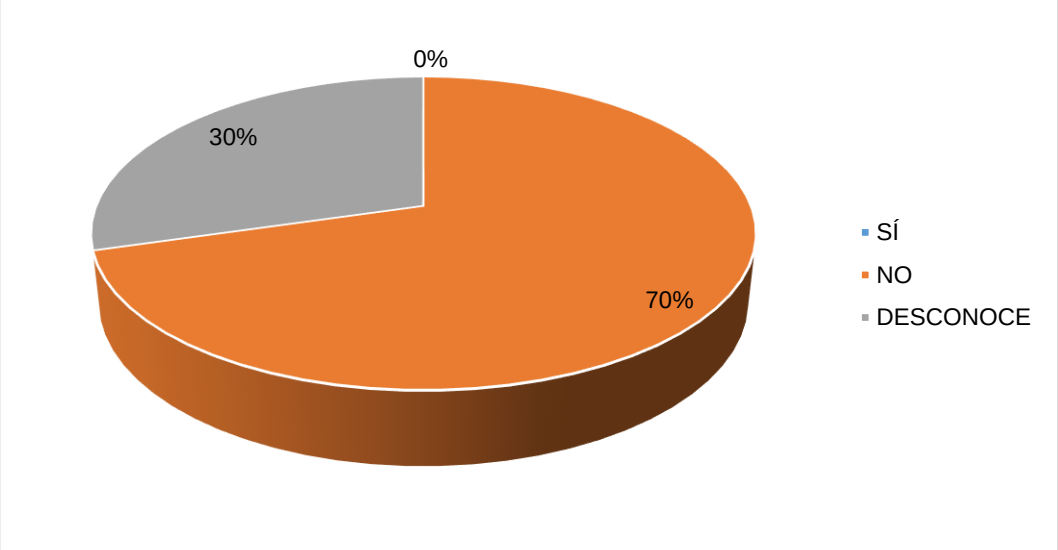
¿CISC ha definido un presupuesto específico aplicado a la gestión de Control Interno y Seguridad de la Información?

Tabla V. Resultado de Encuestas Pregunta N° 1

Detalle	Respuestas	Porcentajes
Sí	0	0%
No	43	70%
Desconoce	18	30%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 1. Resultado de Encuestas Pregunta N° 1



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 1 se puede evidenciar el 70% de los encuestados manifiestan que no existe un presupuesto para gestionar la seguridad de la información y el control interno en la carrera, mientras que el porcentaje restante desconoce si existe tal presupuesto.

Pregunta N° 2

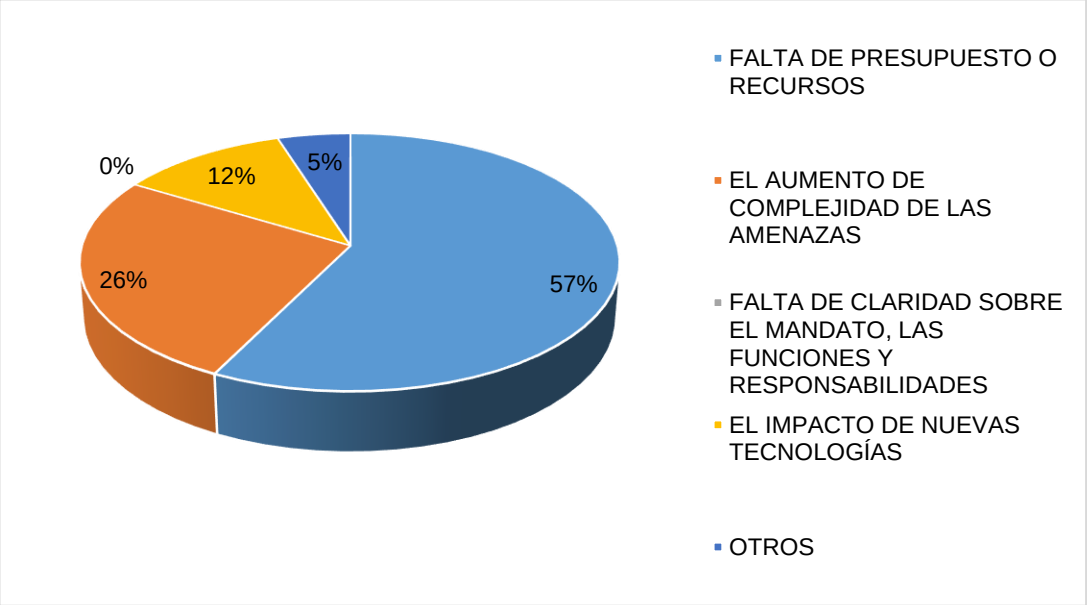
¿Cuáles considera que es el principal obstáculo que CISC enfrenta con respecto a la gestión de seguridad de la información?

Tabla VI. Resultado de Encuestas Pregunta N° 2

Detalle	Respuestas	Porcentajes
Falta de presupuesto o recursos	35	57%
El aumento de complejidad de las amenazas	16	26%
Falta de claridad sobre el mandato, las funciones y responsabilidades	0	0%
El impacto de nuevas tecnologías	7	11%
Otros	3	5%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 2. Resultado de Encuestas Pregunta N° 2



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Los resultados de las encuestas descritas en el Gráfico 2 indican que la falta de recursos y de presupuesto es la principal limitante para gestionar la seguridad de la información en la carrera.

Pregunta N° 3

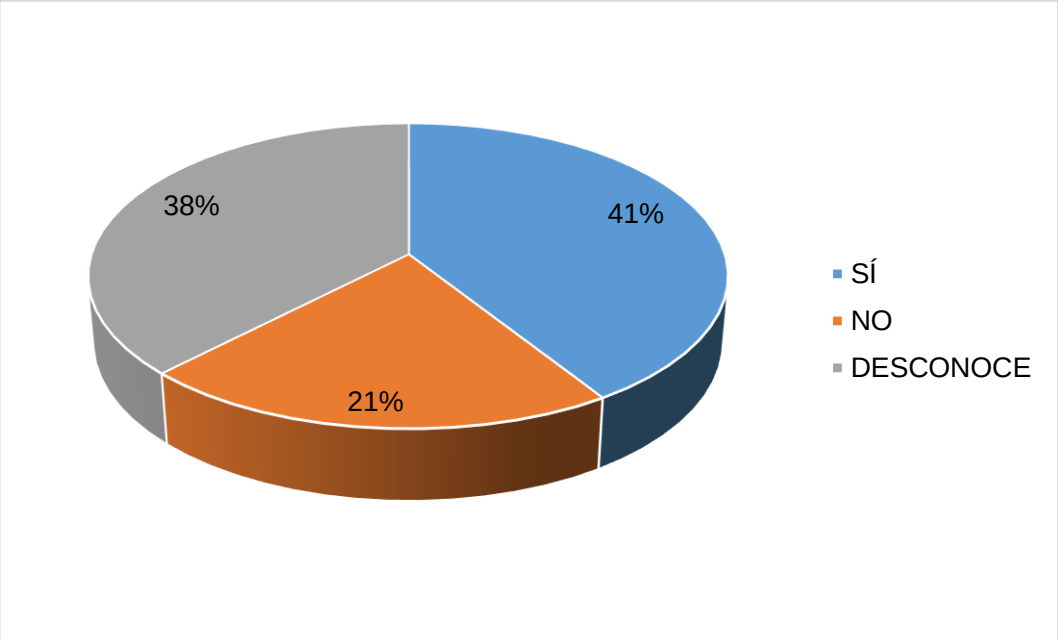
¿CISC cuenta con líneas de investigación de seguridad de la información?

Tabla VII. Resultado de Encuestas Pregunta N° 3

Detalle	Respuestas	Porcentajes
Sí	25	41%
No	13	21%
Desconoce	23	38%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 3. Resultado de Encuestas Pregunta N° 3



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 3 se puede evidenciar que son respuestas con porcentajes similares pero teniendo mayor porcentaje de que la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil si cuenta con líneas de investigación en el área de seguridad de la información.

Pregunta N° 4

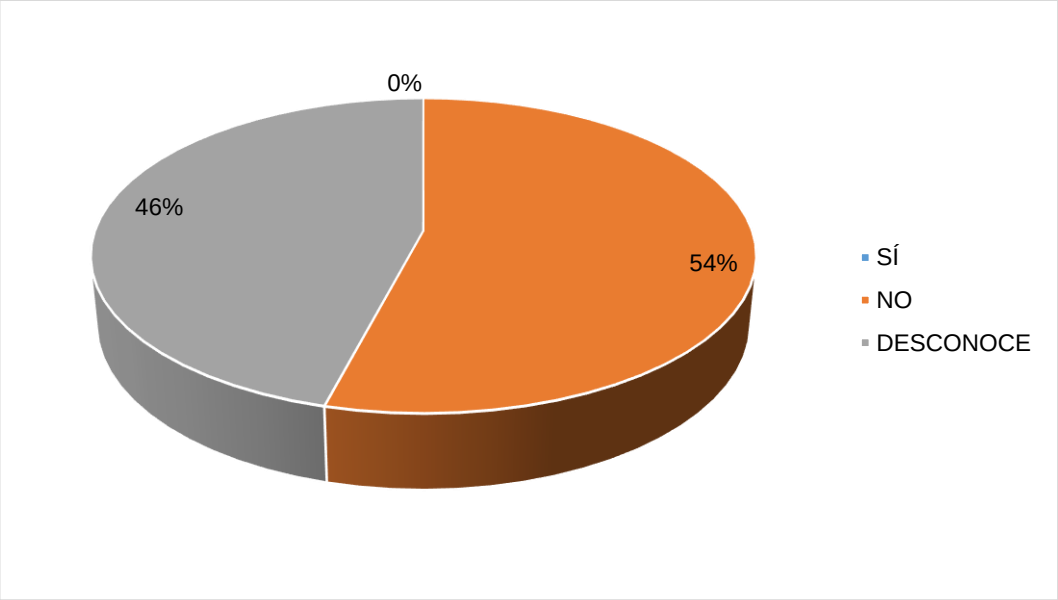
¿CISC ha experimentado una brecha de seguridad durante los últimos 24 meses?

Tabla VIII. Resultado de Encuestas Pregunta N° 4

Detalle	Respuestas	Porcentajes
Sí	0	0%
No	33	54%
Desconoce	28	46%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 4. Resultado de Encuestas Pregunta N° 4



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 4 se puede evidenciar que más de la mitad de los encuestados indican que no han existido en la carrera brechas internas o externas de seguridad en los últimos 24 meses. Sin embargo el Gráfico 4 también muestra un porcentaje considerable indicando que los encuestados desconocen si existieron brechas de seguridad durante los últimos 24 meses.

Pregunta N° 5

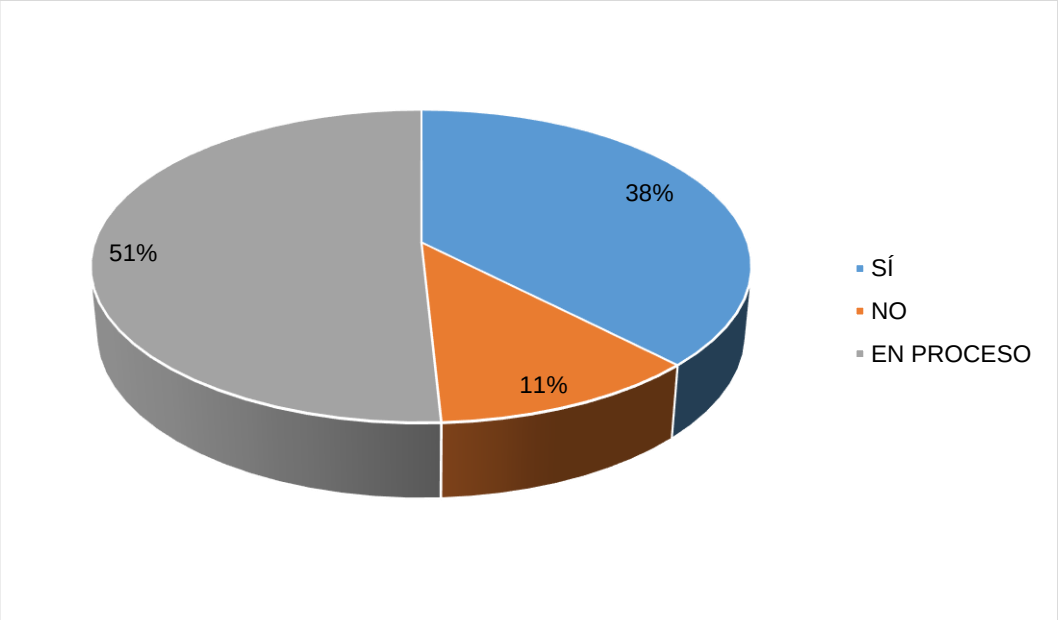
¿CISC cuenta con políticas o normativas para la seguridad de la información?

Tabla IX. Resultado de Encuestas Pregunta N° 5

Detalle	Respuestas	Porcentajes
Sí	23	38%
No	7	11%
En proceso	31	51%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 5. Resultado de Encuestas Pregunta N° 5



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 5 se puede evidenciar que el 51% de los encuestados mencionan que las políticas de seguridad de la información en carrera se encuentran en proceso de documentación y aprobación mientras que otro buen porcentaje, 38% indicó que la carrera si posee normativas de seguridad de la información.

Pregunta N° 6

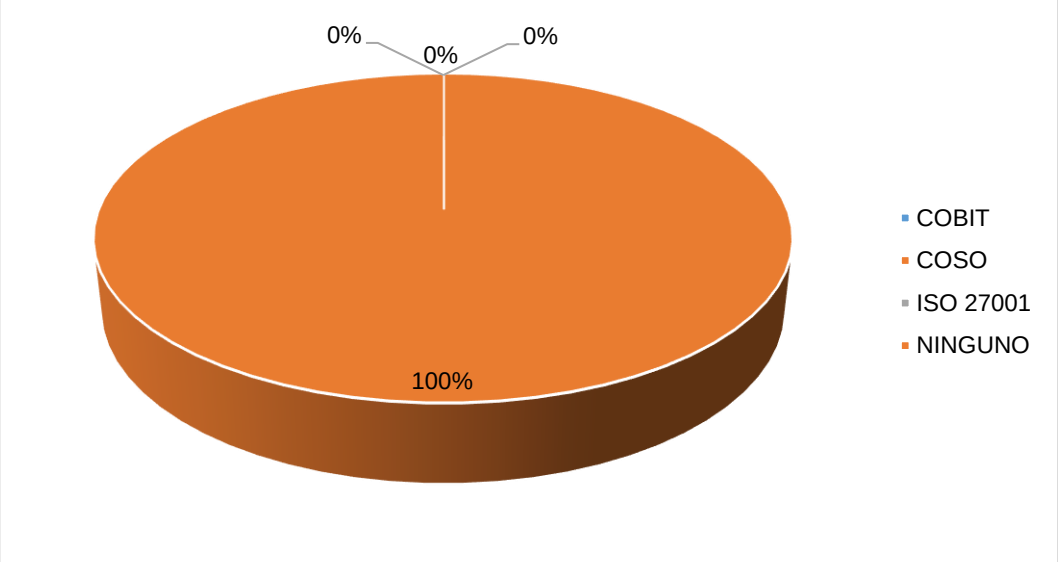
¿CISC se alinea a algún estándar o norma para gestionar la Seguridad de la Información y Control Interno?

Tabla X. Resultado de Encuestas Pregunta N° 6

Detalle	Respuestas	Porcentajes
COBIT	0	0%
COSO	0	0%
ISO 27001	0	0%
Ninguno	61	100%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 6. Resultado de Encuestas Pregunta N° 6



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 6 se puede evidenciar la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil no está alinea a ninguna buena práctica de seguridad de la información o control interno.

Pregunta N° 7

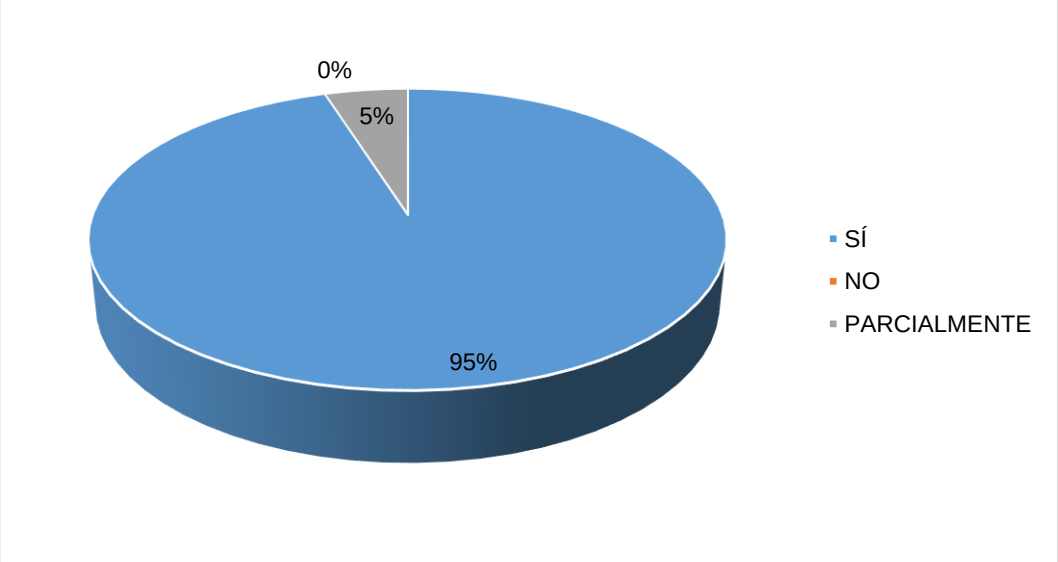
¿CISC ha definido roles y privilegios para el acceso a los sistemas de la institución?

Tabla XI. Resultado de Encuestas Pregunta N° 7

Detalle	Respuestas	Porcentajes
Sí	58	95%
No	0	0%
Parcialmente	3	5%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 7. Resultado de Encuestas Pregunta N° 7



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 7 que un buen porcentaje de los encuestados mencionaron que existen seguridades implementadas para el acceso a los sistemas de información de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil.

Pregunta N° 8

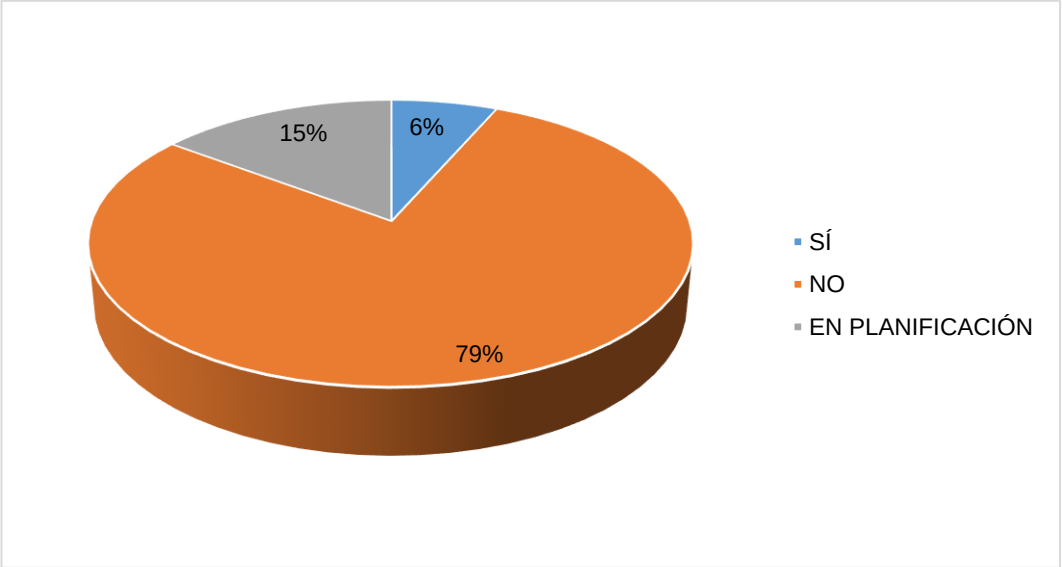
¿Se realizan en CISC eventos relacionados con la concientización/difusión de la Seguridad de la Información?

Tabla XII. Resultado de Encuestas Pregunta N° 8

Detalle	Respuestas	Porcentajes
Sí	4	7%
No	48	79%
En planificación	9	15%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 8. Resultado de Encuestas Pregunta N° 8



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 8 se puede evidenciar que más de la mitad de los encuestados mencionaron que no existen programas de concienciación de temas de seguridad de la información y control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil.

Pregunta N° 9

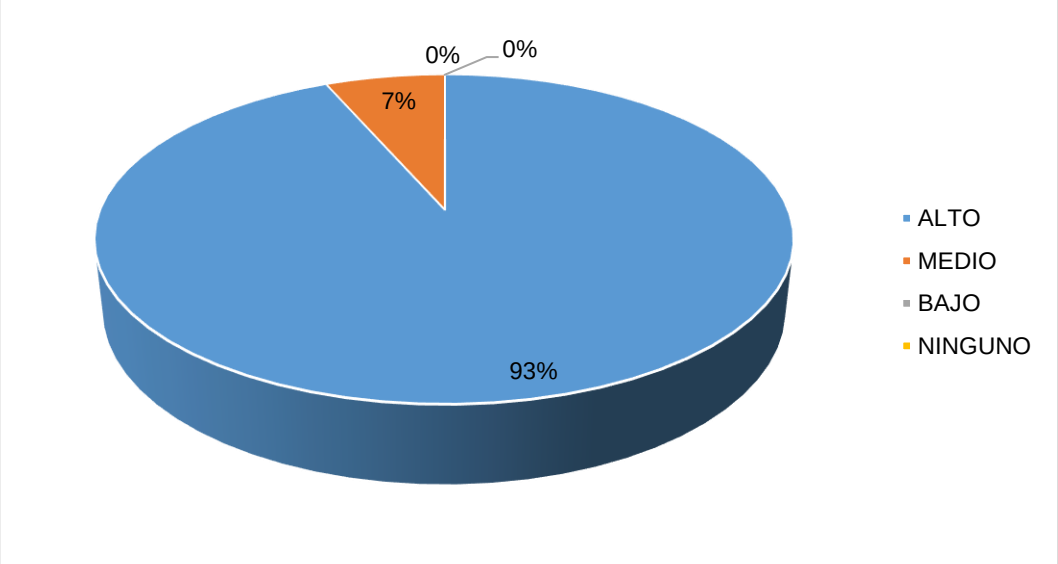
¿Qué grado de interés tendría en una herramienta de software que permita realizar la evaluación del control interno en CISC?

Tabla XIII. Resultado de Encuestas Pregunta N° 9

Detalle	Respuestas	Porcentajes
Alto	57	93%
Medio	4	7%
Bajo	0	0%
Ninguno	0	0%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 9. Resultado de Encuestas Pregunta N° 9



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas, los mismos que se encuentran descritos en el Gráfico 9, se puede observar que un gran porcentaje de encuestados muestran un alto grado de interés en el desarrollo del presente proyecto de titulación.

Pregunta N° 10

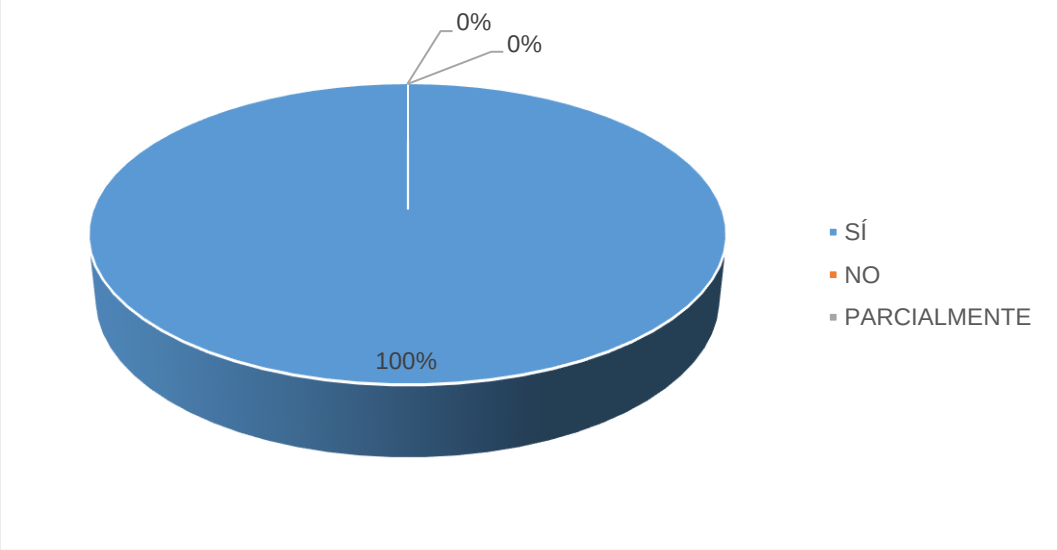
¿Apoyaría la implementación en CISC de una herramienta de software para la evaluación del control interno?

Tabla XIV. Resultado de Encuestas Pregunta N° 10

Detalle	Respuestas	Porcentajes
Sí	61	100%
No	0	0%
Parcialmente	0	0%

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 10. Resultado de Encuestas Pregunta N° 10



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de los datos

Considerando los resultados de las encuestas descritas en el Gráfico 10, es evidente que todos los encuestados apoyarían la implementación de la herramienta de software a desarrollarse.

De acuerdo a todo lo expuesto anteriormente se puede concluir que el proyecto es **operativamente factible.**

3.1.2. FACTIBILIDAD TÉCNICA

Para la factibilidad técnica se examinará el hardware y el software necesarios para llevar a cabo el desarrollo de este sistema de aplicación.

Para la determinación de la factibilidad técnica del presente proyecto de titulación se analizarán los siguientes aspectos:

- Tecnología y solución propuesta.
- Disposición de la tecnología.
- Conocimientos técnicos.
- Cronograma de actividades.

3.1.2.1. Tecnología y solución propuesta

Para el sistema web a desarrollarse se necesitarán las siguientes tecnologías de hardware y software:

Hardware:

A continuación se detalla el hardware necesario para el funcionamiento del sistema de aplicación a desarrollarse:

- **Computadoras personales (PC's)**

  Los requerimientos necesarios para las PCs son los siguientes:

  - Conectividad a la red.
  - Mínimo 2 gigabytes de memoria de RAM.
  - Procesador con más de 8 núcleos.
  - Mínimo 2 gigabytes de espacio en disco duro.
  - Pantalla de 1024 x 768 como mínimo con 256 colores.
  - Mouse.
  - Cualquier sistema operativo.
  - Navegador Web instalado.

La Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil cuenta con equipos de computación los cuales poseen los requisitos mínimos indicados anteriormente para soportar la aplicación.

Software:

A continuación se detalla la clasificación del software necesario para el desarrollo de la herramienta de software:

- Software de programación
- Software de aplicación

Para las clasificaciones de software antes mencionadas, se detalla a continuación la tecnología que se utilizará para el desarrollo del sistema web:

Tabla XV. Herramientas de software a utilizarse en proyecto de titulación

Clasificación	Herramienta de Software	Tipo de Software
Programación	Framework ZK	Software Libre
	JDK 8 Java	Software Libre
	MyEclipse 8.5	Software Libre
	JasperReports	Software Libre
Aplicación	Oracle 11g XE Release 2	Software Libre

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Asimismo, para el funcionamiento de la herramienta de software a desarrollarse no se necesitará información proveniente de sistemas existentes en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil por lo que no se requiere el uso de ningún tipo de interfaces.

3.1.2.2. Disposición de la tecnología

A continuación se mostrará una comparativa entre las herramientas seleccionadas para el desarrollo del sistema web de controles versus dos herramientas existentes en el mercado, las mismas que fueron consideradas de acuerdo a que poseen una gran aceptación en el mercado y una buena demanda de uso en el desarrollo de sistemas de aplicación.

Asimismo, se indicarán las razones de la selección de las herramientas antes mencionadas para el desarrollo del sistema web a desarrollarse.

Comparativa de frameworks actuales:

Tabla XVI. Ventajas y desventajas de Struts

Ventajas	Desventajas
Open Source (Licencia Apache)	Conocimiento profundo de Servlets y JSPs.
Basado en el patrón de diseño MVC.	No abarca todas las capas la aplicación web.
Multiplataforma.	Curva de aprendizaje mediana.
Integración con otros frameworks.	No recomendable para proyectos cortos.
Buena consolidación en el mercado.	Documentación en línea confusa y poco organizada.
Buenas prácticas conocidas.	Pocos libros de Struts.

Elaboración: Carolina Morocho Crespo
Fuente: (Escobedo, 2014)

Tabla XVII. Ventajas y desventajas de ASP.NET

Ventajas	Desventajas
Soporte oficial y amplia documentación.	Software propietario (Microsoft).
Gran comunidad de desarrolladores.	Código cerrado.
Curva de aprendizaje baja.	Para su correcto funcionamiento se requiere de JavaScript y cookies.
Permite el desarrollo de controles propios.	Problemas de seguridad.
Programación modular y orientada a objetos.	Para un desarrollo productivo se requiere un IDE como Visual Studio.
Permite desarrollo con herramientas RAD.	Consumo de recursos muy inefectivo.

Elaboración: Carolina Morocho Crespo
Fuente: (Degiovannini, 2007)

Tabla XVIII. Ventajas y desventajas de ZK

Ventajas	Desventajas
Software de código abierto.	No es recomendado para el desarrollo de aplicaciones que requieren alta interacción como por ejemplo: ○ Videojuegos ○ Edición fotográfica o video ○ Gráficos vectoriales o tridimensionales.
Simplica el desarrollo de aplicaciones web.	
No requiere conocimientos previos en JavaScript o Ajax.	
Prototipado rápido.	
Multiplataforma.	

Elaboración: Carolina Morocho Crespo
Fuente: (Patiño, 2014)

Considerando las ventajas y desventajas de los frameworks evaluados, se llegó a la conclusión de trabajar con el **FRAMEWORK ZK**, ya que entre sus características principales tenemos la facilidad para el desarrollo de aplicaciones web y prototipo rápido.

Comparativa de lenguajes de programación:

Tabla XIX. Ventajas y desventajas de PHP

Ventajas	Desventajas
Sintaxis similar a otros lenguajes.	Necesita un servidor para funcionar.
No se necesita la instalación de PHP en el lado del cliente.	Para aplicaciones de gran tamaño, la programación orientada a objetos es deficiente.
Multiplataforma.	
Libre y gratuito.	Acceso a la base de datos no estandarizado.
Muchos frameworks que facilitan el desarrollo en este lenguaje.	Todo el trabajo se realiza en el servidor y solicitudes pueden llegar a ser ineficientes.

Elaboración: Carolina Morocho Crespo
Fuente: (Rosado, 2015)

Tabla XX. Ventajas y desventajas de Java

Ventajas	Desventajas
Multiplataforma.	Lenguaje interpretado así que es relativamente lento en comparación con otros lenguajes.
Modular al ser orientado a objetos.	Puede ser que no haya JDBC para bases de datos poco comerciales.
Permite la creación de aplicaciones de escritorio, móviles y web.	Velocidad, ya que los lenguajes desarrollados en Java no tienden a ser muy rápidos.
Muchos frameworks que facilitan el desarrollo en este lenguaje.	
Maneja base de datos.	Si se incorporan ciertas herramientas podría requerirse costos adicionales para el desarrollo.
Herramienta libre de licencias.	

Elaboración: Carolina Morocho Crespo
Fuente: (Rosado, 2015)

Tabla XXI. Ventajas y desventajas de JavaServer Pages (JSP)

Ventajas	Desventajas
Ejecución rápida de servlets.	Complejidad de aprendizaje.
Creación de sitios dinámicos.	Rendimiento.
Multiplataforma.	Difícil para los que no conocen Java.
Código estructurado.	Poco práctico para proyectos pequeños.
Integridad con módulos Java.	Mayor tiempo de desarrollo.
Definir etiquetas propias al estilo de HTML.	Interfaz web limitada.

Elaboración: Carolina Morocho Crespo
Fuente: (Rosado, 2015)

Una vez realizada la evaluación de los lenguajes de programación, así como la revisión y análisis de las ventajas y desventajas se llegó a la conclusión de trabajar

con el **LENGUAJE DE PROGRAMACIÓN JAVA**, en razón de que se ajusta al software a desarrollarse y además se mantiene un amplio conocimiento y experiencia sobre esta tecnología.

Comparativa de IDEs actuales

Tabla XXII. Ventajas y desventajas de Eclipse

Ventajas	Desventajas
Amplio Soporte.	Puede llegar a ser confuso para los nuevos desarrollares.
Gran número de plug-ins.	
Código abierto gratuito bajo la licencia pública Eclipse.	La instalación puede resultar completamente desconcertante.
Tecnologías auxiliares como Javascript, base de datos, etc.	
Multiplataforma.	

Elaboración: Carolina Morocho Crespo
Fuente: Página Oficial de Eclipse

Tabla XXIII. Ventajas y desventajas de MyEclipse

Ventajas	Desventajas
Facilita la programación con aspectos debido a que maneja un entorno gráfico.	Dependiendo de la versión puede llegar a tener costos de licenciamiento.
Herramienta más estable para el manejo de aspectos en comparación con herramientas existentes.	Puede llegar a ser excesivamente sensible en muchos puntos de configuración.
Mejoras con cada actualización.	Puede llegar a ser un poco pesado para levantarse y trabajar con él.
Certificado en plataformas Windows, Linux y OS X Apple.	

Elaboración: Carolina Morocho Crespo
Fuente: (Genuitec, 2016)

Tabla XXIV. Ventajas y desventajas de NetBeans

Ventajas	Desventajas
Diseño limpio.	No tiene soporte para Android.
Multiplataforma.	Todos los proyectos son de nivel superior.
Código abierto gratuito bajo la licencia Common Development Distribution.	Consumo considerable de recursos del sistema.
Facilidad de uso.	No cuenta con interfaz para la creación de botones y similares.
Perfecto entorno de desarrollo.	Carece de soportes para webapps.
Descripción bastante completa de los errores de programación.	Lenguaje de programación muy pesado.

Elaboración: Carolina Morocho Crespo
Fuente: Página Oficial de Netbeans

Una vez expuestas cada una de las ventajas y desventajas de los IDEs revisados, se llegó a la conclusión que el **IDE MYECLIPSE** se ajusta de manera adecuada y precisa a este proyecto de titulación facilitando la codificación y el uso amigable con el desarrollador.

Adicionalmente, el IDE MyEclipse fue seleccionado en razón de que se mantiene gran experiencia y amplios conocimientos sobre esta herramienta por lo que facilitará el desarrollo.

Comparativa de base de datos actuales

Tabla XXV. Ventajas y desventajas de Oracle

Ventajas	Desventajas
Base de datos muy popular.	Licencia Propietario.
Base de datos más confiable del mercado.	Una mala configuración ofrece resultados desfavorables.
Gestión de múltiples bases de datos.	Necesidad de ajustes.

Ventajas	Desventajas
Alto rendimiento.	Elevado costo de la información para consultas y últimamente han comenzado a aparecer buenos libros sobre asuntos técnicos.
Base de datos con más orientación hacia Internet.	

Elaboración: Carolina Morocho Crespo
Fuente: (Rosado, 2015)

Tabla XXVI. Ventajas y desventajas de Microsoft SQL Server

Ventajas	Desventajas
Fiabilidad a la hora de recuperar datos.	Utilización de muchos recursos computacionales.
Procedimientos almacenados.	Licencia Propietario.
Soporte de transacciones.	Requiere un sistema operativo Windows.
Entorno gráfico de administración.	No maneja comprensión de datos por lo que ocupa mucho espacio en disco.
Permite trabajar en modo cliente-servidor	Solo permite alojar un máximo de 64 GB.

Elaboración: Carolina Morocho Crespo
Fuente: (Rosado, 2015)

Tabla XXVII. Ventajas y desventajas de MySQL

Ventajas	Desventajas
Base de datos con licencia pública y propietaria.	Base de datos muy limitada.
Integración perfecta con PHP.	No soporta integridad relacional ni transacciones en aplicaciones web no muy complejas
Mayor rendimiento.	
Sin límites en tamaño de registros.	
Facilidad de exportación e importación de datos	Los privilegios de una tabla no se borran automáticamente.

Elaboración: Carolina Morocho Crespo
Fuente: (Rodríguez, 2010)

Se realizó la evaluación de las bases de datos, considerando cada una de sus ventajas y desventajas que ofrecen llegando a la conclusión de trabajar el proyecto de titulación con la **BASE DE DATOS ORACLE**. Si bien esta herramienta no es open source posee alto rendimiento y se acopla perfectamente con las aplicaciones web. Asimismo se mantiene experiencia y amplios conocimientos en esta base de datos lo que facilitará el desarrollo del proyecto de titulación.

3.1.2.3. Conocimientos técnicos

Para el desarrollo de la aplicación web no solo las herramientas son parte importante de este proyecto de titulación sino también debemos considerar los conocimientos técnicos que se deben poseer para el uso de dicha tecnología. Es por este motivo que las herramientas presentadas y mencionadas anteriormente fueron seleccionadas considerando la experiencia y conocimiento que se mantiene de las mismas, permitiendo realizar el desarrollo de la herramienta de software en el tiempo programado.

3.1.2.4 Cronograma de actividades

Para evaluar la factibilidad técnica de la herramienta de software también es importante considerar el tiempo establecido para la ejecución del proyecto.

Para ello se estableció un cronograma de actividades, el mismo que se encuentra detallado en el Anexo B adjunto a este documento.

De acuerdo a todo lo expuesto sobre tecnología y solución propuesta, disposición de la tecnología, conocimientos técnicos y tiempo estimado se puede concluir que el presente proyecto de titulación es **técnicamente factible**.

3.1.3. FACTIBILIDAD LEGAL

En un capítulo anterior se consideraron las leyes, normas y regulaciones existentes en el Ecuador que apoyan legalmente el desarrollo de este proyecto de titulación, las mismas que mencionamos:

- CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)
- LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS

- LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS
- LEY ORGÁNICA DE EDUCACIÓN SUPERIOR
- NORMAS PARA EL CONTROL INTERNO DEL SECTOR PÚBLICO

En cuanto a las herramientas de software que se emplearán en el desarrollo de este proyecto se puede mencionar que en su mayoría son de tecnología open source (Software de código abierto).

Un software de código abierto es un software que se puede utilizar libremente, cambiado, y se comparte por cualquier persona. Un software de código abierto es hecho por muchas personas, y se distribuye bajo licencias que cumplen con la definición de código abierto. (OpenSource.org, 2016)

La herramienta de software a desarrollarse no infringe ninguna ley del Ecuador y se garantiza que no se empleará tecnología pirata, el propósito del sistema web se enfoca básicamente en aportar a la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con una herramienta tecnológica que le permita realizar la evaluación de su control interno en tiempo real y sin requerir la contratación de un especialistas en esta tarea.

De acuerdo a todo lo expuesto sobre las leyes del Ecuador y el uso de la tecnología, se puede concluir que el presente proyecto de titulación es **legalmente factible**.

3.1.4. FACTIBILIDAD ECONÓMICA

Para el desarrollo de este proyecto de titulación se han considerado los siguientes rubros por recursos utilizados:

Tabla XXVIII. Presupuesto del Proyecto

Recursos	Detalle	Cantidad	Valor unitario	Subtotal
Recursos Humanos	Estudiante (por 3 meses)	1	400.00	1,200.00

Recursos	Detalle	Cantidad	Valor unitario	Subtotal
Recursos Software	Servicio de Internet (por 3 meses)	1	35.00	105.00
Recursos Varios	Alimentación (por 3 meses)	1	10.00	200.00
	Movilización (por 3 meses)	1	5.00	60.00
Otros	Copias	500	0.02	10.00
	Impresiones	500	0.10	50.00

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Para el desarrollo del proyecto se necesita una inversión de 1,625.00 dólares americanos, valor realmente mínimo considerando los beneficios que aportará la herramienta de software a la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil y considerando además los altos costos que implicaría la contratación de consultorías especializadas en control interno informático.

Por lo antes expuesto, se puede concluir que el desarrollo de este proyecto de titulación es **económicamente factible.**

3.2. ETAPAS DE LA METODOLOGÍA DEL PROYECTO

Para el proceso de desarrollo de la herramienta se seleccionó la metodología basada en el modelo de cascada. Se considera que esta metodología se adapta al presente proyecto, permitiendo obtener un producto en el tiempo establecido y de gran utilidad para la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil.

A continuación se describen las etapas del proyecto de acuerdo a la metodología de cascada seleccionada para el desarrollo del proyecto:

3.2.1. FASE DE ANÁLISIS

En esta etapa del proyecto se describirán los requerimientos funcionales para la herramienta de software levantados con base a la investigación inicial del problema, identificación de necesidades, antecedentes del problema, alcance, justificación, entre otros.

3.2.1.1. Requerimientos funcionales de la herramienta de software

Se detallan los requisitos funcionales que se incorporarán en la herramienta de software:

Tabla XXIX. Requerimientos funcionales de la herramienta

Código	Descripción del Requerimiento
RF01	Controlará la seguridad de accesos de usuarios. Esta actividad será realizada por el administrador del sistema: o Creación de usuarios o Modificación de usuarios o Eliminación de usuarios o Asignación de perfiles de acceso
RF02	La herramienta será multi-departamental, ya que la evaluación del control interno también se podrá efectuar en diferentes departamentos/unidades de la Carrera. Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.
RF03	Permitirá dar asistencia a otras normas como por ejemplo ISO 22301, siempre y cuando la estructura del catálogo de los controles sea similar a la establecida en la norma ISO 27001. Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.
RF04	La herramienta de software permitirá la configuración los niveles de madurez e ingreso del puntaje o peso por cada nivel. Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.

Código	Descripción del Requerimiento
RF05	Servir de asistente metodológico para la evaluación del control interno de la Carrera a través de la revisión contra las buenas prácticas de la norma ISO 27001. La herramienta ofrecerá la posibilidad de realizar evaluaciones de cumplimiento de diferentes catálogos, donde cada catálogo puede contener requisitos de estándares, leyes o reglamentos aplicables a la institución.
RF06	La herramienta será capaz de generar listados de controles de la norma ISO 27001 y el estado actual.
RF07	La herramienta será capaz de generar gráficas estadísticas con el estado actual de los controles contra el estado ideal definido.

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

3.2.2. FASE DE DISEÑO

En esta etapa del proyecto se efectuará el diseño que contendrá la herramienta de software considerando los requerimientos funcionales descritos en la fase de análisis.

El diseño contará con la definición de actores, diagrama general de caso de uso, definición de casos de uso y diagrama del modelo de entidad relación.

3.2.2.1. Definición de actores

A continuación se describen los diferentes actores identificados para el uso de esta herramienta de software:

- **Nombre del actor:** Administrador
  Descripción: Este actor se encarga de realizar las tareas de administración de la herramienta así como también podrá realizar las

tareas de un usuario final. Entre las tareas que podrá ejecutar este actor tenemos:

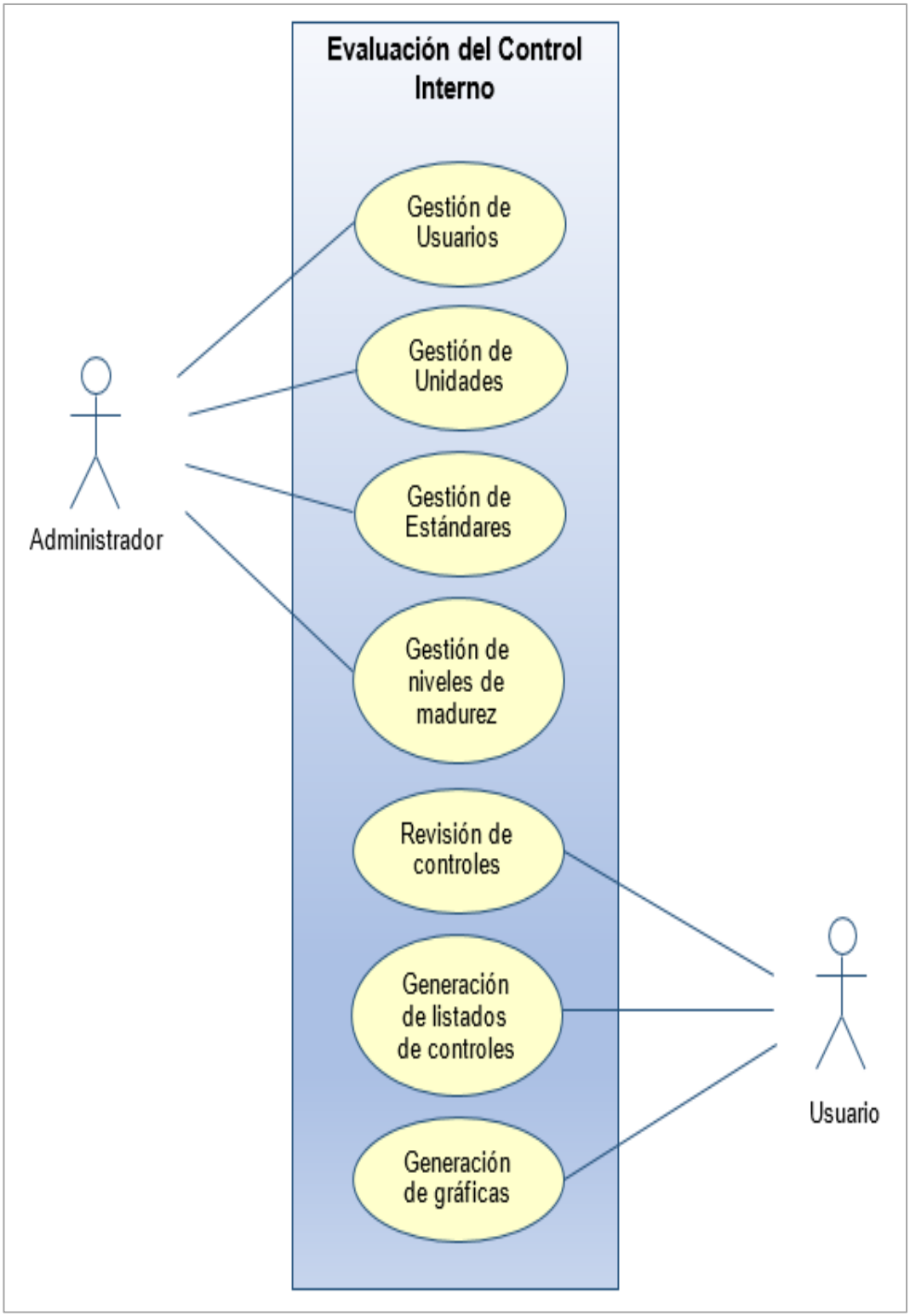
- Gestión de usuarios
  - Alta de usuarios.
  - Modificación de usuarios.
  - Baja de usuarios.
  - Asignación de perfiles de accesos.
- Gestión de unidades
  - Alta, modificación y baja de departamentos/unidades de la carrera.
- Gestión de estándares
  - Alta, modificación y baja de estándares.
- Gestión de niveles de madurez
  - Alta, modificación y baja de niveles de madurez.

- **Nombre del actor:** Usuario
  Descripción: Este actor representa al usuario final que hará uso de la herramienta de software, el cual puede ser cualquier persona involucrada en la evaluación del control interno de la carrera. Este actor no podrá ser capaz de realizar las tareas de administración de la herramienta. Entre las tareas que podrá ejecutar este actor tenemos:
  - Revisión de los controles
    - Evaluación del control interno.
  - Generación de listados de controles
    - Listados con los controles evaluados.
  - Generación de gráficas
    - Gráficas que contienen la evaluación del control interno actual versus el estado ideal o deseado.

3.2.2.2. Diagrama general de casos de uso

En el diagrama general de caso de uso se muestra los requerimientos funcionales que contendrá la herramienta de software y la interacción que tiene con los actores principales: Administrador y Usuario.

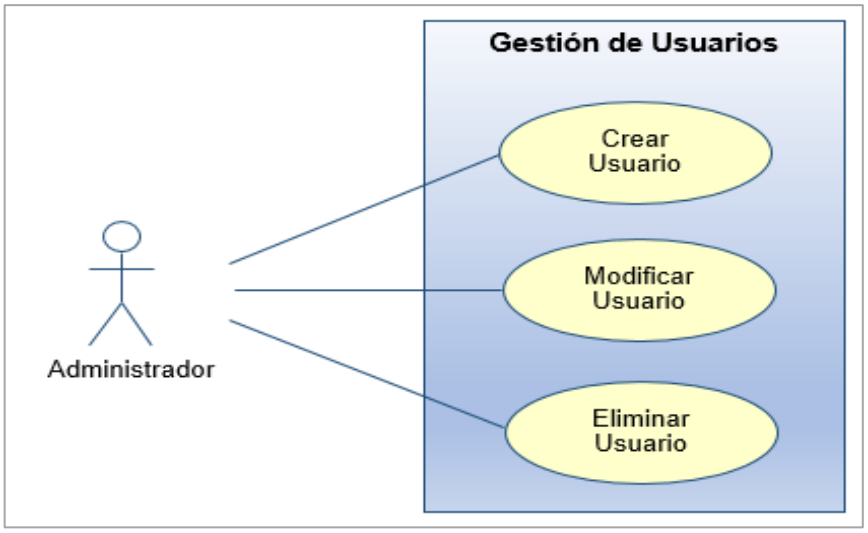
Figura 18. Diagrama general de casos de uso



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

3.2.2.3. Caso de Uso: Gestión de Usuarios

Figura 19. Caso de Uso Gestión de Usuarios



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF01

Actor:

- Administrador

Descripción:

El sistema deberá ser capaz de gestionar la seguridad de accesos de los usuarios. La autenticación a la herramienta se realizará a través de un usuario, contraseña y además contralará el tipo de acceso. Para la creación de un usuario se necesitará lo siguiente:

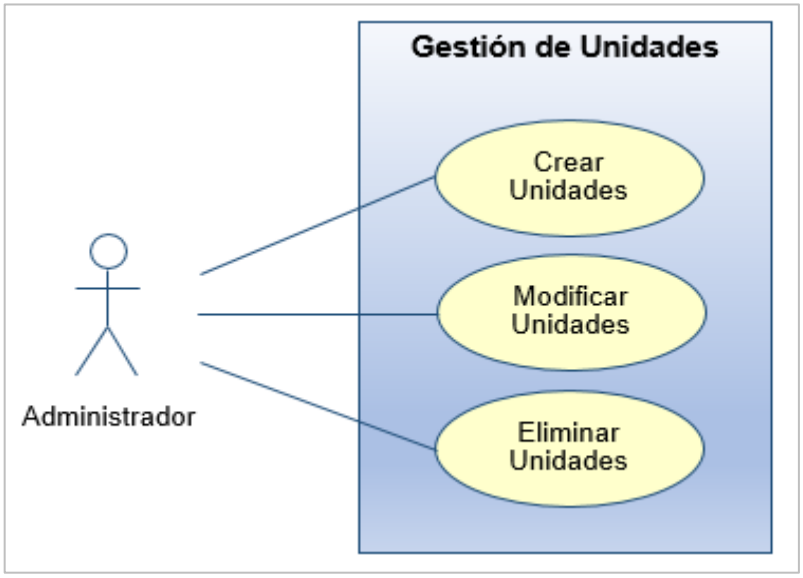
- Identificador del usuario
- Cédula de identidad
- Nombres del usuario
- Cargo
- Correo electrónico
- Contraseña temporal
- Perfil

El Usuario Administrador será el único que puede ser capaz de gestionar los usuarios de la herramienta (Creación-Modificación-Eliminación). Los usuarios finales solo podrán realizar el cambio de su contraseña.

Para revisar los casos de uso detallados para la Gestión de Usuarios referirse al Anexo C de este documento.

3.2.2.4. Caso de Uso: Gestión de Unidades

Figura 20. Caso de Uso Gestión de Unidades



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF02

Actor:

- Administrador

Descripción:

La herramienta será multi-departamental, ya que la evaluación del control interno no solo podrá ser realizada a nivel general en la Carrera de Ingeniería en Sistemas Computacionales sino también puede aplicarse a las diferentes

unidades/departamentos de la misma. Los datos a recoger de una unidad/departamento son los siguientes:

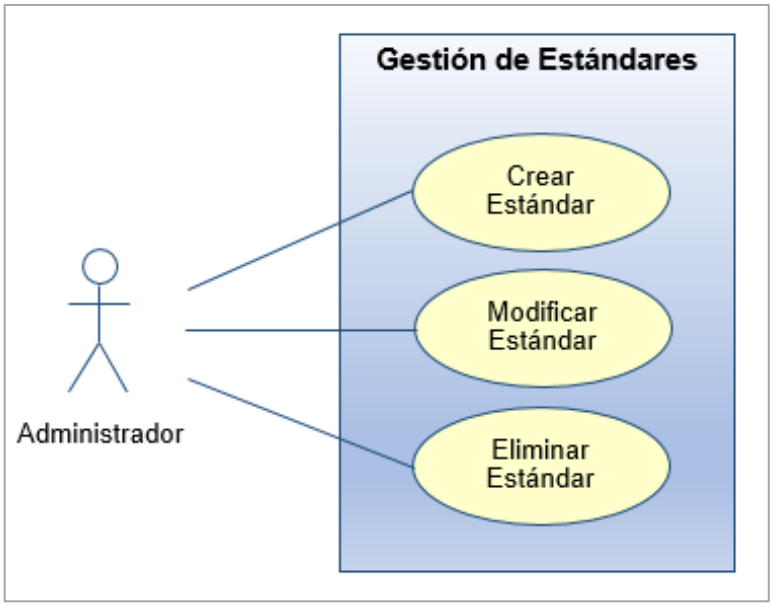
- Nombre de la unidad
- Descripción de la unidad
- Responsable de la unidad

Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.

Para revisar los casos de uso detallados para la Gestión de Unidades referirse al Anexo D de este documento.

3.2.2.5. Caso de Uso: Gestión de Estándares

Figura 21. Caso de Uso Gestión de Estándares



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF03

Actor:

- Administrador

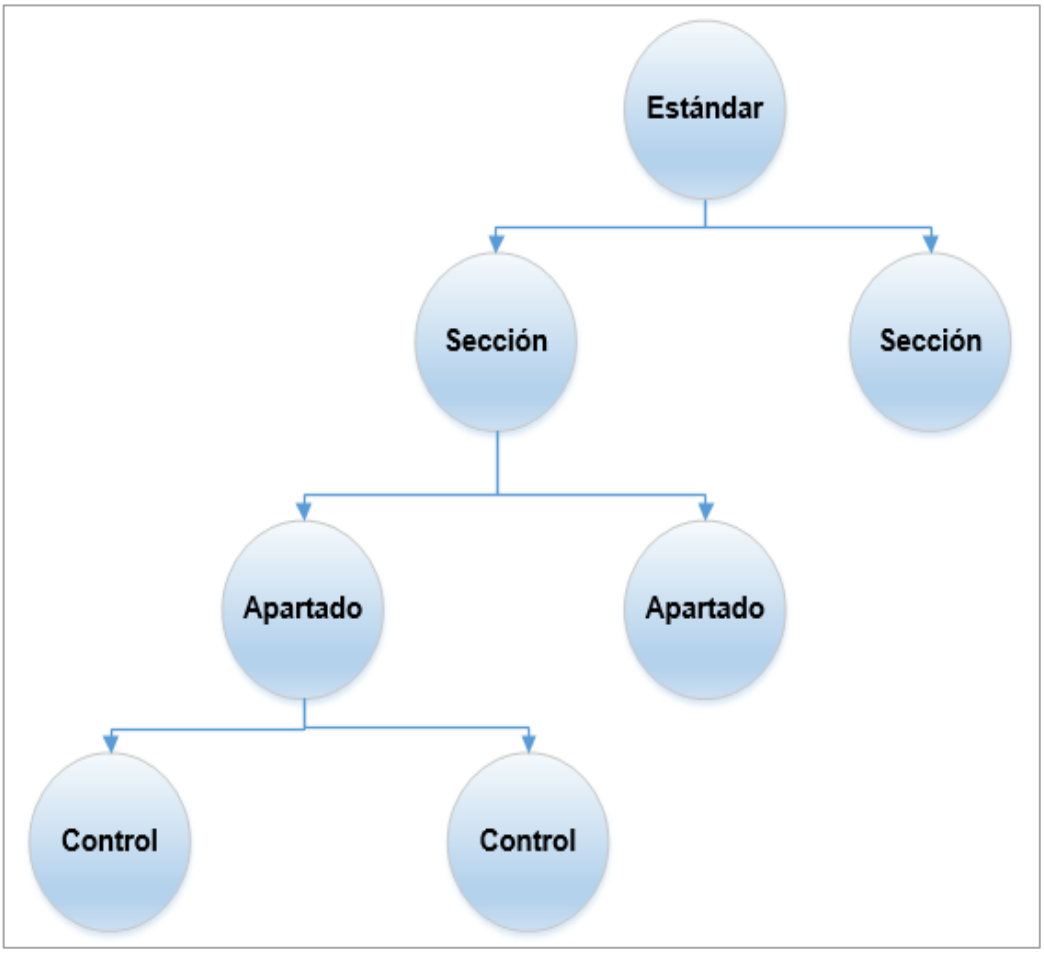
Descripción:

La herramienta será capaz de gestionar nuevos estándares, siempre y cuando mantengan una estructura similar a la establecida en la norma ISO 27001 y que se revisará a continuación:

Para poder crear nuevos estándares en la herramienta, deberán mantener la siguiente estructura:

- **Estándar:** Contiene el catálogo del estándar.
- **Secciones:** Contienen los dominios del estándar.
- **Apartados:** Contiene los objetivos de control del estándar.
- **Controles:** Contiene los elementos a evaluar.

Figura 22. Estructura de los estándares



Elaboración: Carolina Morocho Crespo
Fuente: *(Cómite técnico AEN/CTN 71 - Tecnología de la Información, 2015)*

Siguiendo la estructura antes descrita, se detalla la composición de la norma o estándar ISO 27001:2013.

- 1 Estándar
- 15 dominios (secciones)
- 34 objetivos de controles (apartados)
- 133 controles

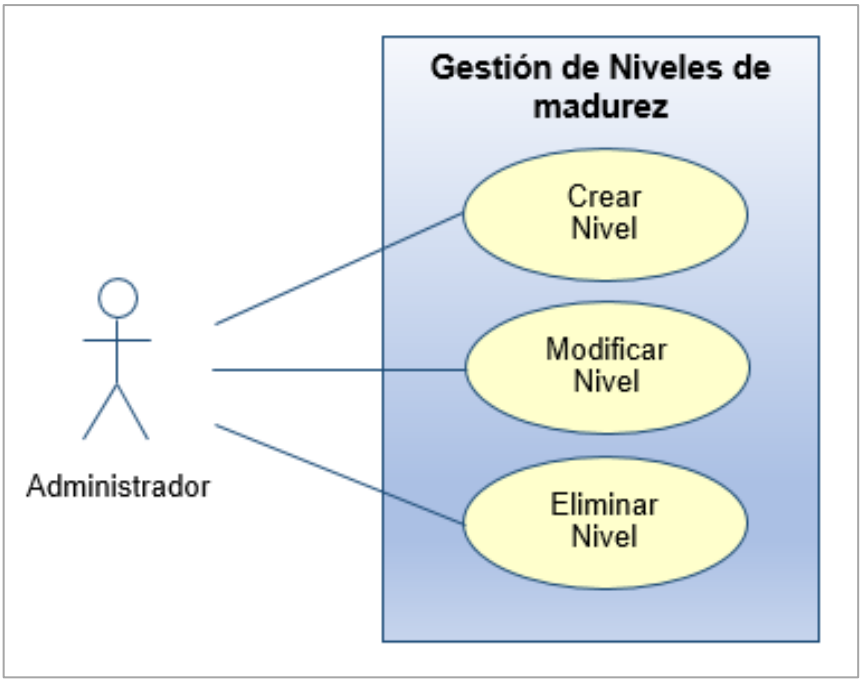
Para un mayor detalle de la estructura de la norma ISO 27001, referirse al Anexo J adjunto a este documento.

Debido a que la herramienta se basa en la evaluación de los controles de la norma ISO 27001, esta información no podrá ser modificada ni eliminada.

Para revisar los casos de uso detallados para la Gestión de Estándares referirse al Anexo E de este documento.

3.2.2.6. Caso de Uso: Gestión de Niveles de Madurez

Figura 23. Caso de Uso Gestión de Niveles de Madurez



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF04

Actor:

- Administrador

Descripción:

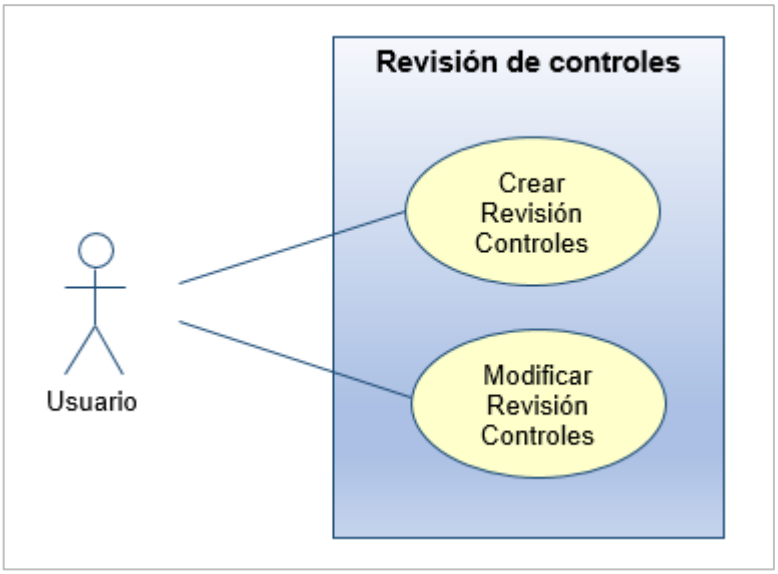
La herramienta permitirá configurar los niveles de madurez de los controles y asignarles el respectivo porcentaje de completitud para cada nivel. Los niveles de madurez permitirán realizar la evaluación del control interno y la configuración estará dada de acuerdo a lo siguiente:

- **Control No Aplica:** El control no es aplicable para la Carrera de Ingeniería en Sistemas Computacionales.
- **Control Aplica:** El control es aplicable para la Carrera de Ingeniería en Sistemas Computacionales y será evaluado de acuerdo a los siguientes niveles de madurez:
    - **Optimizado:** La organización ha refinado su cumplimiento a un nivel de buena práctica.
    - **Administrado:** La organización regularmente mide su cumplimiento y hace mejoras al proceso de forma regular.
    - **Definido:** La organización aplica un enfoque detallado, documentado. Pero no existe medición, ni reforzamiento periódico del mismo.
    - **Repetible:** La organización tiene un enfoque consistente, pero en su mayoría no está documentado.
    - **Inicial:** La organización tiene un enfoque ad-hoc o desestructurado en esta práctica o estándar.
    - **No existente:** No hay evidencia de este estándar o práctica en la organización.

La configuración del porcentaje de cumplimiento será definido por las autoridades de la carrera y posteriormente deberán ser configuradas en la herramienta de software desarrollada. Para revisar los casos de uso detallados para la Gestión de Niveles de Madurez referirse al Anexo F de este documento.

3.2.2.7. Caso de Uso: Revisión de controles

Figura 24. Caso de Uso Revisión de Controles



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF05

Actor:

- Usuario

Descripción:

La herramienta de software permitirá realizar la revisión de los controles cargados de la norma ISO 27001 u otras normas creadas desde Gestión de Estándares. El análisis de brecha de seguridad estará dado por los siguientes datos:

- **Aplica:** Permite identificar si el control aplica o no aplica dentro de la institución.
- **Justificación:** Permite indicar una justificación de aplicabilidad o no aplicabilidad del control.
- **Estado Actual:** Permite indicar el estado de implantación del control dentro de la institución. Los estados están dados por los niveles

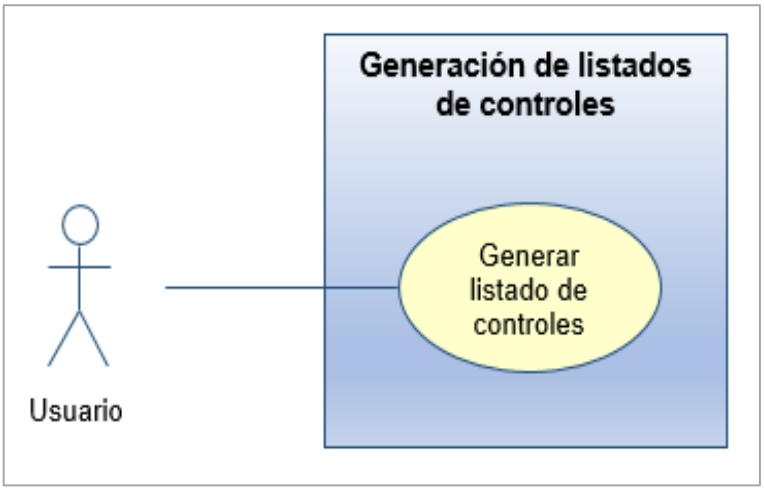
configurados en la sección 3.2.2.6. Caso de Uso: Gestión de Niveles de Madurez.

- **Fecha:** Permite establecer la fecha de evaluación del control.
- **Observaciones:** Permite incluir las observaciones y datos relevantes para justificar el estado del control.
- **Responsable:** Permite establecer el responsable de ejecutar el control dentro de la institución.
- **Revisor:** Permite establecer el usuario que realizó la evaluación del control interno de la institución.

Para revisar los casos de uso detallados para la Revisión de controles referirse al Anexo G de este documento.

3.2.2.8. Caso de Uso: Generación de listados de controles

Figura 25. Caso de Uso Generación de listados de controles



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF06

Actor:

- Usuario

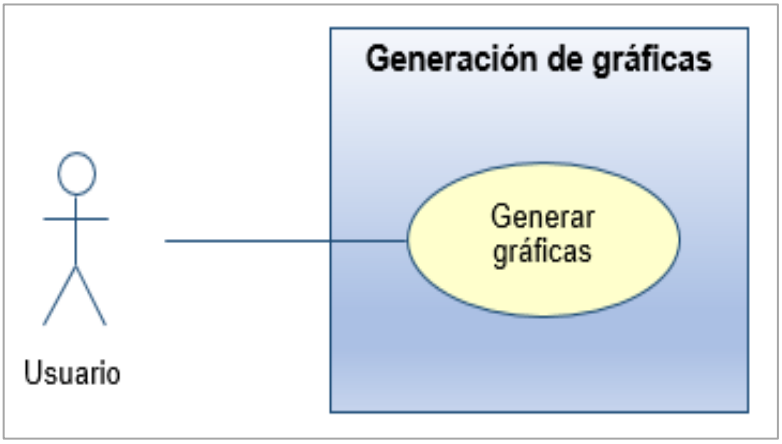
Descripción:

La herramienta será capaz de permitir la generación en formato editable del listado o informe con el estado actual de los controles para cada uno de los estándares.

Para revisar los casos de uso detallados para la Generación de listados de controles referirse al Anexo H de este documento.

3.2.2.9. Caso de Uso: Generación de gráficas

Figura 26. Caso de Uso Generación de Gráficas



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Requisitos Funcionales asociados:

- RF07

Actor:

- Usuario

Descripción:

La herramienta permitirá la generación de gráficas con el estado de madurez actual de los controles para cada uno de los estándares haciendo una comparación con el estado ideal que desea alcanzar la institución.

Para revisar los casos de uso detallados para la Generación de Gráficas referirse al Anexo I de este documento.

3.2.3. FASE DE PROGRAMACIÓN

Para la fase de programación de la herramienta de software se utilizará la arquitectura cliente-servidor de tal forma que permita un rápido despliegue de la aplicación sin la necesidad de requerir de una infraestructura compleja.
Con respecto a la tecnología utilizada para el desarrollo de esta herramienta de software, referirse a la sección de Factibilidad Técnica de este documento donde se encuentra el detalle de:

- Tecnología y solución propuesta.
- Disposición de la tecnología.
- Conocimientos técnicos.

3.2.3.1 Requisitos de instalación

A continuación se detallan los requisitos de hardware y software para la instalación de las herramientas de desarrollo:

- Requisitos de Hardware
  - Conectividad a la red.
  - Mínimo 2 gigabytes de memoria de RAM.
  - Procesador con más de 8 núcleos.
  - Mínimo 2 gigabytes de espacio en disco duro.
  - Pantalla de 1024 x 768 como mínimo con 256 colores.
  - Mouse.

- Requisitos de Software
  - Compatible con cualquier sistema operativo.
  - Navegador web instalado. (Recomendación Google Chrome)

3.2.4. FASE DE PRUEBAS

En esta fase se comprobarán las funcionalidades de la herramienta de software presentada y se validará que cumpla con los objetivos propuestos. Asimismo se verificará que todos los elementos de la herramienta se comportan de acuerdo a lo diseñado y programado.

Las pruebas para los requerimientos funcionales de la herramienta serán los siguientes:

- Pruebas de Gestión de Usuarios
- Pruebas de Gestión de Unidades
- Pruebas de Gestión de Estándares
- Pruebas de Gestión de Niveles de Madurez
- Pruebas de Revisión de controles
- Pruebas de Generación de listados de control
- Pruebas de Generación de gráficas

3.2.5. FASE DE IMPLANTACIÓN

En la fase de implantación, luego de la fase de pruebas y la corrección de los posibles errores identificados al momento de la verificación de la funcionalidad de la herramienta, se procederá a poner en producción el sistema de aplicación para la utilización por parte de los actores identificados: Administrador y Usuarios.

3.3. ENTREGABLES DEL PROYECTO

A continuación se describen los entregables del proyecto de titulación que serán levantados y documentados:

- Cronograma General de Actividades
- Requerimientos Funcionales (Descritos en el presente documento)
- Casos de Uso detallados
- Modelo Entidad Relación
- Código Fuente de aplicación
- Base de datos
- Manual Técnico
- Sistema de aplicación funcional
- Manual de Usuario
- Informe con la evaluación del control interno informático de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil

3.4. CRITERIOS DE VALIDACIÓN DE LA PROPUESTA

La herramienta de software desarrollada para ejecutar la evaluación del control interno a través del análisis de brecha tomando como base las buenas prácticas de la norma ISO 27001 fue validada para comprobar que su diseño y funcionalidad cumple con lo establecido en los requerimientos levantados en la etapa de análisis.

Para la validación de la propuesta se empleará los siguientes métodos:

- Encuestas de satisfacción
- Análisis de la Correlación de Pearson y Tablas de contingencia (Estadístico Chi-cuadrado)

La descripción de estos métodos se encuentra detallados en el Capítulo 4 de este documento.

Asimismo la herramienta de software fue presentada para su juicio y valoración a especialistas en el área de seguridad de la información y desarrollo de software.

- Al Ingeniero David Collantes, consultor de la firma Deloitte con más de 10 años de experiencia en seguridad de la información y control interno, así como también posee la Certificación Auditor Líder ISO 27001:2013.
- Al Ingeniero Luis Vergara, jefe de desarrollo de la compañía Metropolitan Touring con más de 6 años de experiencia en el desarrollo y mantenimiento de sistemas de aplicación y gestión de proyectos de software.
- A la Ingeniera Jacqueline Suárez, gestora de conocimiento de la compañía Astilleros Navales Ecuatoriano EP con más de 6 años de experiencia en gestión de proyectos de software.

CAPÍTULO IV

4. CRITERIOS DE ACEPTACIÓN DEL PRODUCTO

Microsoft Press define a los criterios de aceptación como “las condiciones que un producto de software debe satisfacer para ser aceptado por un usuario, cliente o stakeholder”. Considerando la definición de Press, a continuación se definen los criterios bajo los cuales la herramienta de software se considerará que cumple con los requerimientos funcionales establecidos en la etapa de análisis del proyecto.

Tabla XXX. Criterios de Evaluación de la herramienta de software

Requerimientos	Criterios de Evaluación
RF01: Gestión de Usuarios	Permite crear, modificar y eliminar usuarios en el sistema.
RF02: Gestión de Unidades	Permite crear, modificar y eliminar unidades/departamentos en el sistema.
RF03: Gestión de Estándares	Permite crear, modificar y eliminar catálogos de estándares en el sistema.
RF04: Gestión de Niveles de Madurez	Permite crear, modificar y eliminar niveles de madurez de controles en el sistema.
RF05: Revisión de controles	Permite realizar la evaluación del control interno a través de los niveles de madurez definidos.
RF06: Generación de listados de control	Permite descargar un informe con el listado de controles evaluados en la institución.
RF07: Generación de gráficas	Permite descargar gráficas con el estado actual de los controles evaluados en la institución.

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Para la evaluación y aceptación de la herramienta se confeccionó una plantilla con preguntas de diferente índole tales como: aspectos técnicos, control del sistema, utilidad, entre otros. A continuación se muestra el esquema utilizado:

Tabla XXXI. Esquema de Evaluación del producto

Aspectos	Detalle de evaluación
Utilidad	Facilidad de Uso
	Nivel de adaptación de usuarios
	Da orientaciones antes errores
	Permite la experimentación
Control del Programa	Intuitivo
	Atractivo
	Claridad de contenidos
	Interface de navegación
Técnicos	Documentación y ayudas
	Recursos de hardware y software

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

4.1. ENCUESTA DE SATISFACCIÓN

Para la aceptación del proyecto se presentó el sistema de aplicación a docentes de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil. Para ello, se efectuaron encuestas de satisfacción como herramienta de recolección de información. La calidad y aceptación del sistema está dada por los siguientes puntajes:

Tabla XXXII. Puntuación para aceptación del sistema

Puntaje	Evaluación del sistema	Calidad del sistema
Máximo 5	Excelente	Aceptable
Mayor o igual a 4	Muy buena	
Mayor o igual a 3	Buena	Dudosa
Mayor o igual a 2	Regular	
Mayor o igual a 1	Mala	Inaceptable

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Para mayor detalle del modelo de la encuesta utilizada para la evaluación de satisfacción del producto referirse al Anexo K adjunto a este documento.

4.1.1. POBLACIÓN Y MUESTRA

Para poder medir el grado de satisfacción del proyecto de titulación se realizó una encuesta considerando la siguiente población:

Tabla XXXIII. Población considerada para Encuesta de Satisfacción

Grupo	Población	Docentes
A	Docentes con conocimientos en ingeniería en sistemas computacionales.	37
B	Docentes con conocimientos diferentes a ingeniería en sistemas computacionales.	36

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Para la determinación del tamaño de esta muestra se utilizó la siguiente fórmula:

$$n = Z^2 p * q \;\; N / e^2 (N-1) + Z^2 p*q$$

Tabla XXXIV. Tamaño de la muestra Encuesta de Satisfacción Grupo A

Descripción de la fórmula	Valores
N = Tamaño de la población	37
Z = Nivel de confianza	95%
e = Error muestral	9%
p = Probabilidad a favor	50%
q = Probabilidad en contra	50%
n = Tamaño de la muestra	16

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Tabla XXXV. Tamaño de la muestra Encuesta de Satisfacción Grupo B

Descripción de la fórmula	Valores
N = Tamaño de la población	36
Z = Nivel de confianza	95%
e = Error muestral	9%
p = Probabilidad a favor	50%
q = Probabilidad en contra	50%
n = Tamaño de la muestra	15

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

De acuerdo a la fórmula aplicada y descritas en las tablas anteriores, la muestra utilizada fue de 31 personas de las cuales se seleccionaron del Grupo A: 16 personas y del Grupo B: 15 personas.

Tabla XXXVI. Resultados de Encuesta de Satisfacción

Detalle	Grupo A		Grupo B	
	Respuestas	Porcentajes	Respuestas	Porcentajes
Excelente	90	60%	139	93%
Muy buena	116	77%	78	52%
Buena	32	21%	8	5%
Regular	2	1%	0	0%
Mala	0	0%	0	0%

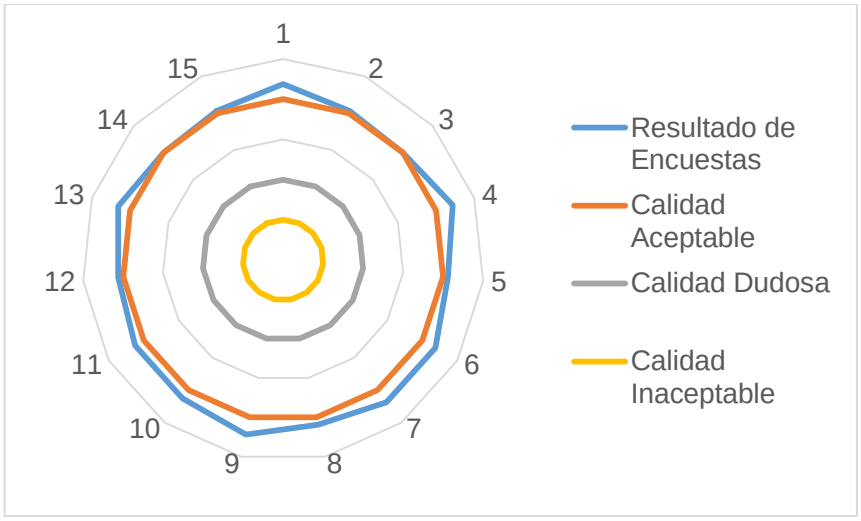
Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Tabla XXXVII. Resultados Generales de Satisfacción por Grupo

Grupo	Promedio General
A	4.23
B	4.33

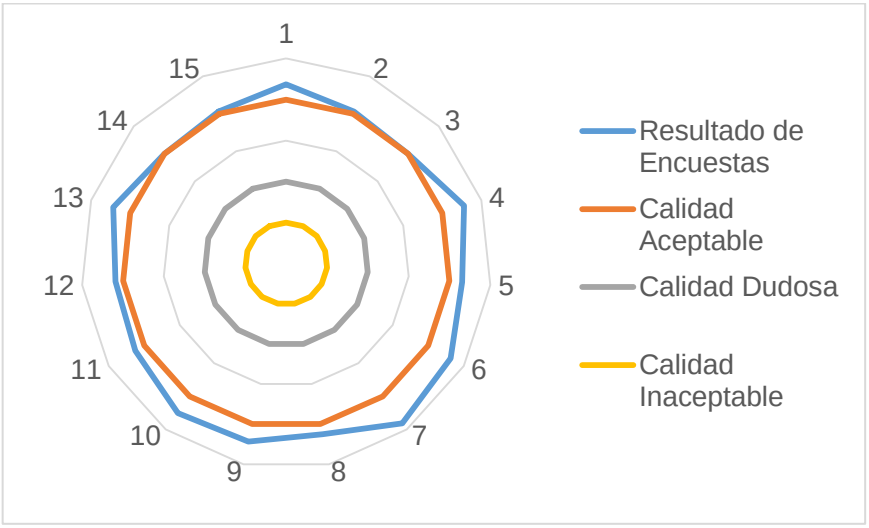
Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 11. Resultados de Encuesta de Satisfacción Grupo A



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Gráfico 12. Resultados de Encuesta de Satisfacción Grupo B



Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Análisis de datos:

El sistema obtuvo una evaluación general superior a los 4 puntos que considerando la tabla XXXII está en el criterio de Aceptable. Los encuestados consideraron que la aplicación es útil para la carrera y cumple con los requerimientos funcionales para los cuales fue desarrollado.

4.1.2. PRUEBA DE CHI CUADRADO

Tabla XXXVIII. Formulación de Hipótesis

Ho	H1
La satisfacción de los encuestados con respecto al sistema web presentado es independiente de los conocimientos en ingeniería de sistemas computacionales.	La satisfacción de los encuestados con respecto al sistema web presentado es dependiente de los conocimientos en ingeniería de sistemas computacionales.

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Tabla XXXIX. Datos observados

	Grupo A	Grupo B	Total
Excelente	6	9	15
Muy buena	7	5	12
Buena	2	1	3
Regular	1	0	1
Mala	0	0	0
Total	16	15	31

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Tabla XL. Datos esperados

	Grupo A	Grupo B	
Excelente	7.74	7.26	
Muy buena	6.19	5.81	
Buena	1.55	1.45	
Regular	0.52	0.48	
Mala	0.00	0.00	
Total	16.00	15.00	31.00

Elaboración: Carolina Morocho Crespo
Fuente: Datos de la investigación

Cálculo del valor de Chi cuadrado

$x^2 = (6-7.74)^2/7.74 + (7-6.19)^2/6.19 + (2-1.55)^2/1.55 + (1-0.52)^2/0.52 + (9-7.26)^2/7.26 + (5-5.81)^2/5.81 + (1-1.45)^2/1.45 + (0-0.48)^2/0.48$

$x^2 = 0.39 + 0.11 + 0.13 + 0.45 + 0.42 + 0.11 + 0.14 + 0.48$

$x^2 = 2.24$

Grado de libertad

$v = (2 – 1) * (2 - 1)$

$v = 1 * 1$

$v = 1$

Valor estadístico tomado de la Tabla Chi Cuadrado

Tabla x^2 = Nivel de significación del 0,05 con un grado de libertad

Tabla x^2 = 3.84

Comparación del estadístico con el resultado obtenido

Chi cuadrado ≤ Valor estadístico

2.24 ≤ 3.84

Análisis Chi Cuadrado

Con esta comparación se puede concluir que la satisfacción de los encuestados con respecto al sistema presentado es independiente de los conocimientos de ingeniería en sistemas computacionales (Hipótesis Nula Ho).

4.2. INFORME DE ASEGURAMIENTO DE CALIDAD DEL SISTEMA

Con la finalidad de garantizar la calidad de la herramienta de software desarrollada se procedió a la elaboración de un informe en donde se incluye la evaluación del sistema de aplicación asegurando su funcionamiento y disposición para los actores planteados: Administrador y Usuario.

En el informe de Aseguramiento de Calidad se han incluido las siguientes secciones:

- Resumen Ejecutivo
- Gestión de Entregables
- Gestión de Riesgos
- Detalle de Alertas y Recomendaciones
- Actividades Realizadas

Para mayor detalle del informe referirse al Anexo L adjunto a este documento.

4.3. INFORME DE EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO

Como parte del presente proyecto de titulación se procedió a levantar un informe que contiene la evaluación del control interno informático de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil y que permitirá cumplir con los siguientes objetivos:

- Conocer la situación actual del control interno de la Carrera para que las autoridades puedan actuar en sus brechas de seguridad.
- Comparar el estado actual en el que se encuentra la Carrera con los requerimientos del estándar de buenas prácticas ISO/IEC 27001 para que las autoridades conozcan su situación frente a las buenas prácticas de seguridad.

En el informe de Evaluación del Control Interno Informático de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil se han incluido las siguientes secciones:

- Objetivos de la evaluación
- Alcance
- Metodología de Análisis
- Resultados
- Planes y recomendaciones de acción para mejoras

Para mayor detalle del informe referirse al Anexo M adjunto a este documento.

4.4. CONCLUSIONES

Una vez finalizada la elaboración del documento del proyecto de titulación y el proceso de desarrollo de la herramienta de software, a continuación se especifica el cumplimiento de los objetivos planteados y las principales conclusiones:

El principal objetivo de este proyecto era el desarrollo de una herramienta de software que facilite la evaluación del control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil tomando como referencia la norma ISO/IEC 27001. Este objetivo fue cubierto al entregar un sistema de aplicación desarrollado con herramientas relevantes en el mercado y que permite hacer la evaluación de alto nivel de los controles con los que actualmente cuenta la carrera.

Se explicaron los beneficios de la evaluación del control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil. Durante todo el desarrollo del proyecto, se han expuesto las oportunidades que tendrá la carrera al contar con una herramienta que muestre el estado actual de los controles internos, esto servirá de gran ayuda para realizar planes de acción y orientar al cumplimiento de las buenas prácticas de seguridad.

La herramienta de software es capaz de generar información relevante, suficiente y oportuna para lograr la implementación de controles que permitan minimizar los riesgos tecnológicos. En la actualidad, las herramientas de software resultan de gran utilidad para las autoridades de cualquier institución puesto que proporcionan documentación actualizada, la herramienta desarrollada permite la generación de gráficas e informes con los resultados de la evaluación de control interno que se ejecute en la carrera.

A través del análisis de brecha efectuado por la herramienta de software, se puede conocer la situación actual del control interno de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil. Esto permite que se conozcan las debilidades de control que mantiene la institución y de esta forma

permitirá trabajar en dichas debilidades y generar acciones que eviten daños o fuga de información.

La herramienta de software permite comparar el estado o situación actual en la que se encuentra la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con los requerimientos del estándar de buenas prácticas ISO/IEC 27001 y a través de los resultados generados por la herramienta, las autoridades de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil obtendrán los resultados de la evaluación del control interno de la institución.

Luego del análisis y revisión del control interno informático realizado a las principales categorías de control detalladas a continuación:

- Política de Seguridad de la Información
- Control de Accesos
- Seguridad Física y Ambiental
- Seguridad en las operaciones
- Seguridad de las comunicaciones
- Adquisición, Desarrollo y Mantenimiento de Sistemas

Se estableció que el nivel de madurez de los controles de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil frente a la norma ISO/IEC 27001 es **5 - Repetible**, lo cual indica que la institución aplica un enfoque consistente, pero que en muchos de los casos no cuenta con documentación que soporte la implementación de los controles.

Por todo lo antes expuesto se llega a la conclusión de que el proyecto de titulación y la herramienta de software alcanzaron los objetivos propuestos.

4.5. RECOMENDACIONES

A continuación se describen las principales recomendaciones a tener en cuenta para garantizar el buen desempeño de la herramienta de software para la

evaluación del control interno en la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil:

Se deberá delegar a un colaborador de la carrera para que actúe como administrador de la herramienta, para que de esta forma dicha persona tenga a su cargo las seguridades, gestión de los usuarios, entre otros y que pueda ser orientado para que a su vez, según sea necesario, capacite a otros colaboradores. Se recomienda que para realizar la gestión de normas se deberá tener en cuenta que las normas a crearse en el sistema de aplicación deben mantener una misma estructura que la incluida en las buenas prácticas de la ISO 27001, la cual maneja definiciones de dominios, objetivos de control y controles.

Al momento la herramienta de software únicamente realiza el análisis de brecha para los controles definidos en la norma ISO 27001, sin embargo esta herramienta podría tomarse como base para incluir otros temas relacionados con el sistema de gestión de seguridad de la información conocido por sus siglas SGSI, tales como: inventario de activos de información, análisis y evaluación de riesgos.

La herramienta de software también puede ser adaptada para que se incluyan controles no solo en temas de informática sino podrían considerarse controles con respecto a la administración, finanzas, entre otros.

Otro punto importante que podría considerarse para robustecer la herramienta de software desarrollada, sería incluir el manejo del sistema de gestión de continuidad del negocio tomando como base los requisitos establecidos en la norma internacional ISO 22301.

En caso de que existan dudas, inquietudes o novedades sobre el uso del sistema de aplicación, se recomienda recurrir al manual técnico o de usuario desarrollados para la administración y comprensión de la herramienta.

BIBLIOGRAFÍA

Aenor Ecuador. (25 de Mayo de 2014). *Aenor Ecuador*. Obtenido de http://www.aenorecuador.com/seguridad-de-la-informaci%C3%B3n.aspx

Alegsa. (2016). *Diccionario de informática y tecnología*. Obtenido de Diccionario de informática y tecnología: http://www.alegsa.com.ar/Dic/usuario.php

Al-Mayahi, I., & Mansoor, S. (2006). *ISO 27001 Gap Analysis - Case Study.* Obtenido de ISO 27001 Gap Analysis - Case Study: http://worldcomp-proceedings.com/proc/p2012/SAM9779.pdf

Ascanio, J. (16 de Junio de 2015). *Modelo de cascada*. Obtenido de Prezi: Para el presente proyecto de titulación

Aumatell, C. (2003). *Auditoría de la información.* Aragón: UOC.

Belt Ibérica S.A. (20 de Octubre de 2004). Obtenido de Seguridad de la Información y protección de datos: http://www.belt.es/expertos/HOME2_experto.asp?id=2245

Burrel, B. (8 de Julio de 2014). *10 consejos para proteger la información de instituciones educativas*. Obtenido de Sitio Web welivesecurity: http://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/

Cómite técnico AEN/CTN 71 - Tecnología de la Información. (Julio de 2015). *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.* Madrid: AENOR.

Committee of Sponsoring Organizations. (2013). *Informe COSO.*

Consulting Integral. (2015). *Consulting Integral*. Obtenido de Sitio Consulting Integral: http://consultingintegral.es/medidas-de-seguridad-lopd/

Cooper, W., & Lybrand, R. (1997). *Los Nuevos Conceptos del Control Interno: Informe COSO.* Ediciones Díaz de Santos.

Dean, R. A. (2015). *Universidad Nacional de Río Cuarto. Facultad de Ingeniería*. Obtenido de La investigación tecnológica en las ciencias de ingeniería y la innovación tecnológica: http://www.unrc.edu.ar/publicar/23/dossidos.html

Degiovannini, M. (Febrero de 2007). *Comparativa de Frameworks Web.* Obtenido de JavaHispano.org:

http://static1.1.sqspcdn.com/static/f/923743/15025206/1320739503647/frameworks_web.pdf?token=0p0jLXicjEHOLxPkNFSBDnZXMYo%3D

Deloitte. (2013). Estudio Global sobre Seguridad en TMT.

Deloitte. (Junio de 2016). Encuesta sobre Tendencias de Cyber Riesgos y Seguridad de la Información.

Diario Argentino Ámbito. (1 de Mayo de 2016). Apresan a estudiante que hackeaba web de UADE para cambiar sus notas. *Ámbito*. Obtenido de http://www.ambito.com/837375-apresan-a-estudiante-que-hackeaba-web-de-uade-para-cambiar-sus-notas

Diario EL COMERCIO. (30 de Enero de 2015). Cómo evitar los ataques de las cibermafias. *EL COMERCIO*.

Diario EL COMERCIO. (26 de Julio de 2015). Ecuador se muestra vulnerable a ciberataques. *EL COMERCIO*.

Diario Expreso. (26 de Febrero de 2013). Univ. Espíritu Santo sufrió un ataque informático. *Univ. Espíritu Santo sufrió un ataque informático*.

EcuRed. (2016). *AJAX*. Obtenido de AJAX: http://www.ecured.cu/AJAX

Eguiluz, J. (25 de Marzo de 2009). *Introducción a JavaScript.* Obtenido de Introducción a JavaScript: https://librosweb.es/libro/javascript/capitulo_1.html

Ernst & Young. (2015). *Ernst & Young.* Obtenido de Sitio Web EY: http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf

Escobedo, H. (20 de Noviembre de 2014). *Análisis Comparativo de Framework de desarrollo de aplicación*. Obtenido de Prezi: https://prezi.com/xdl15wsnvyjd/analisis-comparativo-de-framework-de-desarrollo-de-aplicacio/

ESET Security. (2016). ESET Security Report Latinoamérica 2016.

Fernández, C. M. (Julio-Septiembre de 2012). *Asociación Española para la Calidad.* Obtenido de itio Web AEC: http://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128

Fundación AtixLibre. (28 de Febrero de 2013). *Revista Digital ATIX.* Obtenido de Revista Digital ATIX: http://atix.switnet.org/atix21.pdf

Genuitec. (2016). *MyEclipse*. Obtenido de MyEclipse: http://www.software.com.ar/p/genuitec-myeclipse#product-description

Gestiopolis. (08 de Abril de 2001). *¿Qué es el estudio de factibilidad en un proyecto?* Obtenido de Gestiopolis: http://www.gestiopolis.com/que-es-el-estudio-de-factibilidad-en-un-proyecto/

GMS. (17 de Febrero de 2016). Seguridad Web. Guayaquil, Ecuador: Bsco. Obtenido de Sitio Web Canal News Ecuador: http://canalnews.ec/category-seguridad/175-gms-presento-recomendaciones-para-prevenir-ataques-ciberneticos-en-instituciones-educativas

Instituto Canadiense de Contadores Autorizados. (1995). *Guía de control interno COCO.* Canadá.

INTOSAI. (2001). *Guía para las normas de control interno del sector público.* Bélgica: INTOSAI.

ISACA. (2012). *COBIT: Un marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Estados Unidos: ISACA.

ISACA. (2016). Manual de Preparación Examen CISM 14° edición. Ecuador.

ISO27000es. (2012). *ISO27000 en español*. Obtenido de ISO27000 en español: http://www.iso27000.es/sgsi.html

Jaspersoft. (2002). *JasperReports Library Reference Materials*. Obtenido de JasperReports Library Reference Materials: http://community.jaspersoft.com/wiki/jasperreports-library-reference-materials

Levin, R., & Rubin, D. (1996). *Estadística para administradores.* Pearson Educación.

Luján, S. (2002). *Programación de aplicaciones web: historia, principios básicos y clientes web.* España: Club universitario.

McAfee. (2012). Data Loss by the Numbers.

Mcleod, R. (2000). *Sistemas de Información Gerencial.* México: Prentice Hall.

Mendoza, M. (2 de Julio de 2015). *welivesecurity*. Obtenido de http://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/

Montoya, J. (26 de Agosto de 2014). *Tecnologías para el desarrollo de aplicaciones web*. Obtenido de Tecnologías para el desarrollo de

aplicaciones web: https://prezi.com/ohanpxoyzgyx/13-tecnologias-para-el-desarrollo-de-aplicaciones-web/

Navarrete, R. (19 de Enero de 2002). *Tecnologías de información y su utilidad en la empresa*. Obtenido de Tecnologías de información y su utilidad en la empresa: http://www.gestiopolis.com/tecnologias-de-informacion-y-su-utilidad-en-la-empresa/

Norma ITIL. (2016). *Herramientas y metodologías*. Obtenido de Herramientas y metodologías: http://itilv3.osiatis.es/proceso_mejora_continua_servicios_TI/herramientas_metodologias.php

OpenSource.org. (2016). *Iniciativa Open Source*. Obtenido de Iniciativa Open Source: https://opensource.org/

Oracle. (2010). *Documento técnico de Oracle.* Obtenido de http://www.oracle.com/technetwork/es/database/enterprise-edition/documentation/productos-oracle-database-11g-2247590-esa.pdf

Patiño, N. (7 de Marzo de 2014). *ZK Framework*. Obtenido de Prezi: https://prezi.com/rs87lwtdaueg/zk-framework/

Ponemon Institute. (18 de Noviembre de 2015). *Digital Guardian.* Obtenido de https://digitalguardian.com/blog/findings-2015-ponemon-institute-cost-cybercrime-study-threats-vs-defenses-gap

Pressman, R. (2010). *Ingeniería de Software: Un enfoque práctico.* México: McGraw-Hill.

PricewaterhouseCoopers S.C. (2014). *Año de transición al nuevo CoOSO 2013.* Obtenido de https://www.pwc.com/mx/es/publicaciones/archivo/2014-02-punto-vista.pdf

Rodríguez, H. (2010). *Ventajas y desventajas de POSTGRESQL, MYSQL Y ORACLE.* Obtenido de Ventajas y desventajas de POSTGRESQL, MYSQL Y ORACLE.

Rosado, S. (2 de Febrero de 2015). *Tabla comparativa de los lenguajes de programación*. Obtenido de Desarrollo Web: http://desarrollowebydesarrolloweb.blogspot.com/2015/02/tabla-comparativa-de-los-lenguajes-de.html

Rosado, S. (8 de Febrero de 2015). *Tabla comparativa de los sistemas gestores de base de datos*. Obtenido de Desarrollo web:

http://desarrollowebydesarrolloweb.blogspot.com/2015/02/tabla-comparativa-de-los-sistemas.html

SBQ Consultores. (Junio de 2016). ISO 27001:2014. Protegiendo su activo más valioso: la información. España.

World Wide Web Consortium (W3C). (2016). *Guía breve de CSS*. Obtenido de Guía breve de CSS: http://www.w3c.es/Divulgacion/GuiasBreves/HojasEstilo

ZKOSS. (2016). *ZK Framework*. Obtenido de ZK Framework: https://www.zkoss.org/product/zk

ANEXO A

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

CUESTIONARIO

"DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL"

1. Conoce usted si, ¿CISC ha definido un presupuesto específico aplicado a la gestión de Control Interno y Seguridad de la Información?

A. SÍ
B. NO
C. DESCONOCE

2. ¿Cuáles considera que son los principales obstáculos que CISC enfrenta con respecto a la gestión de seguridad de la información?

A. FALTA DE PRESUPUESTO O RECURSOS
B. EL AUMENTO DE COMPLEJIDAD DE LAS AMENAZAS
C. FALTA DE CLARIDAD SOBRE EL MANDATO, LAS FUNCIONES Y RESPONSABILIDADES
D. EL IMPACTO DE NUEVAS TECNOLOGÍAS
E. OTROS

3. ¿CISC cuenta con líneas de investigación de seguridad de la información?

A. SÍ
B. NO
C. DESCONOCE

4. ¿CISC ha experimentado una brecha de seguridad durante los últimos 24 meses?

A. SÍ
B. NO
C. DESCONOCE

5. ¿CISC cuenta con políticas o normativas para la seguridad de la información?

A. Sí
B. NO
C. EN PROCESO

6. ¿CISC se alinea a algún estándar o norma para gestionar la Seguridad de la Información y Control Interno?

A. COBIT
B. COSO
C. ISO 27001
D. NINGUNO

7. ¿CISC ha definido roles y privilegios para el acceso a los sistemas de la institución?

A. SÍ
B. NO
C. PARCIALMENTE

8. ¿Se realizan en CISC eventos relacionados con la concientización/difusión de la Seguridad de la Información?

A. SÍ
B. NO
C. EN PLANIFICACIÓN

9. ¿Qué grado de interés tendría en una herramienta de software que permita realizar la evaluación del control interno en CISC?

A. ALTO
B. MEDIO
C. BAJO
D. NINGUNO

10. ¿Apoyaría la implementación en CISC de una herramienta de software para la evaluación del control interno?

A. SÍ
B. NO
C. PARCIALMENTE

ANEXO B

CRONOGRAMA DE ACTIVIDADES

Nombre de tarea	Duración	Comienzo	Fin
DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL	**75 días**	**mar 24/05/16**	**lun 05/09/16**
DESARROLLO DE LOS CAPÍTULOS DEL PROYECTO DE TITULACIÓN	**75 días**	**mar 24/05/16**	**lun 05/09/16**
Desarrollo del Capítulo 1	**6 días**	**mar 24/05/16**	**mar 31/05/16**
Descripción del Capítulo 1 del Proyecto de Titulación	6 días	mar 24/05/16	mar 31/05/16
Entregar Capítulo 1 del Proyecto de Titulación	1 día	mar 31/05/16	mar 31/05/16
Desarrollo del Capítulo 2	**7 días**	**mié 08/06/16**	**jue 16/06/16**
Descripción del Capítulo 2 del Proyecto de Titulación	6 días	mié 08/06/16	mié 15/06/16
Entregar Capítulo 2 del Proyecto de Titulación	1 día	jue 16/06/16	jue 16/06/16
Desarrollo del Capítulo 3	**10 días**	**vie 24/06/16**	**jue 07/07/16**
Descripción del Capítulo 3 del Proyecto de Titulación	9 días	vie 24/06/16	mié 06/07/16
Entregar Capítulo 3 del Proyecto de Titulación	1 día	jue 07/07/16	jue 07/07/16
Desarrollo del Capítulo 4	**6 días**	**lun 29/08/16**	**lun 05/09/16**
Descripción del Capítulo 4 del Proyecto de Titulación	5 días	lun 29/08/16	vie 02/09/16
Entregar Capítulo 4 del Proyecto de Titulación	1 día	lun 05/09/16	lun 05/09/16
PLANTEAMIENTO DE HERRAMIENTAS A UTILIZAR	**2 días**	**mar 24/05/16**	**mié 25/05/16**
Revisión de herramientas de desarrollo existentes en el mercado	1 día	mar 24/05/16	mar 24/05/16
Análisis de factibilidad técnica de herramientas de desarrollo	1 día	mié 25/05/16	mié 25/05/16
DESARROLLO DEL SISTEMA WEB	**52 días**	**vie 24/06/16**	**lun 05/09/16**
Diseño de casos de uso	2 días	vie 24/06/16	lun 27/06/16
Diseño del Modelo Entidad Relación	2 días	mar 28/06/16	mié 29/06/16
Construcción de la base de datos	4 días	jue 30/06/16	mar 05/07/16
Diseño de pantallas del sistema	2 días	mié 06/07/16	jue 07/07/16
Construcción de pantallas	7 días	vie 08/07/16	lun 18/07/16
Codificación de funcionalidad del sistema	32 días	mar 19/07/16	mié 31/08/16
Pruebas de funcionamiento del sistema	2 días	jue 01/09/16	vie 02/09/16
ENTREGAR PROYECTO DE TITULACIÓN	**1 día**	**lun 05/09/16**	**lun 05/09/16**

ANEXO C

CASO DE USO: GESTIÓN DE USUARIOS

<table>
<tr><td>Caso De Uso</td><td colspan="2">RF01</td><td>N #</td><td>1</td></tr>
<tr><td>Actores</td><td colspan="4">Administrador (Principal)
Sistema</td></tr>
<tr><td>Propósito</td><td colspan="4">Crear usuario en el sistema</td></tr>
<tr><td>Tipo</td><td colspan="4">Básico</td></tr>
<tr><td>Resumen</td><td colspan="4">Control de la seguridad de accesos de usuarios. Esta actividad será realizada por el administrador del sistema.</td></tr>
<tr><td>Precondiciones</td><td colspan="4">Para crear usuarios en el sistema se debe tener permisos de administrador.</td></tr>
<tr><td>Post Condiciones</td><td colspan="4">Sólo los usuarios creados podrán tener acceso a la herramienta.</td></tr>
<tr><td>Referencias</td><td colspan="4">RF01</td></tr>
<tr><td colspan="5">Curso Típico De Eventos</td></tr>
<tr><td colspan="2">Acciones Del Actor</td><td colspan="3">Respuesta Del Sistema</td></tr>
<tr><td colspan="2">1. El administrador ingresa al módulo Seguridades.
2. El administrador selecciona el menú Administración.
3. El administrador selecciona el submenú Usuarios.
6. El administrador presiona el botón Crear.
8. El administrador ingresa los datos del usuario: nombre de usuario, cédula, nombres, cargo, correo electrónico y contraseña temporal.
9. El administrador selecciona el perfil que contendrá el usuario.
9. El administrador presiona el botón Guardar.</td><td colspan="3">4. El sistema valida que el usuario que está accediendo al submenú Usuarios tenga permisos de administrador.
5. El sistema muestra la lista de usuarios creados con la opción Crear.
7. El sistema muestra la pantalla de creación de usuarios con la información que se debe ingresar y los botones Guardar y Cancelar.
10. El sistema valida los datos ingresados y graba en la base de datos la información del usuario dado de alta.
12. El sistema muestra el mensaje: “Usuario creado exitosamente”.</td></tr>
<tr><td colspan="5">Curso Alterno De Eventos</td></tr>
<tr><td colspan="5">1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”.
2. Si no se ha ingresado la identificador del usuario, el sistema mostrará el mensaje de error: “Llenar campo requerido: Código Usuario”.
3. Si no se ha ingresado la contraseña temporal para el usuario, el sistema mostrará el mensaje de error: “Llenar campo requerido: Contraseña”.</td></tr>
</table>

ANEXO C (cont.)

CASO DE USO: GESTIÓN DE USUARIOS

Caso De Uso	**RF01**	**N #**	**2**
Actores	Administrador (Principal) Sistema		
Propósito	Modificar usuario en el sistema		
Tipo	Básico		
Resumen	Control de la seguridad de accesos de usuarios. Esta actividad será realizada por el administrador del sistema.		
Precondiciones	Para modificar usuarios en el sistema se debe tener permisos de administrador. Sólo los usuarios creados podrán ser modificados.		
Post Condiciones	NA		
Referencias	RF01		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al Módulo Seguridades. 2. El administrador selecciona el menú Administración. 3. El administrador selecciona el submenú Usuarios. 6. El administrador selecciona el usuario a ser modificado. 8. El administrador podrá modificar los datos del usuario: código del usuario o contraseña. 9. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Usuarios tenga permisos de administrador. 5. El sistema muestra la lista de usuarios actuales con acceso al sistema. 7. El sistema muestra la pantalla con la información del usuario y los botones Guardar y Limpiar. 10. El sistema valida los datos modificados y graba en la base de datos la información actualizada del usuario. 11. El sistema muestra el mensaje: “Modificado exitosamente”.

Curso Alterno De Eventos
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si no se ha ingresado la identificador del usuario, el sistema mostrará el mensaje de error: “Llenar campo requerido: Código Usuario”. 3. Si no se ha ingresado la contraseña temporal para el usuario, el sistema mostrará el mensaje de error: “Llenar campo requerido: Contraseña”.

ANEXO C (cont.)

CASO DE USO: GESTIÓN DE USUARIOS

Caso De Uso	**RF01**	**N #**	**3**
Actores	Administrador (Principal) Sistema		
Propósito	Eliminar usuario del sistema		
Tipo	Básico		
Resumen	Control de la seguridad de accesos de usuarios. Esta actividad será realizada por el administrador del sistema.		
Precondiciones	Para eliminar usuarios en el sistema se debe tener permisos de administrador. Sólo los usuarios creados podrán ser eliminados.		
Post Condiciones	Los usuarios eliminados no podrán acceder al sistema.		
Referencias	RF01		
Curso Típico De Eventos			
Acciones Del Actor	**Respuesta Del Sistema**		
1. El administrador ingresa al módulo Seguridades. 2. El administrador selecciona el menú Administración. 3. El administrador selecciona el submenú Usuarios. 6. El administrador selecciona el usuario a ser deshabilitado. 8. El administrador deshabilita el usuario dando clic en el checkbox Activo. 9. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Usuarios tenga permisos de administrador. 5. El sistema muestra la lista de usuarios actuales con acceso al sistema. 7. El sistema muestra la pantalla con la información del usuario, checkbox Activo y los botones Guardar y Limpiar. 10. El sistema muestra el mensaje: “Usuario deshabilitado”.		
Curso Alterno De Eventos			
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”.			

ANEXO D

CASO DE USO: GESTIÓN DE UNIDADES

Caso De Uso	**RF02**	**N #**	**1**
Actores	Administrador (Principal) Sistema		
Propósito	Crear unidad en el sistema		
Tipo	Básico		
Resumen	La herramienta será multi-departamental, ya que la evaluación del control interno no solo podrá ser realizada a nivel general en la Carrera de Ingeniería en Sistemas Computacionales sino también puede aplicarse a las diferentes unidades/departamentos de la misma.		
Precondiciones	Para crear unidades en el sistema se debe tener permisos de administrador.		
Post Condiciones	Sólo se podrá realizar la evaluación del control interno a las unidades creadas.		
Referencias	RF02		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al módulo Seguridades. 2. El administrador selecciona el menú Administración. 3. El administrador selecciona el submenú Unidades. 6. El administrador presiona el botón Crear. 8. El administrador ingresa los datos de la unidad: nombre de la unidad, descripción de la unidad y responsable de la unidad. 9. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Unidades tenga permisos de administrador. 5. El sistema muestra la lista de unidades creadas y el botón Crear. 7. El sistema muestra la pantalla de creación de unidades con la información que se debe ingresar y los botones Guardar y Cancelar. 10. El sistema valida los datos ingresados y graba en la base de datos la información de la unidad creada. 11. El sistema muestra el mensaje: “Unidad creada exitosamente”.

Curso Alterno De Eventos
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si la información para la creación de la unidad/departamento no está completa, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”.

ANEXO D (cont.)

CASO DE USO: GESTIÓN DE UNIDADES

Caso De Uso	**RF02**	**N #**	**2**
Actores	Administrador (Principal) Sistema		
Propósito	Modificar unidades en el sistema		
Tipo	Básico		
Resumen	La herramienta será multi-departamental, ya que la evaluación del control interno no solo podrá ser realizada a nivel general en la Carrera de Ingeniería en Sistemas Computacionales sino también puede aplicarse a las diferentes unidades/departamentos de la misma.		
Precondiciones	Para modificar unidades en el sistema se debe tener permisos de administrador. Sólo las unidades creadas podrán ser modificadas.		
Post Condiciones			
Referencias	RF02		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al módulo Seguridades. 2. El administrador selecciona el menú Administración. 3. El administrador selecciona el submenú Unidades. 6. El administrador selecciona la unidad a ser modificada. 8. El administrador podrá modificar los datos del usuario: nombre de la unidad, descripción de la unidad y responsable de la unidad. 9. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Unidades tenga permisos de administrador. 5. El sistema muestra la lista de unidades existentes. 7. El sistema muestra la pantalla con la información de la unidad y los botones Guardar, Eliminar y Cancelar. 10. El sistema valida los datos modificados y graba en la base de datos la información actualizada de la unidad. 11. El sistema muestra el mensaje: “Guardado exitosamente”.
Curso Alterno De Eventos	
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si no se ha ingresado toda la información de la unidad, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”.	

ANEXO D (cont.)

CASO DE USO: GESTIÓN DE UNIDADES

Caso De Uso	**RF02**	**N #**	**3**
Actores	Administrador (Principal) Sistema		
Propósito	Eliminar unidad del sistema		
Tipo	Básico		
Resumen	La herramienta será multi-departamental, ya que la evaluación del control interno no solo podrá ser realizada a nivel general en la Carrera de Ingeniería en Sistemas Computacionales sino también puede aplicarse a las diferentes unidades/departamentos de la misma.		
Precondiciones	Para modificar unidades en el sistema se debe tener permisos de administrador. Sólo las unidades creadas y que no posean revisión de controles podrán ser eliminadas.		
Post Condiciones	No se podrán efectuar revisiones de control interno en unidades eliminadas.		
Referencias	RF02		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al módulo Seguridades. 2. El administrador selecciona el menú Administración. 3. El administrador selecciona el submenú Unidades. 6. El administrador selecciona la unidad a ser eliminada. 8. El administrador presiona el botón Eliminar.	4. El sistema valida que el usuario que está accediendo al submenú Unidades tenga permisos de administrador. 5. El sistema muestra la lista de unidades existentes 7. El sistema muestra la pantalla con la información de la unidad y los botones Guardar, Eliminar y Cancelar. 9. El sistema muestra el mensaje: “Unidad eliminada”.

Curso Alterno De Eventos
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si al momento de eliminar la unidad se mantiene revisiones de controles, el sistema mostrará el mensaje de error: “Unidad no puede ser eliminada”.

ANEXO E

CASO DE USO: GESTIÓN DE ESTÁNDARES

<table>
<tr><td>Caso De Uso</td><td>RF03</td><td>N #</td><td>1</td></tr>
<tr><td>Actores</td><td colspan="3">Administrador (Principal)
Sistema</td></tr>
<tr><td>Propósito</td><td colspan="3">Crear estándar en el sistema</td></tr>
<tr><td>Tipo</td><td colspan="3">Principal</td></tr>
<tr><td>Resumen</td><td colspan="3">Permitirá dar asistencia a otras normas como por ejemplo ISO 22301, siempre y cuando la estructura del catálogo de los controles sea similar a la establecida en la norma ISO 27001. Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.</td></tr>
<tr><td>Precondiciones</td><td colspan="3">Para ingresar estándares en el sistema se debe tener permisos de administrador. Sólo se podrán ingresar estándares que posean la misma estructura que la norma ISO 27001.</td></tr>
<tr><td>Post Condiciones</td><td colspan="3">Sólo se podrá realizar la evaluación del control interno considerando los estándares registrados en el sistema.</td></tr>
<tr><td>Referencias</td><td colspan="3">RF03</td></tr>
<tr><td colspan="4">Curso Típico De Eventos</td></tr>
<tr><td colspan="2">Acciones Del Actor</td><td colspan="2">Respuesta Del Sistema</td></tr>
<tr><td colspan="2">1. El administrador ingresa al módulo Controles.
2. El administrador selecciona el menú Catálogos.
5. El administrador presiona el botón Seleccionar.
7. El administrador presiona el botón Nuevo.
9. El administrador ingresa los dominios, objetivos de control y controles.
10. El administrador presiona el botón Guardar.</td><td colspan="2">3. El sistema valida que el usuario que está accediendo al menú Catálogos tenga permisos de administrador.
4. El sistema muestra una ventana con la lista de estándares creados y el botón Seleccionar.
6. El sistema muestra una pantalla con el detalle de controles del estándar seleccionado y el botón Nuevo.
8. El sistema muestra una pantalla para el mantenimiento del control y los botones Guardar y Cancelar.
11. El sistema valida los datos ingresados y graba en la base de datos la información de dominios, objetivos de control y controles ingresados.
12. El sistema muestra el mensaje: “Guardado exitosamente”.</td></tr>
<tr><td colspan="4">Curso Alterno De Eventos</td></tr>
<tr><td colspan="4">1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”.
2. Si la información para la generación de estándar no está completa, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”.</td></tr>
</table>

ANEXO E (cont.)

CASO DE USO: GESTIÓN DE ESTÁNDARES

Caso De Uso	**RF03**	**N #**	**2**
Actores	Administrador (Principal) Sistema		
Propósito	Modificar estándar en el sistema		
Tipo	Principal		
Resumen	Permitirá dar asistencia a otras normas como por ejemplo ISO 22301, siempre y cuando la estructura del catálogo de los controles sea similar a la establecida en la norma ISO 27001. Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.		
Precondiciones	No se podrá modificar la norma ISO 27001.		
Post Condiciones	Sólo se podrá realizar la evaluación del control interno considerando los estándares registrados en el sistema.		
Referencias	RF03		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al módulo Controles. 2. El administrador selecciona el menú Parametrizaciones. 3. El administrador selecciona el submenú Catálogos. 5. El administrador da clic sobre el botón Modificar. 7. El administrador modifica los dominios, objetivos de control y controles. 8. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Catálogos tenga permisos de administrador. 4. El sistema muestra la lista de estándares creados y los botones Nuevo y Modificar. 6. El sistema muestra una pantalla con los dominios, objetivos de control y controle, checkbox Activo y los botones Guardar y Limpiar. 9. El sistema valida los datos ingresados y graba en la base de datos la información de dominios, objetivos de control y controles ingresados. 10. El sistema muestra el mensaje: “Modificación exitosa”.

Curso Alterno De Eventos
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si la información para la generación de estándar no está completa, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”. 3. Si el usuario desea modificar la norma ISO27001 el sistema mostrará el mensaje de error: “Estándar no puede ser modificado”

ANEXO E (cont.)

CASO DE USO: GESTIÓN DE ESTÁNDARES

Caso De Uso	**RF03**	**N #**	**3**
Actores	Administrador (Principal) Sistema		
Propósito	Eliminar estándar en el sistema		
Tipo	Principal		
Resumen	Permitirá dar asistencia a otras normas como por ejemplo ISO 22301, siempre y cuando la estructura del catálogo de los controles sea similar a la establecida en la norma ISO 27001. Esta actividad no podrá ser manipulada por los usuarios finales de la herramienta.		
Precondiciones	No se podrá modificar la norma ISO 27001.		
Post Condiciones	No se podrán efectuar revisiones de control interno en estándares eliminados.		
Referencias	RF03		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al módulo Controles. 2. El administrador selecciona el menú Parametrizaciones. 3. El administrador selecciona el submenú Catálogos. 5. El administrador da clic sobre el botón Modificar. 7. El administrador da clic sobre el checkbox Activo para deshabilitar los controles. 8. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Catálogos tenga permisos de administrador. 4. El sistema muestra la lista de estándares creados y los botones Nuevo y Modificar. 6. El sistema muestra una pantalla con los dominios, objetivos de control y controle, checkbox Activo y los botones Guardar y Limpiar. 9. El sistema valida los datos ingresados y graba en la base de datos la información de dominios, objetivos de control y controles ingresados. 10. El sistema muestra el mensaje: “Control deshabilitado”.

Curso Alterno De Eventos
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si al momento de eliminar el estándar se mantiene revisiones de controles, el sistema mostrará el mensaje de error: “Estándar no puede ser eliminado”. 3. Si el usuario desea modificar la norma ISO27001 el sistema mostrará el mensaje de error: “Estándar no puede ser eliminado”

ANEXO F

CASO DE USO: GESTIÓN DE NIVELES DE MADUREZ

Caso De Uso	**RF04**	**N #**	**1**
Actores	Administrador (Principal) Sistema		
Propósito	Crear nivel de madurez en el sistema		
Tipo	Principal		
Resumen	Permitirá configurar los niveles de madurez de los controles y asignarles el respectivo porcentaje de completitud para cada nivel.		
Precondiciones	Sólo se podrán crear niveles de madurez para estándares existentes en el sistema.		
Post Condiciones	Si no existen niveles de madurez creados no se podrá realizar la evaluación del control interno.		
Referencias	RF04		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El administrador ingresa al módulo Controles. 2. El administrador selecciona el menú Parametrizaciones. 3. El administrador selecciona el submenú Estados. 6. El administrador selecciona el estándar a configurar los niveles de madurez. 8. El administrador ingresa los datos de los niveles de madurez y el porcentaje de completitud por cada nivel. 9. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Estados tenga permisos de administrador. 5. El sistema muestra la lista de estándares creados. 7. El sistema muestra la pantalla de creación de niveles de madurez y los botones Guardar, Eliminar y Cancelar. 10. El sistema valida los datos ingresados y graba en la base de datos la información de los niveles creados para el estándar. 11. El sistema muestra el mensaje: “Niveles de madurez creados exitosamente”.
Curso Alterno De Eventos	
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si no existe los porcentajes de completitud para algún nivel de madurez, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”.	

ANEXO F (cont.)

CASO DE USO: GESTIÓN DE NIVELES DE MADUREZ

Caso De Uso	**RF04**	**N #**	**2**
Actores	Administrador (Principal) Sistema		
Propósito	Modificar niveles de madurez en el sistema		
Tipo	Principal		
Resumen	Permitirá configurar los niveles de madurez de los controles y asignarles el respectivo porcentaje de completitud para cada nivel.		
Precondiciones	Sólo se podrán modificar niveles de madurez previamente creados en el sistema.		
Post Condiciones	Si existen revisiones de controles, no se podrán modificar los niveles de madurez.		
Referencias	RF04		
Curso Típico De Eventos			
Acciones Del Actor	**Respuesta Del Sistema**		
1. El administrador ingresa al módulo Controles. 2. El administrador selecciona el menú Parametrizaciones. 3. El administrador selecciona el submenú Estados. 6. El administrador selecciona el estándar a configurar los niveles de madurez. 8. El administrador modifica los datos de los niveles de madurez. 9. El administrador presiona el botón Guardar.	4. El sistema valida que el usuario que está accediendo al submenú Estados tenga permisos de administrador. 5. El sistema muestra la lista de estándares creados. 7. El sistema muestra la pantalla de niveles de madurez existentes para ese estándar y los botones Guardar, Eliminar y Cancelar. 10. El sistema valida los datos modificados y graba en la base de datos la información de los niveles modificados para el estándar. 11. El sistema muestra el mensaje: “Niveles de madurez modificados exitosamente”.		
Curso Alterno De Eventos			
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si no existe los porcentajes de completitud para algún nivel de madurez, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”. 3. Si al momento de modificar los niveles de madurez de cualquier estándar se mantienen revisiones de controles, el sistema mostrará el mensaje de error: “Niveles de madurez no puede ser modificado”.			

ANEXO F (cont.)

CASO DE USO: GESTIÓN DE NIVELES DE MADUREZ

Caso De Uso	**RF04**	**N #**	**3**
Actores	Administrador (Principal) Sistema		
Propósito	Eliminar niveles de madurez en el sistema		
Tipo	Principal		
Resumen	Permitirá configurar los niveles de madurez de los controles y asignarles el respectivo porcentaje de completitud para cada nivel.		
Precondiciones	Sólo se podrán eliminar niveles de madurez que no fueron considerados en la evaluación de controles.		
Post Condiciones			
Referencias	RF04		
Curso Típico De Eventos			
Acciones Del Actor	**Respuesta Del Sistema**		
1. El administrador ingresa al módulo Controles. 2. El administrador selecciona el menú Parametrizaciones. 3. El administrador selecciona el submenú Estados. 6. El administrador selecciona el estándar a eliminar los niveles de madurez. 8. El administrador presiona el botón Eliminar.	4. El sistema valida que el usuario que está accediendo al submenú Estados tenga permisos de administrador. 5. El sistema muestra la lista de estándares creados. 7. El sistema muestra la pantalla de niveles de madurez existentes para ese estándar y los botones Guardar, Eliminar y Cancelar. 9. El sistema muestra el mensaje: “Nivel de madurez ha sido eliminado”.		
Curso Alterno De Eventos			
1. Si el usuario no tiene permisos de Administrador, el sistema mostrará el mensaje de error: “Usuario sin permisos Administrador”. 2. Si no existe los porcentajes de completitud para algún nivel de madurez, el sistema mostrará el mensaje de error: “Información no está completa, favor revisar”. 3. Si al momento de eliminar los niveles de madurez de cualquier estándar se mantienen revisiones de controles, el sistema mostrará el mensaje de error: “Nivel de madurez no puede ser eliminado”.			

ANEXO G

CASO DE USO: REVISIÓN DE CONTROLES

<table>
<tr><td>Caso De Uso</td><td colspan="2">RF05</td><td>N #</td><td>1</td></tr>
<tr><td>Actores</td><td colspan="4">Usuario (Principal)
Sistema</td></tr>
<tr><td>Propósito</td><td colspan="4">Revisión de controles de buenas prácticas</td></tr>
<tr><td>Tipo</td><td colspan="4">Principal</td></tr>
<tr><td>Resumen</td><td colspan="4">Permitirá realizar la revisión de los controles cargados de la norma ISO 27001 u otras normas creadas desde Gestión de Estándares.</td></tr>
<tr><td>Precondiciones</td><td colspan="4">Para la evaluación de controles se necesita tener establecido unidades, estándares y niveles de madurez.</td></tr>
<tr><td>Post Condiciones</td><td colspan="4">No aplica</td></tr>
<tr><td>Referencias</td><td colspan="4">RF05</td></tr>
<tr><td colspan="5">Curso Típico De Eventos</td></tr>
<tr><td colspan="2">Acciones Del Actor</td><td colspan="3">Respuesta Del Sistema</td></tr>
<tr><td colspan="2">1. El usuario ingresa al módulo Controles.
2. El usuario selecciona el menú Análisis.
5. El usuario selecciona un proyecto creado previamente para realizar la evaluación de controles
7. El usuario selecciona el estándar a evaluar.
8. El usuario presiona el botón Nuevo.
9. El usuario coloca la fecha de la evaluación del estándar.
13.
12. El usuario ingresa en el campo Estado actual el nivel de madurez para cada control.
13. El usuario ingresa los valores para los campos: Justificación, Responsable del Control y Observaciones.
14. El usuario da clic sobre el botón Guardar</td><td colspan="3">3. El sistema valida que el usuario que está accediendo al menú Análisis tenga asignado el rol de Usuario.
4. El sistema muestra la pantalla de los proyectos creados.
6. El sistema muestra una pantalla donde se encuentran los estándares evaluados y además existe un combo box con los estándares creados seguido de los botones Nuevo y Eliminar.
10. El sistema muestra el nombre del estándar junto a los otros evaluados y la opción de Fecha de revisión.
11. El sistema permite el ingreso al estándar a evaluar y muestra una pantalla con los campos: controles, justificación, responsable, revisor y observaciones. Adicional muestra los botones Guardar y Cancelar.
15. El sistema almacena la información de la evaluación del control interno y muestra el mensaje: “Transacción exitosa”.</td></tr>
<tr><td colspan="5">Curso Alterno De Eventos</td></tr>
<tr><td colspan="5">1. Si el usuario no tiene asignado el rol de Seguridad de la Información, el sistema mostrará el mensaje de error: “Usuario sin permisos al rol adecuado”.</td></tr>
</table>

ANEXO H

CASO DE USO: GENERACIÓN DE LISTADOS DE CONTROLES

<table>
<tr><td>Caso De Uso</td><td>RF06</td><td>N #</td><td>1</td></tr>
<tr><td>Actores</td><td colspan="3">Usuario (Principal)
Sistema</td></tr>
<tr><td>Propósito</td><td colspan="3">Generación de informe con la evaluación del control interno</td></tr>
<tr><td>Tipo</td><td colspan="3">Principal</td></tr>
<tr><td>Resumen</td><td colspan="3">La herramienta será capaz de permitir la generación en formato editable del listado o informe con el estado actual de los controles para cada uno de los estándares.</td></tr>
<tr><td>Precondiciones</td><td colspan="3">Sólo se podrá descargar el informe con el listado de controles para aquellos estándares que han sido evaluados.</td></tr>
<tr><td>Post Condiciones</td><td colspan="3">No aplica</td></tr>
<tr><td>Referencias</td><td colspan="3">RF06</td></tr>
<tr><td colspan="4">Curso Típico De Eventos</td></tr>
<tr><td colspan="2">Acciones Del Actor</td><td colspan="2">Respuesta Del Sistema</td></tr>
<tr><td colspan="2">1. El usuario ingresa al módulo Controles.
2. El usuario selecciona el menú Análisis.
3. El usuario selecciona el submenú Gestor Documental.
6. El usuario selecciona una unidad creada previamente.
8. El usuario selecciona el estándar.
10. El usuario presiona el botón Descargar.</td><td colspan="2">4. El sistema valida que el usuario que está accediendo al submenú Gestor Documental sea un usuario autorizado.
5. El sistema muestra la pantalla de unidades creadas.
7. El sistema muestra una pantalla donde se encuentran los estándares evaluados.
9. El sistema muestra la evaluación de los controles para la unidad y estándar seleccionados y en la parte superior de la pantalla el botón Descargar.
11. El sistema descarga el informe con la evaluación de los controles.</td></tr>
<tr><td colspan="4">Curso Alterno De Eventos</td></tr>
<tr><td colspan="4">1. Si el usuario no tiene asignado un rol para descargar informes, el sistema mostrará el mensaje de error: “Usuario sin permisos al rol adecuado”.</td></tr>
</table>

ANEXO I

CASO DE USO: GENERACIÓN DE GRÁFICAS

Caso De Uso	**RF07**	**N #**	**1**
Actores	Usuario (Principal) Sistema		
Propósito	Generación de gráficas de análisis de brecha de controles.		
Tipo	Principal		
Resumen	La herramienta permitirá la generación de gráficas con el estado de madurez actual de los controles para cada uno de los estándares haciendo una comparación con el estado ideal que desea alcanzar la institución.		
Precondiciones	Sólo se podrá descargar las gráficas con el análisis de brechas de controles para aquellos estándares que han sido evaluados.		
Post Condiciones	No aplica		
Referencias	RF07		

Curso Típico De Eventos	
Acciones Del Actor	**Respuesta Del Sistema**
1. El usuario ingresa al módulo Controles. 2. El usuario selecciona el menú Análisis. 3. El usuario selecciona el submenú Gestor Documental. 6. El usuario selecciona una unidad creada previamente. 8. El usuario selecciona el estándar. 10. El usuario presiona el botón Gráficas.	4. El sistema valida que el usuario que está accediendo al submenú Gestor Documental sea un usuario autorizado. 5. El sistema muestra la pantalla de unidades creadas. 7. El sistema muestra una pantalla donde se encuentran los estándares evaluados. 9. El sistema muestra la evaluación de los controles para la unidad y estándar seleccionados y en la parte superior de la pantalla el botón Gráficas. 11. El sistema genera las gráficas con el análisis de brecha de los controles.
Curso Alterno De Eventos	
1. Si el usuario no tiene asignado un rol para descargar informes, el sistema mostrará el mensaje de error: “Usuario sin permisos al rol adecuado”.	

ANEXO J

INVENTARIO DE CONTROLES
NORMA UNE-ISO/IEC 27001:2013

A.5	Políticas de seguridad de la información
A.5.1	Directrices de gestión de la seguridad de la información
A.5.1.1	Políticas para la seguridad de la información
A.5.1.2	Revisión de las políticas para la seguridad de la información
A.6	Organización de la seguridad de la información
A.6.1	Organización interna
A.6.1.1	Roles y responsabilidades en seguridad de la información
A.6.1.2	Segregación de tareas
A.6.1.3	Contacto con las autoridades
A.6.1.4	Contacto con grupos de interés especial
A.6.1.5	Seguridad de la información en la gestión de proyectos
A.6.2	Los dispositivos móviles y el teletrabajo
A.6.2.1	Política de dispositivos móviles
A.6.2.2	Teletrabajo
A.7	Seguridad relativa a los recursos humanos
A.7.1	Antes del empleo
A.7.1.1	Investigación de antecedentes
A.7.1.2	Términos y condiciones del empleo
A.7.2	Durante el empleo
A.7.2.1	Responsabilidades de gestión
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información
A.7.2.3	Proceso disciplinario
A.7.3	Finalización del empleo o cambio en el puesto de trabajo
A.7.3.1	Responsabilidades ante la finalización o cambio
A.8	Gestión de activos
A.8.1	Responsabilidad sobre los activos
A.8.1.1	Inventario de activos
A.8.1.2	Propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devolución de activos
A.8.2	Clasificación de la información
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A.8.2.3	Manipulado de la información
A.8.3	Manipulación de los soportes
A.8.3.1	Gestión de soportes extraíbles
A.8.3.2	Eliminación de soportes
A.8.3.3	Soportes físicos en tránsito
A.9	Control de acceso

A.9.1	Requisitos de negocio para el control de acceso
A.9.1.1	Política de control de acceso
A.9.1.2	Acceso a las redes y a los servicios de red
A.9.2	Gestión de acceso de usuario
A.9.2.1	Registro y baja de usuario
A.9.2.2	Provisión de acceso de usuario
A.9.2.3	Gestión de privilegios de acceso
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios
A.9.2.5	Revisión de los derechos de acceso de usuario
A.9.2.6	Retirada o reasignación de los derechos de acceso
A.9.3	Responsabilidades del usuario
A.9.3.1	Uso de la información secreta de autenticación
A.9.4	Control de acceso a sistemas y aplicaciones
A.9.4.1	Restricción del acceso a la información
A.9.4.2	Procedimientos seguros de inicio de sesión
A.9.4.3	Sistema de gestión de contraseñas
A.9.4.4	Uso de utilidades con privilegios del sistema
A.9.4.5	Control de acceso al código fuente de los programas
A.10	Criptografía
A.10.1	Controles criptográficos
A.10.1.1	Política de uso de los controles criptográficos
A.10.1.2	Gestión de claves
A.11	Seguridad física y del entorno
A.11.1	Áreas seguras
A.11.1.1	Perímetro de seguridad física
A.11.1.2	Controles físicos de entrada
A.11.1.3	Seguridad de oficinas, despachos y recursos
A.11.1.4	Protección contra las amenazas externas y ambientales
A.11.1.5	El trabajo en áreas seguras
A.11.1.6	Áreas de carga y descarga
A.11.2	Seguridad de los equipos
A.11.2.1	Emplazamiento y protección de equipos
A.11.2.2	Instalaciones de suministro
A.11.2.3	Seguridad del cableado
A.11.2.4	Mantenimiento de los equipos
A.11.2.5	Retirada de materiales propiedad de la empresa
A.11.2.6	Seguridad de los equipos fuera de las instalaciones
A.11.2.7	Reutilización o eliminación segura de equipos
A.11.2.8	Equipo de usuario desatendido
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia
A.12	Seguridad de las operaciones
A.12.1	Procedimientos y responsabilidades operacionales
A.12.1.1	Documentación de procedimientos de los operación
A.12.1.2	Gestión de cambios
A.12.1.3	Gestión de capacidades

A.12.1.4	Separación de los recursos de desarrollo, prueba y operación
A.12.2	Protección contra el software malicioso (malware)
A.12.2.1	Controles contra el código malicioso
A.12.3	Copias de seguridad
A.12.3.1	Copias de seguridad de la información
A.12.4	Registros y supervisión
A.12.4.1	Registro de eventos
A.12.4.2	Protección de la información de registro
A.12.4.3	Registros de administración y operación
A.12.4.4	Sincronización del reloj
A.12.5	Control del software en explotación
A.12.5.1	Instalación del software en explotación
A.12.6	Gestión de la vulnerabilidad técnica
A.12.6.1	Gestión de las vulnerabilidades técnicas
A.12.6.2	Restricción en la instalación de software
A.12.7	Consideraciones sobre la auditoria de sistemas de información
A.12.7.1	Controles de auditoría de sistemas de información
A.13	Seguridad de las comunicaciones
A.13.1	Gestión de la seguridad de redes
A.13.1.1	Controles de red
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Segregación en redes
A.13.2	Intercambio de información
A.13.2.1	Políticas y procedimientos de intercambio de información
A.13.2.2	Acuerdos de intercambio de información
A.13.2.3	Mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o no revelación
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información
A.14.1	Requisitos de seguridad en sistemas de información
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas
A.14.1.3	Protección de las transacciones de servicios de aplicaciones
A.14.2	Seguridad en el desarrollo y en los procesos de soporte
A.14.2.1	Política de desarrollo seguro
A.14.2.2	Procedimiento de control de cambios en sistemas
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A.14.2.4	Restricciones a los cambios en los paquetes de software
A.14.2.5	Principios de ingeniería de sistemas seguros
A.14.2.6	Entorno de desarrollo seguro
A.14.2.7	Externalización del desarrollo de software
A.14.2.8	Pruebas funcionales de seguridad de sistemas
A.14.2.9	Pruebas de aceptación de sistemas
A.14.3	Datos de prueba
A.14.3.1	Protección de los datos de prueba
A.15	Relación con proveedores

A.15.1	Seguridad en las relaciones con proveedores
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores
A.15.1.2	Requisitos de seguridad en contratos con terceros
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones
A.15.2	Gestión de la provisión de servicios del proveedor
A.15.2.1	Control y revisión de la provisión de servicios del proveedor
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor
A.16	Gestión de incidentes de seguridad de la información
A.16.1	Gestión de incidentes de seguridad de la información y mejoras
A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Notificación de los eventos de seguridad de la información
A.16.1.3	Notificación de puntos débiles de la seguridad
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información
A.16.1.5	Respuesta a incidentes de seguridad de la información
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información
A.16.1.7	Recopilación de evidencias
A.17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio
A.17.1	Continuidad de la seguridad de la información
A.17.1.1	Planificación de la continuidad de la seguridad de la información
A.17.1.2	Implementar la continuidad de la seguridad de la información
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.17.2	Redundancias
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información
A.18	Cumplimiento
A.18.1	Cumplimiento de los requisitos legales y contractuales
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
A.18.1.2	Derechos de propiedad intelectual (DPI)
A.18.1.3	Protección de los registros de la organización
A.18.1.4	Protección y privacidad de la información de carácter personal
A.18.1.5	Regulación de los controles criptográficos
A.18.2	Revisiones de la seguridad de la información
A.18.2.1	Revisión independiente de la seguridad de la información
A.18.2.2	Cumplimiento de las políticas y normas de seguridad
A.18.2.3	Comprobación del cumplimiento técnico

ANEXO K

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

ENCUESTA DE SATISFACCIÓN

"DESARROLLO DE UNA HERRAMIENTA DE SOFTWARE COMO ASISTENTE METODOLÓGICO PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL"

Instrucción:

Marque con una **X** el valor que mejor refleje su opinión a las siguientes preguntas, tomando en cuenta:

5. Excelente 4. Muy Bueno 3. Bueno 2. Regular 1. Malo

Pregunta		Calificación				
		5	4	3	2	1
Utilidad						
1	¿Es de fácil manejo?					
2	¿Se requiere de amplios conocimientos sobre control interno?					
3	¿Permite localizar fácilmente la información?					
4	¿El sistema permite adaptabilidad a los usuarios?					
5	¿Se requiere de amplios conocimientos sobre control interno?					
6	¿El sistema muestra con claridad los errores presentados?					
7	¿El sistema se ajusta a los criterios de evaluación?					

Control del Programa						
8	¿Su interface es amigable al usuario?					
9	¿El sistema es interactivo?					
10	¿El diseño de pantallas es el adecuado?					
11	¿Es adecuado el uso de botones, ventanas, combo box, etc.?					
12	¿El vocabulario es el adecuado?					
13	¿El sistema es intuitivo para el registro de la información?					
Técnicos						
14	¿Los recursos empleados en el desarrollo son los adecuados?					
15	¿Existe documentación técnica y de usuario del sistema?					

ANEXO L

INFORME DE ASEGURAMIENTO DE CALIDAD

	Día del Informe:	Jueves 01-09-2016
Carolina Morocho Crespo	*Periodo Inicio:*	Lunes 01-08-2016
Responsables del Control	*Periodo Término:*	Miércoles 31-08-2016

1. Resumen Ejecutivo

1.1. Situación Actual

Detallamos a continuación las actividades claves ejecutadas en este periodo:

Ejecución de pruebas funcionales de los desarrollos correspondientes al módulo de Seguridad.

- Ejecución de pruebas funcionales de los desarrollos correspondientes al módulo de Controles.
- Seguimiento a la resolución de incidentes de pruebas funcionales del módulo de Seguridad.
- Seguimiento a la resolución de incidentes de pruebas funcionales del módulo de Controles.
- Reunión de avance del proyecto de titulación con la participación del tutor Ing. Ismelis Castellanos.

1.2. Indicadores de Gestión

TIEMPO	**Se ha identificado el 2% de retraso de acuerdo a las actividades planificadas.**	
COSTOS	**Los costos incurridos en el proyecto se encuentran dentro del presupuesto.**	
RESULTADOS	**Los entregables generados hasta la fecha cumplen con los requisitos de calidad.**	

1.3. Resumen de Alertas Tempranas y Críticas

Alertas de Control		
Actividades	**Nivel de Riesgo**	**Esfuerzo de Resolución**
ALERTA TEMPRANA Retraso en el avance de Pruebas Funcionales para los Módulos: Seguridad y Controles		

Leyendas

Estas leyendas serán utilizadas para describir los atributos de las observaciones informadas por el equipo de Aseguramiento de Calidad.

Riesgo

- **Alto:** El riesgo puede tener un impacto muy adverso en el Proyecto. Se requerirán acciones adicionales significativas y de alta prioridad.
- **Medio:** El riesgo puede tener un impacto limitado en el Proyecto. Pueden ser requeridas acciones específicas y de atención para mitigar el riesgo.
- **Bajo:** El riesgo puede causar problemas mínimos al Proyecto. Para controlar el riesgo será suficiente implementar acciones en el entorno del Proyecto y será requerida una atención normal.

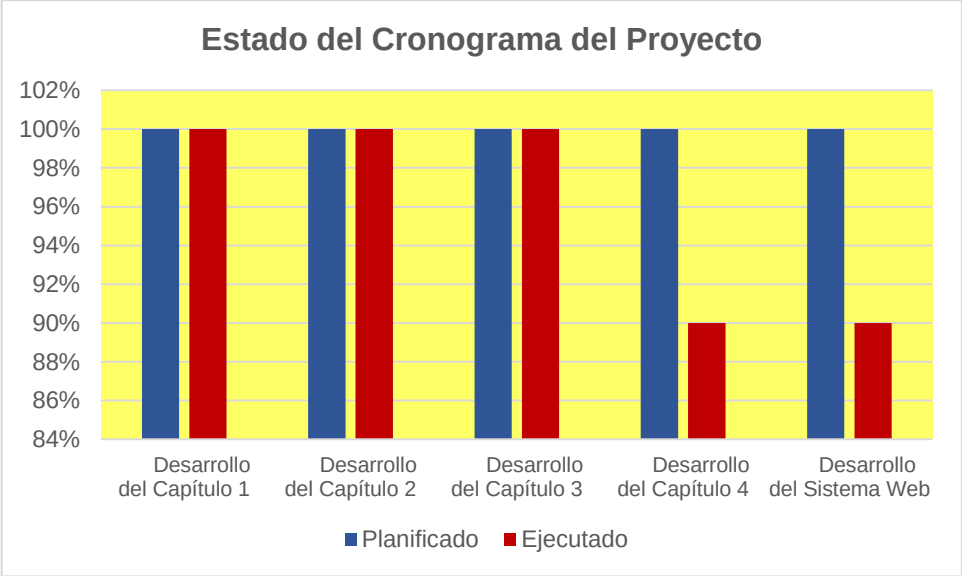
Esfuerzo de Resolución

- **Alto:** Requiere de varios días y varias personas para la solución de la observación.
- **Medio:** La solución puede requerir desde algunas horas hasta algunos días de esfuerzo y no involucra un número considerable de personas.
- **Bajo:** Se deben de realizar cambios menores lo cual puede incurrir en algunas horas de esfuerzo y con un número limitado de personas.

1.4. Resumen de Cumplimiento de los Cronogramas

Referencia a:
* Cronograma General del Proyecto

1.4.1. Panorama General del Proyecto



El gráfico muestra el porcentaje acumulado de cumplimiento de las actividades ejecutadas sobre las actividades planificadas hasta el periodo de reporte. Se ha identificado el 2% de desvío en el cumplimiento del cronograma, correspondiente a las actividades de pruebas de desarrollos.

2. Gestión de Entregables

2.1. Calidad de Resultados

Reuniones de Seguimiento - Pruebas Funcionales

De acuerdo a lo planificado en el Cronograma General del Proyecto, se han realizado reuniones de seguimiento de avance de pruebas funcionales validando el cumplimiento de criterios de calidad en la documentación generada del Proyecto.

3. Gestión de Riesgos

3.1. Riesgos abiertos durante el período de revisión

La gestión de riesgos del proyecto, prevé un evento o condición probable que impacte en los objetivos del proyecto. En el Proyecto de titulación, se ha definido un plan de gestión de riesgos, en el cual se incluye los planes de respuesta

respectivos. El monitoreo de estos riesgos es mensual; en dicho monitoreo se revisa si existen cambios en las probabilidades de materialización del riesgo así como la efectividad de los planes de respuesta.

N°	Riesgos abiertos en el periodo de revisión	Plan de Acción	Responsable
PROBABILIDAD DE OCURRENCIA CON TENDENCIA A INCREMENTAR			
1	Tiempo insuficiente para realizar las actividades de proyecto.	- Llevar un adecuado control de la duración de las actividades de acuerdo a lo planificado en el cronograma. - Identificar retrasos y comunicar oportunamente para establecer nuevas estrategias. - Incrementar recursos en caso de que aplique para cumplir con los tiempos establecidos.	Sponsor del Proyecto
2	Tiempos de respuesta de novedades reportadas referentes a pruebas funcionales mayor al planificado.	- resolución de los incidentes con prioridad 1 con la finalidad de que sean atendidos a la brevedad posible. - Reuniones de seguimiento semanales para identificar el estado de los incidentes generados.	Líder de Pruebas
PROBABILIDAD DE OCURRENCIA CON TENDENCIA A MANTENERSE			
3	Mantener Metodologías de pruebas funcionales	- Coordinar y comunicar oportunamente con los equipos del proyecto las actividades adicionales requeridas para completar el proceso de pruebas funcionales. - Monitorear el cumplimiento de las actividades identificando desvíos significativos que impacten a la fecha de salida del proyecto. - Evaluar la posibilidad de incrementar recursos para la atención y ejecución de las nuevas tareas.	Sponsor del Proyecto

4. Detalle de Alertas y Recomendaciones

4.1. Alertas Tempranas

Retraso en el avance de Pruebas Funcionales – Módulos Seguridad y Controles

De acuerdo al cronograma general del proyecto, se encuentran ejecutando las actividades correspondientes a pruebas funcionales de los módulos Seguridad y Controles, teniendo el siguiente avance con corte a la fecha del presente informe:

Módulo	Avance General
Seguridad	90%
Controles	90%

Las situaciones detalladas han ocasionado un desfase de 2% en el cronograma general del proyecto, generando el riesgo de incumplimiento de los plazos establecidos para la ejecución de estas tareas y actividades sucesoras. A la fecha de corte del presente informe, el equipo de proyecto continúa ejecutando los planes de acción mitigantes con el fin de continuar recuperando el tiempo.

5. Actividades Realizadas

5.1. Actividades de Seguimiento

- Seguimiento a la ejecución de pruebas funcionales, 04-Agosto-2016.
- Reunión con el tutor del proyecto de titulación, 08-Agosto-2016.
- Seguimiento a la ejecución de pruebas funcionales, 12-Agosto-2016.
- Reunión con el tutor del proyecto de titulación, 15-Agosto-2016.
- Seguimiento a la ejecución de pruebas funcionales, 23-Agosto-2016.
- Reunión con el tutor del proyecto de titulación, 26-Agosto-2016.

ANEXO M

EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO

	Día del Informe:	Jueves 01-09-2016
Carolina Morocho Crespo	*Periodo Inicio:*	Lunes 01-08-2016
Responsables del Control	*Periodo Término:*	Miércoles 31-08-2016

1. Objetivo de la evaluación del control interno

Determinar el estado actual de madurez del Control Interno Informático de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil (en adelante CISC), tomando como referente la norma ISO/IEC 27001.

1.1. Objetivos Específicos

- Conocer la situación actual del control interno informático de CISC.
- Identificar el nivel de madurez de cada uno los controles implementados en CISC frente a los detallados en la norma ISO/IEC 27001.

2. Alcance

La presente evaluación del control interno informático fue desarrollada bajo los siguientes supuestos:

- La información relevada refleja la situación actual de CISC.
- No se requieren pruebas de eficacia operativa para confirmar la operación de los controles.
- La evaluación a ejecutarse es a nivel de subdominios.

2.1. Áreas revisadas

Para el presente informe se revisaron los controles definidos en la norma ISO/IEC 27001 y aplicables para CISC, los cuales describen los objetivos de control y controles establecidos para realizar una adecuada gestión del control interno. A

continuación se mencionan las siguientes categorías principales que soportan los controles informáticos:

- Política de Seguridad de la Información
- Control de Accesos
- Seguridad Física y Ambiental
- Seguridad en las operaciones
- Seguridad de las comunicaciones
- Adquisición, Desarrollo y Mantenimiento de Sistemas

La evaluación se basó en estas seis (6) categorías principales de control.

3. Metodología de Análisis

Con base en el plan de trabajo establecido en el cronograma del proyecto, esta evaluación del control interno informático la realizamos mediante la ejecución de entrevistas al Ing. Jorge Alvarado – Coordinador del Departamento de Software de CISC.

3.1. Análisis de Controles

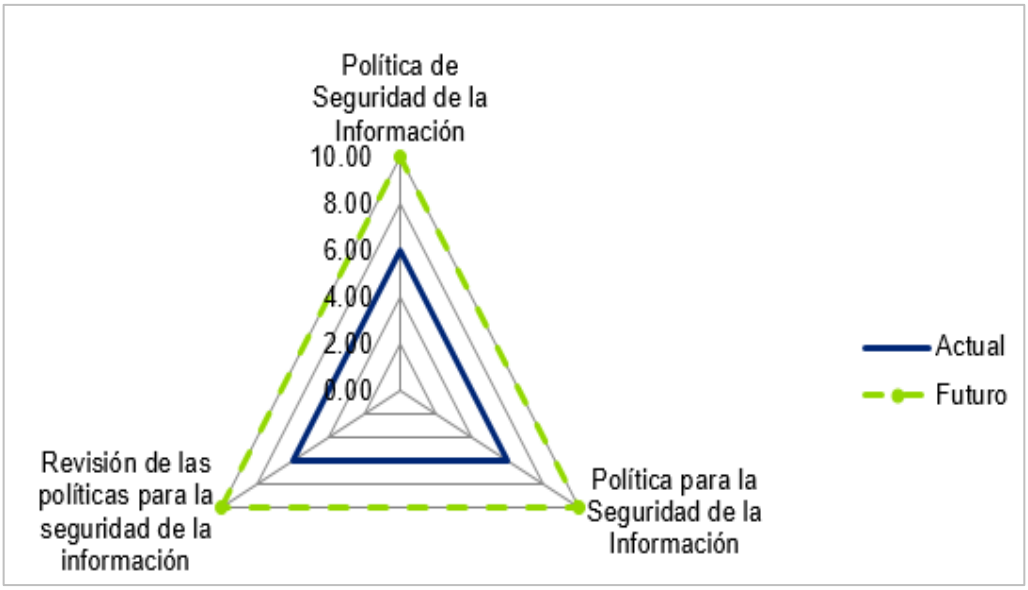
Con el objetivo de realizar la evaluación de los controles definidos en CISC frente al Anexo A de la norma ISO27001, utilizamos un Modelo Genérico de Madurez. Dicho modelo establece seis posibles niveles de madurez de acuerdo con los criterios generales mencionados a continuación:

Nivel de Madurez	Descripción
10 - Optimizado	La carrera ha refinado su cumplimiento a un nivel de buena práctica.
8 – Administrado	La carrera regularmente mide su cumplimiento y hace mejoras al proceso de forma regular.
6 – Definido	La carrera aplica un enfoque detallado, documentado. Pero no existe medición, ni reforzamiento periódico del mismo.
4 – Repetible	La carrera tiene un enfoque consistente, pero en su mayoría no está documentado.

Nivel de Madurez	Descripción
2 – Inicial	La carrera tiene un enfoque ad-hoc o desestructurado en esta práctica o estándar.
0 – No definido	No hay evidencia de este estándar o práctica en la carrera.

El análisis del estado de madurez de los controles se realizó por dominio y sub-dominio. Dicho análisis no contempló la ejecución de pruebas exhaustivas para determinar su estado actual (Referirse a los supuestos de la sección 2 - Alcance).

El nivel de madurez por cada dominio y subdominio fue representando a través de un gráfico araña como se muestra a continuación:



El nombre del dominio se encuentra en la parte superior del gráfico y dependiendo del número de subdominios que contiene dicho dominio, se graficarán alrededor en la figura correspondiente.

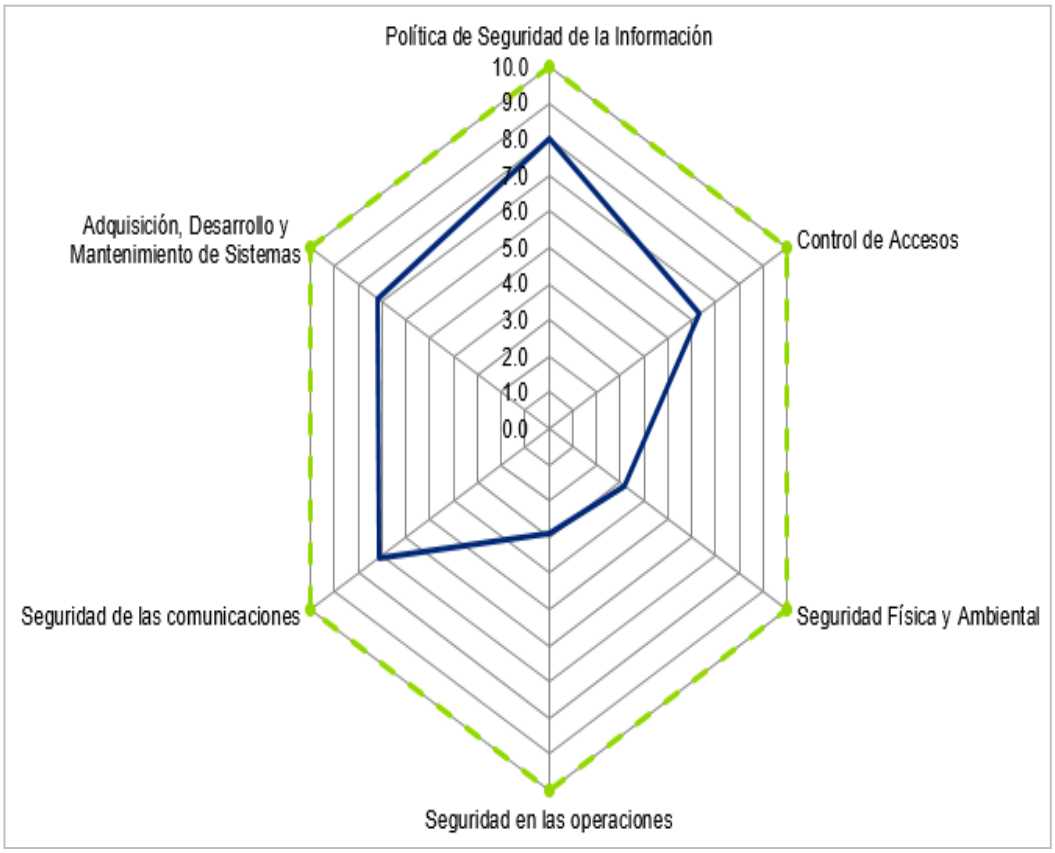
4. Resultados

A continuación se presentan los resultados de la evaluación de los controles implementados en CISC contra los controles definidos en las buenas prácticas de la norma ISO/IEC 27001.

4.1. Controles

Luego del análisis y revisión del control interno informático realizado a las categorías incluidas en la sección 2 - Alcance de este documento, establecimos que el nivel de madurez de CISC frente a la norma es **5 - Repetible**, lo cual indica que CISC aplica un enfoque consistente, pero que en muchos de los casos no cuenta con documentación que soporte la implementación de los controles.

El siguiente gráfico resume el estado de madurez para cada dominio y el estado que se sugiere como meta de CISC: **Optimizado.**



Nivel de madurez logrado en CISC frente a los dominios de control de la Norma ISO 27001

4.2. Resultados por dominios de control

Adicionalmente el análisis estableció el nivel de madurez alcanzado para cada una de las categorías principales de control. Estos niveles de madurez se encuentran descritos en la sección 3.1. Análisis de Controles de este documento.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a la revisión y el nivel de madurez en el que se encuentra CISC, con respecto al dominio A.1 Política de Seguridad de la Información, los subdominios se encuentran en un Nivel de Madurez: **8 - Administrado.**

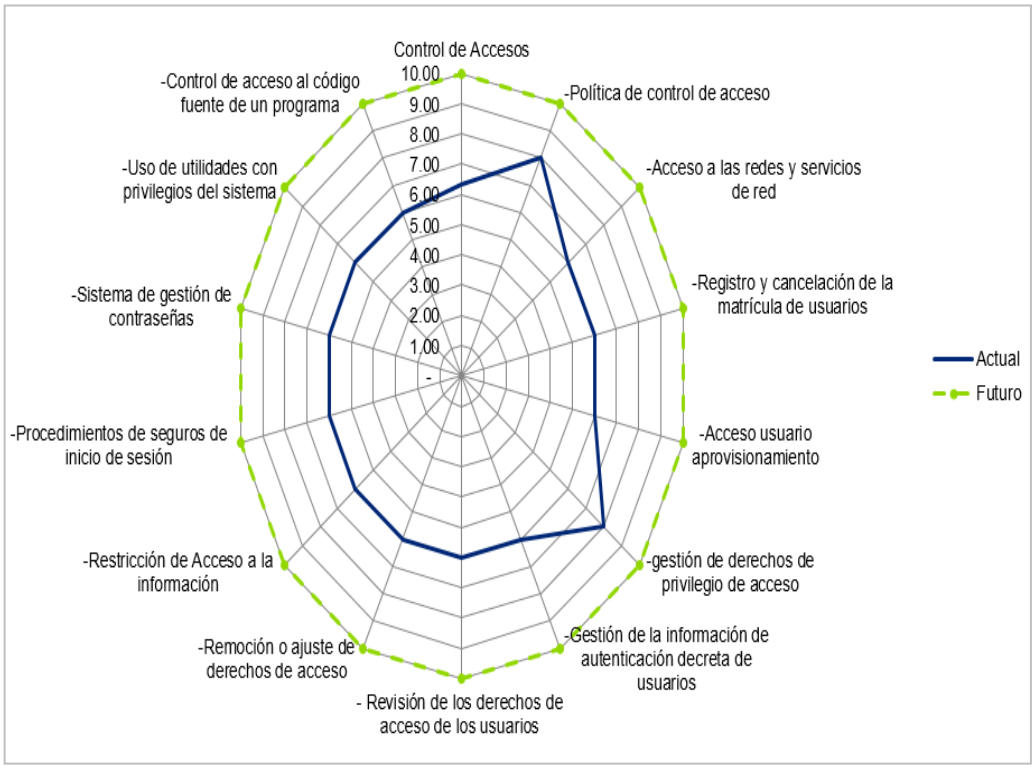
Nivel de madurez logrado en CISC frente al dominio A.1 Política de Seguridad de la información.

Los subdominios evaluados se indican a continuación:

Subdominio	Nombre de Subdominio
1.1.1	Política para la Seguridad de la Información
1.1.2	Revisión de las políticas para la seguridad de la información

CONTROL DE ACCESO

De acuerdo a la revisión y el nivel de madurez en el que se encuentra CISC, con respecto al dominio A.2 Control de Acceso, los subdominios se encuentran en un Nivel de Madurez: **6 – Definido.**



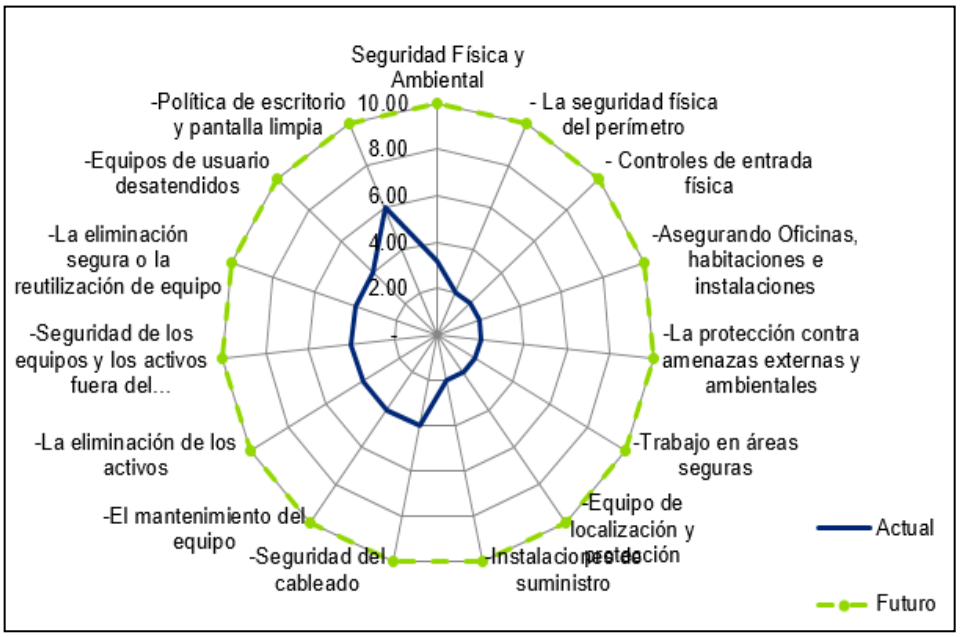
Nivel de madurez logrado en CISC frente al dominio A.2 Control de Acceso.

Los subdominios evaluados se indican a continuación:

Subdominio	Nombre de Subdominio
2.1.1	Política de control de acceso
2.1.2	Acceso a las redes y servicios de red
2.2.1	Registro y cancelación de la matrícula de usuarios
2.2.2	Acceso usuario aprovisionamiento
2.2.3	Gestión de derechos de privilegio de acceso
2.2.4	Gestión de la información de autenticación de usuarios
2.2.5	Revisión de los derechos de acceso de los usuarios
2.2.6	Remoción o ajuste de derechos de acceso
2.3.1	Restricción de Acceso a la información
2.3.2	Procedimientos de seguros de inicio de sesión
2.3.3	Sistema de gestión de contraseñas
2.3.4	Uso de utilidades con privilegios del sistema
2.3.5	Control de acceso al código fuente de un programa

SEGURIDAD FÍSICA Y AMBIENTAL

De acuerdo a la revisión y el nivel de madurez en el que se encuentra CISC, con respecto al dominio A.3 Seguridad Física y Ambiental, los subdominios se encuentran en un Nivel de Madurez: **3 - Inicial.**



Nivel de madurez logrado en CISC frente al dominio A.3 Seguridad Física y Ambiental.

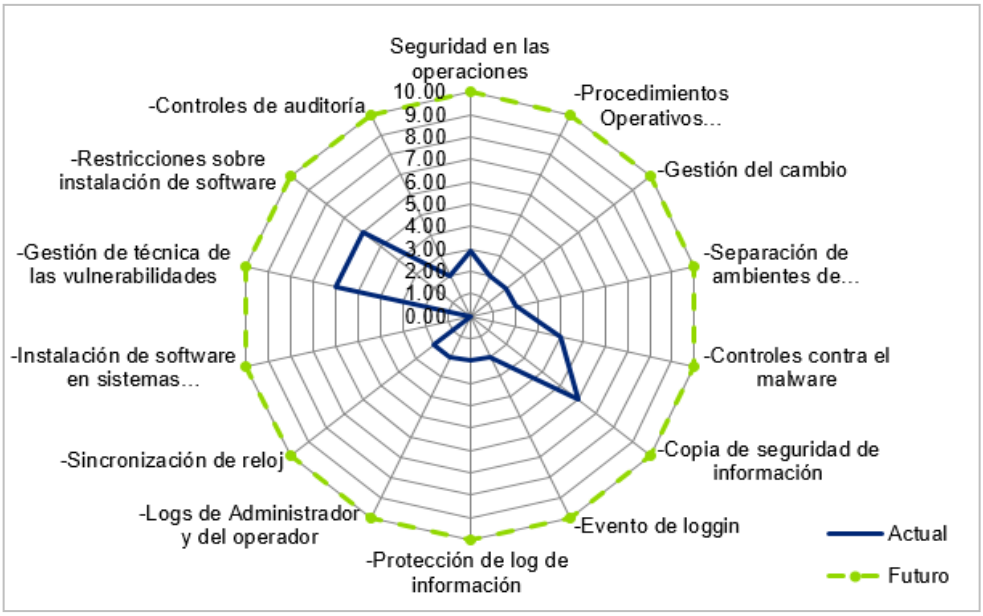
Los subdominios evaluados se indican a continuación:

Subdominio	Nombre de Subdominio
3.1.1	La seguridad física del perímetro
3.1.2	Controles de entrada física
3.1.3	Asegurando Oficinas, habitaciones e instalaciones
3.1.4	La protección contra amenazas externas y ambientales
3.1.5	Trabajo en áreas seguras
3.2.1	Equipo de localización y protección
3.2.2	Instalaciones de suministro
3.2.3	Seguridad del cableado
3.2.4	El mantenimiento del equipo

Subdominio	Nombre de Subdominio
3.2.5	La eliminación de los activos
3.2.6	Seguridad de los equipos fuera del establecimiento
3.2.7	La eliminación segura o la reutilización de equipo
3.2.8	Equipos de usuario desatendidos
3.2.9	Política de escritorio y pantalla limpia

SEGURIDAD EN LAS OPERACIONES

De acuerdo a la revisión y el nivel de madurez en el que se encuentra el CISC, respecto al dominio A.4 Seguridad en las Operaciones, los subdominios se encuentran en un Nivel de Madurez: **3 - Inicial.**



Nivel de madurez logrado en CISC frente al dominio A.4 Seguridad en las Operaciones.

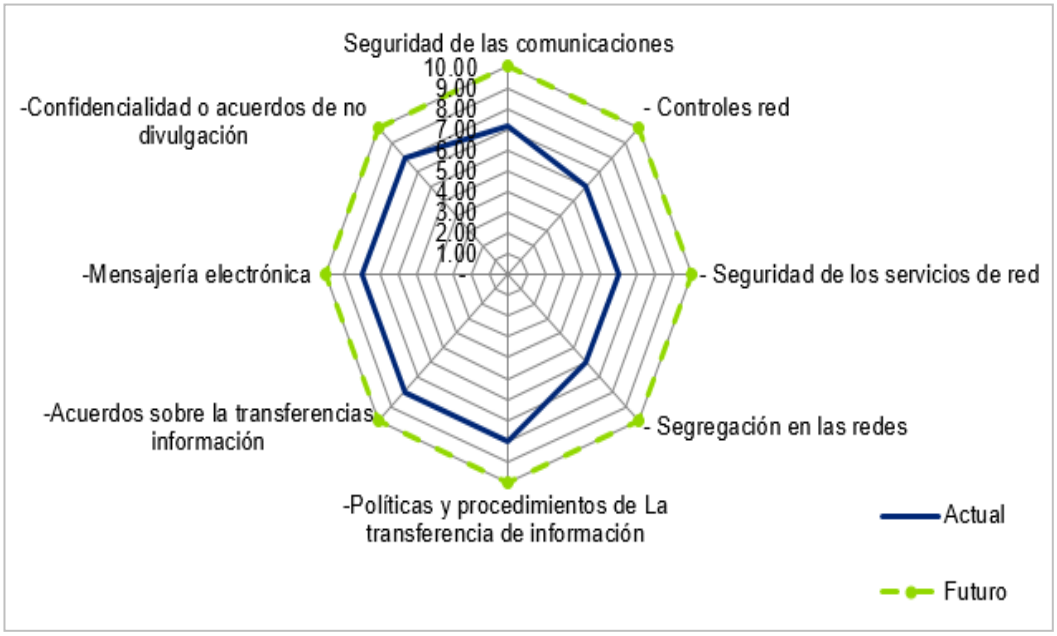
Los subdominios evaluados se indican a continuación:

Subdominio	Nombre de Subdominio
4.1.1	Procedimientos Operativos Documentados
4.1.2	Gestión del cambio

Subdominio	Nombre de Subdominio
4.1.3	Separación de ambientes desarrollo, pruebas y producción
4.2.1	Controles contra el malware
4.3.1	Copia de seguridad de información
4.4.1	Evento de loggin
4.4.2	Protección de log de información
4.4.3	Logs de Administrador y del operador
4.4.4	Sincronización de reloj
4.5.1	Instalación de software en sistemas operacionales
4.6.1	Gestión de técnica de las vulnerabilidades
4.6.2	Restricciones sobre instalación de software
4.7.1	Controles de auditoría

SEGURIDAD DE LAS COMUNICACIONES

De acuerdo a la revisión y el nivel de madurez en el que se encuentra CISC, con respecto al dominio A.5 Seguridad de las comunicaciones, los subdominios se encuentran en un Nivel de Madurez: **7 - Definido.**



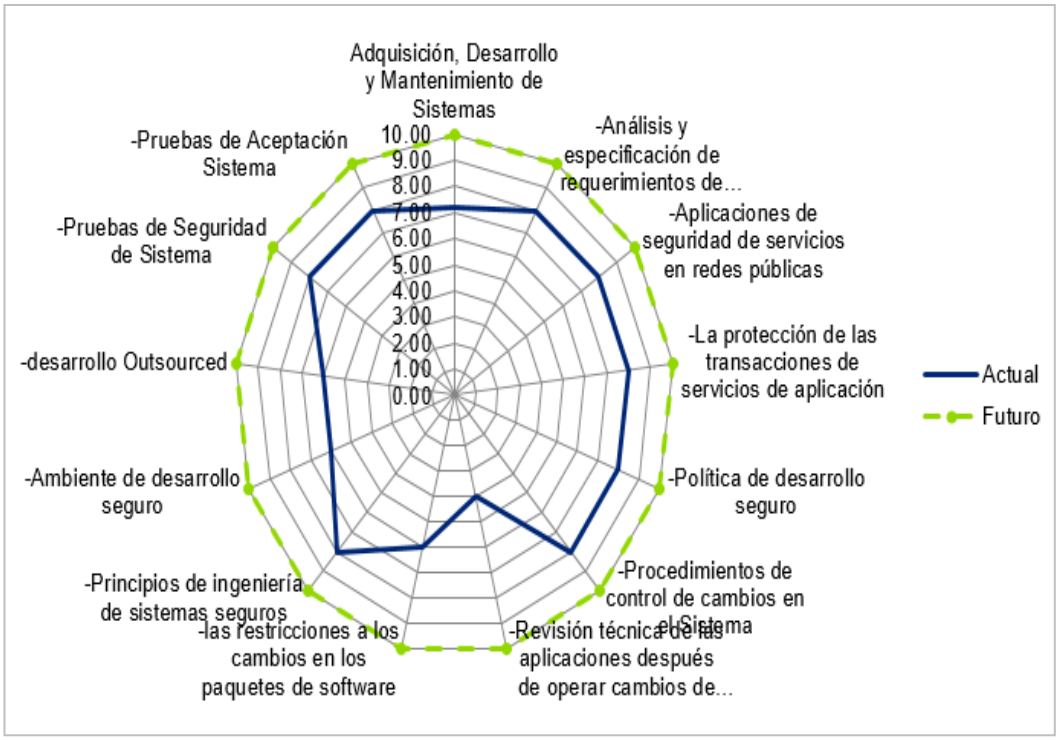
Nivel de madurez logrado en CISC frente al dominio A.5 Seguridad de las Comunicaciones.

Los subdominios evaluados se indican a continuación:

Subdominio	Nombre de Subdominio
5.1.1	Controles red
5.1.2	Seguridad de los servicios de red
5.1.3	Segregación en las redes
5.2.1	Políticas y procedimientos de transferencia de información
5.2.2	Acuerdos sobre la transferencias información
5.2.3	Mensajería electrónica
5.2.4	Confidencialidad o acuerdos de no divulgación

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

De acuerdo a la revisión y el nivel de madurez en el que se encuentra CISC, con respecto al dominio A.6 Adquisición, Desarrollo y Mantenimiento de Sistemas, los subdominios se encuentran en un Nivel de Madurez: **7 - Definido.**



Nivel de madurez logrado en CISC frente al dominio A.6 Adquisición, Desarrollo y Mantenimiento de Sistemas

Los subdominios evaluados se indican a continuación:

Subdominio	Nombre de Subdominio
6.1.1	Análisis y especificación de requerimientos de Seguridad de la información
6.1.2	Aplicaciones de seguridad de servicios en redes públicas
6.1.3	La protección de las transacciones de servicios de aplicación
6.2.1	Política de desarrollo seguro
6.2.2	Procedimientos de control de cambios en el Sistema
6.2.3	Revisión técnica de las aplicaciones después de operar cambios de plataforma
6.2.4	Restricciones a los cambios en los paquetes de software
6.2.5	Principios de ingeniería de sistemas seguros
6.2.6	Ambiente de desarrollo seguro
6.2.7	Externalización del desarrollo de software.
6.2.8	Pruebas de Seguridad de Sistema
6.2.9	Pruebas de Aceptación Sistema

5. Planes y recomendación de acción para mejoras

Para el presente informe se han establecido las principales iniciativas a ejecutar por parte de CISC respecto a la definición e implementación de controles.

Se agruparon aquellos controles que tenían un enfoque de aplicabilidad común para determinar iniciativas macro. Las iniciativas de agrupación son:

#	Iniciativas
1	Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, entre otros)
2	Implantación de controles
3	Aplicación de enfoques de mejora continua

A continuación se describen cada una de las iniciativas:

Iniciativa 1
Nombre de Iniciativa:
Definición, formalización y aprobación del marco normativo de seguridad de la información (políticas, procedimientos, reglamentos, manuales, etc.)
Objetivo:
Establecer un marco normativo mediante la definición de políticas, procedimientos, reglamentos y otra documentación normativa, que permita implantar los controles en CISC con base en los controles descritos en la Norma ISO/IEC 27001.
Principales actividades:
– Identificar el marco normativo necesario para dar cumplimiento a lo solicitado por la Norma ISO/IEC 27001. – Confirmar los documentos que formarán parte del marco normativo y que serán desarrollados como parte del proyecto y desarrollar aquellos que aún estén pendientes. – Formalizar, aprobar y socializar los documentos del marco normativo con las áreas impactadas. – Incorporar dichos documentos del marco normativo a un esquema de mejora continua que permita asegurar su correcto mantenimiento, revisión y actualización.

Iniciativa 2
Nombre de Iniciativa:
Implantación de controles
Objetivo:
Poner en ejecución los controles documentados en la iniciativa 1 en caso de no estar en operación, considerando los lineamientos dados en dichos documentos. Establecer un período de estabilización para corroborar que dichos controles están operando tal como fueron diseñados.

Iniciativa 2
Principales actividades:
– Implantar los controles documentados en el marco normativo. – Socializar con los impactados el funcionamiento de los controles, y la evidencia que se requiere generar producto de su ejecución. – Establecer un período de estabilización para los controles implantados y dar seguimiento con el fin de determinar que estén operando acorde a cómo fueron diseñados. – Actualizar la documentación para que refleje la realidad de operación de los controles. – Monitorear en conjunto con las áreas responsables la ejecución de dichos controles para asegurar su pertinencia.

Iniciativa 3
Nombre de Iniciativa:
Aplicación de enfoques de mejora continua
Objetivo:
Monitorear y medir el cumplimiento de los procesos y la efectividad de los controles implementados, establecidos en las iniciativas 1 y 2 respectivamente; mediante la implementación de métricas e indicadores, con el fin de establecer acciones de mejoramiento continuo.
Principales actividades:
– Definir y establecer procedimientos de monitoreo de los documentos establecidos en el marco normativo y los controles implementados. – Realizar revisiones regulares de los procedimientos y la efectividad de controles implementados, considerando los resultados de los monitoreos efectuados. – Comunicar los resultados de las revisiones a las personas o áreas involucradas. – Establecer acciones de mejora tanto preventiva como correctiva. Estas acciones incluyen la actualización o redefinición de procedimientos y automatización de controles.