UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE INGENIERÍA

GESTIÓN DE CLAVES Y CONTROL DE ACCESO A UN SISTEMA WEB EDUCATIVO BASADA EN LA NORMA ISO/IEC 27001:2005

REPORTE DE APLICACIÓN DE CONOCIMIENTOS

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

PRESENTA:
ESTEFANIA ARRIAGA ROSADO

ASESOR:
DRA. VIANNEY MUÑOZ JIMÉNEZ

TOLUCA, ESTADO DE MÉXICO, SEPTIEMBRE DE 2016

UAEM | Universidad Autónoma del Estado de México

DEPTO. DE EVALUACIÓN PROFESIONAL
No. Oficio: 0042/2016
Ciudad Universitaria, Toluca, Méx. a 13 de septiembre del 2016

C. ESTEFANÍA ARRIAGA ROSADO
PASANTE DE INGENIERÍA EN COMPUTACIÓN
P R E S E N T E

En respuesta a su solicitud, a continuación transcribo el tema aprobado por esta Dirección, que propuso la ***DRA. VIANNEY MUÑOZ JIMÉNEZ*** con el fin de que lo desarrolle en la modalidad de ***REPORTE DE APLICACIÓN DE CONOCIMIENTOS*** le informo que se autoriza la ***impresión de su trabajo*** para presentar su Evaluación Profesional.

"GESTIÓN DE CLAVES Y CONTROL DE ACCESO A UN SISTEMA WEB EDUCATIVO BASADA EN LA NORMA ISO/IEC 27001:2005".

Ruego a usted tomar nota de que en cumplimiento a lo especificado por la Ley de Profesiones, deberá prestar Servicio Social durante un tiempo mínimo de seis meses, como requisito indispensable para sustentar su Evaluación Profesional.

Así mismo, para la elaboración del ***REPORTE DE APLICACIÓN DE CONOCIMIENTOS y*** demás trámites, deberá sujetarse a la reglamentación respectiva de esta Universidad.

A T E N T A M E N T E
PATRIA, CIENCIA Y TRABAJO
"2016, Año del Aniversario de la Universidad Autónoma del Estado de México"
"2016 Año de Leopoldo Flores Valdés"

ESTADOS UNIDOS MEXICANOS · UNIVERSIDAD AUTÓNOMA · PATRIA, CIENCIA Y TRABAJO · ESTADO DE MÉXICO

FACULTAD DE INGENIERÍA
U. A. E. M.

M. EN I. RAÚL VERA NOGUEZ
DIRECTOR

**/Saha.☺

EMS
Enterprise Management Service

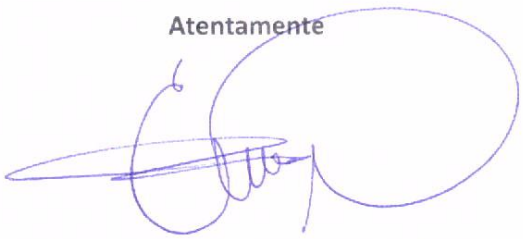
Ciudad de México, a 11 de agosto de 2016

A QUIEN CORRESPONDA:

Por medio de la presente se hace constar que la empresa **Enterprise Management Service, S.A. de C.V.** deslinda de toda responsabilidad a **Estefanía Arriaga Rosado**, así como a la **Facultad de Ingeniería** de la **Universidad Autónoma del Estado de México** (UAEMex), de mostrar información confidencial en su trabajo de titulación " **GESTIÓN DE CLAVES Y CONTROL DE ACCESO A UN SISTEMA WEB EDUCATIVO BASADA EN LA NORMA ISO/IEC 27001:2005**", generado como producto de investigación de su participación como becario en el proyecto **Espacio Digital para el Aprendizaje Autónomo: MetaSpace etapa 2**.

Habiendo previamente revisado el trabajo de titulación y aceptado que el contenido no compromete información confidencial, se extiende este documento a los 11 días del mes de agosto del 2016.

Atentamente



Lic. Ernesto Javier Padilla Calderón

Gerente de Proyectos de Educación a Distancia

Enterprise Management Service, S.A de C.V.
Av. Santa Fe No. 481 Piso 8
Col. Cruz Manca, C.P. 05349
Cuajimalpa, Ciudad de México

Conm. (01 55) 5980 2950
Fax. (01 55) 5980 2982

CARTA DE CESIÓN DE DERECHOS DE AUTOR

El que suscribe Estefania Arriaga Rosado Autor(es) del trabajo escrito de evaluación profesional en la opción de RAC con el título Gestión de claves y control de acceso a un sistema web educativo basado en la norma ISO/IEC 27001:2005 por medio de la presente con fundamento en lo dispuesto en los artículos 5, 18, 24, 25, 27, 30, 32 y 148 de la Ley Federal de Derechos de Autor, así como los artículos 35 y 36 fracción II de la Ley de la Universidad Autónoma del Estado de México; manifiesto mi autoría y originalidad de la obra mencionada que se presentó en la Facultad de Ingeniería (lugar) _____ para ser evaluada con el fin de obtener el Título Profesional de Ingeniero en Computación.

Así mismo expreso mi conformidad de ceder los derechos de reproducción, difusión y circulación de esta obra, en forma NO EXCLUSIVA, a la Universidad Autónoma del Estado de México; se podrá realizar a nivel nacional e internacional, de manera parcial o total a través de cualquier medio de información que sea susceptible para ello, en una o varias ocasiones, así como en cualquier soporte documental, todo ello siempre y cuando sus fines sean académicos, humanísticos, tecnológicos, históricos, artísticos, sociales, científicos u otra manifestación de la cultura.

Entendiendo que dicha cesión no genera obligación alguna para la Universidad Autónoma del Estado de México y que podrá o no ejercer los derechos cedidos.

Por lo que el autor da su consentimiento para la publicación de su trabajo escrito de evaluación profesional.

a) Texto completo. ☒
b) Por capítulos. ☐
c) Solamente portada y tabla de contenido. ☐

Se firma presente en la ciudad de Toluca De Lerdo, a los 19 días del mes de Septiembre de 2016

Estefania Arriaga Rosado

Nombre y firma de conformidad

Agradecimientos

Agradezco a mis padres, María Teresa Rosado Hidalgo y Oscar Guillermo Arriaga Rosales, por el apoyo constante que me brindaron desde el momento de mi nacimiento hasta este importante momento, que es el de desarrollarme profesionalmente. Sin duda, no lo hubiera logrado y les demostraré que su inversión no será en vano, utilizando mis conocimientos con ética y moral.

Quiero agradecer a Adrián Terrón Díaz que estuvo conmigo desde el inicio de la carrera de ingeniería en computación hasta el final, con su constante apoyo intrínseco.

Quiero agradecer a todos los profesores que se preocuparon desinteresadamente por mi aprendizaje y me enseñaron, no solo sobre conocimientos en computación, si no que aportaron lecciones de vida que me serán útiles a lo largo del trayecto.

Por último quiero agradecer a amigos y colegas que trabajaron conmigo a lo largo de la carrera y durante el proyecto.

Resumen

En este documento se reporta el trabajo realizado dentro de un proyecto de desarrollo de software Educativo a nivel básico, medio superior, superior y corporativo, en el cual colaboró la Facultad de Ingeniería de la Universidad Autónoma del Estado de México y una organización del sector privado con registro CONACYT PEI4-220949.

El sistema web educativo es de carácter multidisciplinario, es decir, su desarrollo involucró a profesionales como diseñadores gráficos, especialistas en pedagogía e ingenieros en sistemas computacionales. El desarrollo del sistema web educativo se realizó en dos etapas, en la primera etapa se diseñaron e implementaron los perfiles correspondientes a la educación básica. En su segunda etapa, se implementaron los perfiles correspondientes a la educación media superior, educación superior y nivel corporativo.

En los últimos años, la tecnología ha evolucionado considerablemente, en donde nosotros como usuarios, deseamos que nuestros dispositivos y nuestra información estén vinculados entre sí y disponible en cualquier momento para ser consultada o utilizada a través de los diversos medios de comunicación vía internet. Sin embargo, tanto los usuarios como los desarrolladores y diseñadores de la tecnología no consideran como un rubro importante la implementación de la seguridad de la información. Gran parte de la información considerada *importante* está a la vista de atacantes, quienes esperan que se presente la oportunidad mínima para obtener la información de usuarios y de las empresas, haciendo uso de ella de forma indebida y delictiva.

Con el avance de la tecnología, se han desarrollado normas y metodologías para la seguridad de la información, como es el caso de la norma ISO/IEC 27001:2005 quien permite a los desarrolladores y empresas, analizar e implementar un *Sistema de Gestión de Seguridad de la Información* conocido por sus siglas SGSI, con la finalidad de proteger los activos o información que se consideren de gran valor en función del costo que podría representar su daño o pérdida. La información es considerada como el recurso más valioso de una empresa y del propio

usuario, es por ello la necesidad de que sea protegida de cualquier atacante para evitar el mal uso de está.

En el presente reporte de aplicación de conocimientos, se describen los conceptos básicos y mínimos requeridos para mantener la seguridad de la información. Se presentan las normas y metodologías de seguridad de información que son empleadas para la implementación de mecanismos y controles de seguridad en un sistema web, tomado como caso de estudio un sistema web educativo a nivel básico, medio superior, superior y corporativo. Además, se detallan las actividades que se realizaron durante el desarrollo del proyecto para la implementación de controles de seguridad para un sistema web educativo previamente diseñado y desarrollado por programadores pertenecientes al mismo proyecto y bajo la premisa de no afectar la funcionalidad del sistema web, empleando la menor cantidad de recursos posibles. Cumpliendo así el rol que desempeñé dentro del proyecto que se enfocó en la implementación de la seguridad en el sistema web educativo.

El proyecto inició en el mes de abril de 2015 y finalizó en el mes de marzo de 2016.

Tabla de contenido

Índice de Figuras

Índice de Tablas

Introducción

La seguridad informática es un tema de gran importancia a nivel nacional e internacional, es un proceso evolutivo que representa una ventaja competitiva sobre las diferentes empresas que ofertan los mismos servicios y productos en el mercado. La seguridad informática brinda un estado de confort a los usuarios de un sistema, al proporcionarles índices aceptables de seguridad, garantizando que su información y propiedad estén a salvo de amenazas e intrusos que de forma ilícita, ya sea, intencionada o accidental hagan un mal uso de los datos.

Es importante implementar los mecanismos necesarios para la seguridad informática de un sistema de información, ya que sin este pueden existir pérdidas monetarias y en algunos casos hasta problemas legales. Si la empresa no proporciona un correcto Sistema de Gestión de Seguridad de la Información (SGSI) puede ser víctima de delitos informáticos, donde el objetivo de los criminales informáticos es hacer uso de la información y otros recursos para obtener un beneficio propio, que en general perjudica a la empresa y su imagen, pero sobre todo y en diferentes medidas a los usuarios.

Los SGSI protegen los procesos del sistema contra incidentes de seguridad de la información que comprometen la integridad y autenticidad de la información. En resumen, proteger los activos de la empresa es una estrategia para ayudar a las empresas u organizaciones a cumplir con sus objetivos e impulsar sus ganancias.

Objetivo General

Documentar la implementación, análisis y diseño de un sistema de seguridad de la información, apoyándose en la norma ISO/IEC 27001:2005 para un sistema web educativo.

Alcance y limitaciones

Los controles y mecanismos de seguridad de la información que se analizaron e implementaron en este reporte de aplicación de conocimiento se limitan a las mejores prácticas y guías de las normas ISO/IEC 27001. La seguridad implementada para el sistema web educativo es exclusivamente a nivel de software. Los controles de seguridad que se implementaron fueron elegidos con respecto al avance del desarrollo del sistema web educativo, con el objetivo de no afectar la funcionalidad del sistema.

Es necesario realizar periódicamente un análisis de riesgos con respecto a la seguridad de la información en el sistema web educativo, para detectar o prevenir las nuevas amenazas que pudieran presentarse en el sistema. Se debe remarcar que sí la empresa no establece roles y políticas de seguridad debidamente definidos, los controles implementados por muy buenos que sean no servirán del todo, debido a que la principal vulnerabilidad del sistema web educativo es el propio usuario. De ahí, la importancia de capacitar al usuario para que no proporcione información personal como claves y contraseñas a personas ajenas, ya que estas pueden hacer mal uso de la información perjudicando la vulnerabilidad del sistema.

Por cuestiones de confidencialidad, en este reporte de aplicación de conocimiento no se incluye ninguna imagen, diagrama o parte del código que se elaboró para el desarrollo e implementación del software web educativo, ya que la empresa encargada de la construcción de éste así lo requirió con el fin de proteger los derechos de autor del sistema.

Organización del documento

Este reporte de aplicación de conocimiento está organizado de la siguiente manera:

En el Capítulo 1- *Antecedentes y planteamiento del problema:* se describe los fundamentos, las propiedades y controles de la seguridad de la información, así como las amenazas y ataques frecuentes a la misma. Se presenta la norma ISO/IEC 27001:2005, la cual nos permite presentar una propuesta para implementar las mejores prácticas de un Sistema de Gestión de la Seguridad de la Información (SGSI).

En el capítulo 2 – *Informe de actividades*: se presenta el informe de las actividades realizadas durante el periodo del desarrollo del proyecto con relación a la seguridad de la información. Se describe el análisis de riesgo y la estimación de impacto y probabilidad de riesgo al mantener esos riesgos. En este capítulo se describe la propuesta planteada para reducir el riesgo en incidentes relacionados con la seguridad de la información del sistema web educativo.

En el capítulo 3 – *Resultados*: se presenta los resultados obtenidos de las pruebas realizadas al sistema web educativo para determinar el comportamiento de los controles de seguridad de la información implementados en el sistema. Se discuten los resultados obtenidos al evaluar las propiedades de seguridad de la información antes y después de haberse implementado dichos controles de seguridad.

Finalmente, en la sección de *Conclusiones:* se presentan las conclusiones obtenidas del trabajo realizado y del proyecto con respecto al tema de seguridad de la información en el sistema web educativo.

Capítulo 1 Antecedentes y planteamiento del problema

En este capítulo se describen los antecedentes, fundamentos y definiciones relacionados al tema de seguridad de la información de un sistema web.

1.1 Fundamentos de la seguridad de la información

En la actualidad, la seguridad de la información se considera de suma importancia y es relevante invertir recursos para implementarla debido al creciente valor estratégico de la información. Entender y comprender los fundamentos de la seguridad de la información nos permite conocer e implementar controles de seguridad de la información apropiadas a las características y requerimientos de la empresa. En los párrafos siguientes, se describen los conceptos básicos de seguridad de la información utilizados a lo largo del desarrollo de este reporte de aplicación de conocimiento:

1) Seguridad informática
2) Análisis de riesgos
3) Eventos en la seguridad de la información
4) Incidente en la seguridad de la información

La *seguridad informática***,** se define como la preservación de la confidencialidad, integridad y disponibilidad de la información; en está, pueden estar involucrados otras propiedades como autenticidad, no repudio y confiabilidad [1]. El objetivo principal de la seguridad informática es proteger los activos (información) de la empresa u organización.

Un *activo*, se define como cualquier elemento que tenga valor para la organización. En particular, la *información* es un activo importante que debe ser salvaguardada [1].

El *análisis de riesgos*, es un estudio que sirve para determinar el impacto y el riesgo que se obtendría al presentarse un incidente en la seguridad de la información [2]. En el análisis de riesgo se determina:

- a) los activos relevantes a la empresa, su valor e impacto
- b) las amenazas a las que están expuestos los activos
- c) los controles con los cuales se pueden proteger los activos y,
- d) la estimación del impacto o costo que se tendría por el daño o pérdida de estos activos.

Un *evento en la seguridad de la información*, es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información que puede ser relevante para la seguridad del sistema [1].

Finalmente, un *incidente en la seguridad*, consiste en una serie de eventos de seguridad de la información no deseados o inesperados, quienes podrían comprometer las operaciones comerciales y amenazan la seguridad de la información [1].

1.2 Análisis de Riesgos de la Seguridad del sistema web educativo

Durante el análisis de riesgo de la seguridad de la información en el sistema web educativo se determinan las vulnerabilidades que este puede presentar, se calcula el daño que podría causar si una de esas vulnerabilidades es explotada por una amenaza. De esta manera, la empresa debe priorizar los riesgos e implementar los controles de seguridad necesarios para proteger su información.

El análisis de riesgos debe realizarse frecuentemente, debido a que la tecnología y las amenazas cambian constantemente, así como las necesidades de la empresa y el mercado.

Para el análisis de riesgo la empresa debe elegir un enfoque sistemático, para este trabajo se sugiere que la empresa elija la metodología MAGERIT V3 [2].

MAGERIT es una metodología de análisis y evaluación de riesgos elaborada por el Consejo Superior de Administración Electrónica por el gobierno de España, se compone de tres libros conocidos como método, catálogo de elementos y guía de técnicas. Esta metodología propone cinco pasos para realizar un correcto análisis de riesgos quienes se adaptan satisfactoriamente a este proyecto [2].

Paso 1: Determinar los activos relevantes para la empresa, su inter-relación y su valor proporcional a éste, y la perdida por la degradación del activo.

Paso 2: Determinar a qué amenazas están expuestos los activos que se identificaron y se desean proteger.

Paso 3: Determinar qué controles de seguridad de la información hay disponibles y su eficacia frente a los riesgos.

Paso 4: Estimar el impacto del daño sobre el activo, resultado de la producción de un incidente en la seguridad de la información o de una amenaza.

Paso 5: Estimar el riesgo, definido como el impacto en relación con la probabilidad de que un incidente de seguridad de la información ocurra y se produzca una amenaza.

La Figura 1-1, ilustra cómo se realiza un análisis y evaluación de riesgos en función del valor del activo, las amenazas a los que está expuesto y la probabilidad de incidencia de seguridad de la información.

1.3 Análisis de Riesgos Cualitativo Mediante Tablas

En este análisis, los elementos se ordenan por relevancia. Se realizan por medio de tablas, las cuales se consideran no son precisas, pero aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas [3].

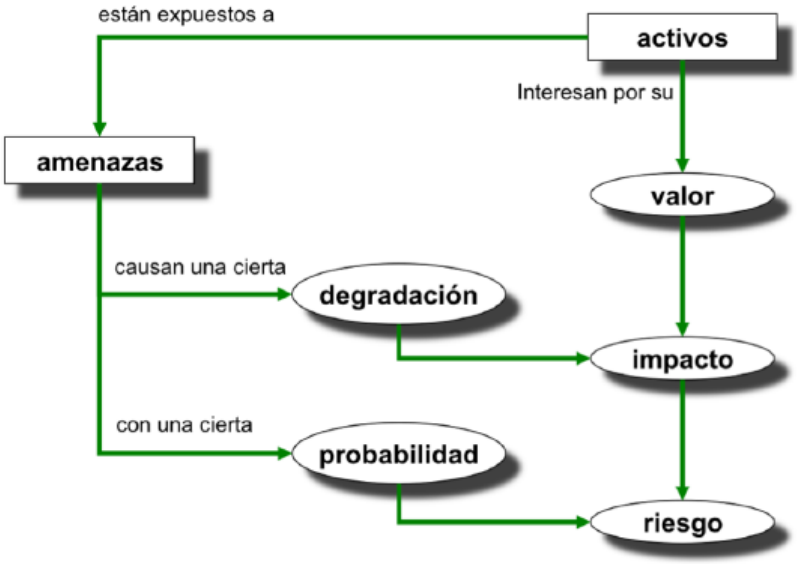


Figura 1-1 Elementos del análisis y evaluación de riesgos

Se puede calcular el *impacto* con base en tablas sencillas de doble entrada, Tabla 1-1 muestra el modelo a utilizar para el cálculo de estimación de impacto [3]:

Tabla 1-1 Tabla para Estimación de Impacto [3]

impacto		***degradación***		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

La Tabla 1-2, muestra la descripción de las escalas utilizadas para evaluación del impacto.

Tabla 1-2 Escala cualitativa para el Cálculo de Riesgo [3]

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Los activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata. El impacto puede combinarse con la frecuencia, tal como se ilustra en la Tabla 1-3 para determinar el riesgo:

Tabla 1-3 Cálculo de Riesgo [3]

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Por otro lado, la norma ISO/IEC TR 13335-3 [4] sugiere otras metodologías de análisis y evaluación de riesgos que la empresa puede elegir, logrando el mismo objetivo con respecto a las necesidades, características y requerimientos de la empresa.

1.4 Propiedades de seguridad de la Información

Una propiedad de la seguridad es mejorar la seguridad de los sistemas de la información y la transferencia de información de una organización. Las

propiedades están diseñadas para contrarrestar los ataques a la seguridad de la información y hacen uso de uno o más mecanismos para proporcionar la propiedad [5]. Las propiedades de la seguridad de la información son los siguientes:

- **Disponibilidad:** La información debe estar disponible y utilizable cuando una entidad autorizada lo requiera. Esto incluye, evitar que la información sea bloqueada [1].
- **Confidencialidad:** La información debe estar disponible y no debe ser divulgada a personas, entidades o procesos no autorizados. Sólo la persona o entidad autorizada pueda entender la información, de esta forma, si es interceptada, los intrusos no podrán entenderla de forma coherente. Esta propiedad se puede lograr mediante el cifrado simétrico y asimétrico. En la sección 1.5 se describen estas formas de cifrado [1].
- **Integridad:** La información se debe salvaguardar con exactitud. Esto es, la información no ha sido alterada y además se debe comprobar que no se ha producido alguna manipulación en la información original. Esto se puede lograr con un diseño de funciones adecuadas, como puede ser el uso de métodos *hash*, que consisten en un algoritmo de cifrado simétrico y permiten comprobar que el contenido no ha sido modificado [1].
- **Autenticidad**: permite identificar la fuente y el generador de la información [1].

Estas propiedades de la información se consideran fundamentales, si alguna falla o falta, se considera que no existe seguridad informática en el sistema.

1.5 Controles de seguridad de la información

Un *mecanismo o control de seguridad* es un mecanismo o control diseñado para detectar un ataque a la seguridad de la información de un sistema, prevenirlo o re-establecerse de él. Algunos controles se describen a continuación [5].

- **Cifrado**: es el uso de algoritmos matemáticos para transformar un conjunto de datos en una salida que solo es coherente para quien esté autorizado. Se utiliza cero o más llaves de cifrado para el cifrado y descifrado de la información.
- **Firma digital:** es un conjunto de datos sometidos a un cifrado que permite al receptor verificar la fuente, autenticidad y la integridad de la información y protegerla de la falsificación o la alteración.
- **Control de acceso:** es una serie de mecanismos o controles de seguridad de la información, que regulan los permisos de acceso a los recursos y la información.
- **Control de enrutamiento:** proporciona rutas físicamente seguras dependiendo del tipo de la información y permite monitorear el tráfico con el objetivo de evitar que atacantes accedan al flujo de la información.

1.6 Amenazas y ataques a la seguridad de la información

Una *amenaza* es una posibilidad de violación de la seguridad, que existe cuando se presenta una vulnerabilidad en el sistema o los recursos de la empresa u organización, que pudiera degradar la seguridad y causar un daño o impacto [5].

Un *ataque* es una degradación a la seguridad del sistema derivado de una amenaza que explota una vulnerabilidad del sistema o los recursos de la empresa u organización; con lo cual se busca evadir y comprometer las propiedades de la seguridad y violar la política de seguridad que aplica para un sistema y los recursos [5].

Los ataques pueden clasificarse en ataques pasivos y ataques activos. Los *ataques pasivos* suceden cuando el atacante tiene acceso a información no autorizada, el atacante busca obtener esta información o analizar en tráfico de información. Estos ataques son los más difíciles de detectar, ya que no implican una alteración en la información, sin embargo, es posible evitarlos mediante el uso de cifrado. Los *ataques activos* implican la fabricación de información falsa o modificación de la información y se dividen en cuatro categorías descritas a continuación [5].

- **Suplantación:** se produce cuando un atacante toma la identidad de una persona autorizada o registrada en el sistema. Con esta operación, el atacante busca adquirir privilegios para consultar y tomar información a la que no está autorizado o manipular los procesos del sistema web.
- **Repetición:** implica capturar información para su posterior retransmisión de forma no autorizada.
- **Modificación:** la información es sometida a una alteración, es retrasada o reorganizada, para afectar la autenticidad e integridad de la información.
- **Interrupción:** impide el uso o la gestión normal de la información; puede tener por objetivo, suprimir la información o sobrecargar de peticiones para lograr un ataque de negación de servicio.

Los ataques pasivos suelen ser difíciles de detectar y mitigar, al no modificarse la información, el emisor y el receptor de la información no detectan este tipo de ataque hasta que la información ha sido robada y generado un daño a la empresa. Para solucionar este problema, se puede implementar protección física en todos los activos y rutas de comunicación. Se debe proteger los procesos y si es posible, encapsularlos para evitar que los usuarios y atacantes los conozcan.

1.7 Tipos de Inyección SQL

La inyección de código SQL se considera una de las vulnerabilidades más importantes en los sistemas web que utilizan bases de datos para almacenar su información y puede ser objeto de una amenaza que genere todos los ataques mencionados en la sección 1.6.

La inyección SQL es la inserción no autorizada de scripts con sentencias SQL válidas, normalmente los atacantes utilizan errores de diseño, de programación y de validación para insertar código SQL y obtener información o afectar la integridad de la base de datos [6].

Las reglas básicas de los diseñadores de la seguridad de la información son: el programador web no debe confiar en los datos que

ingresa el usuario y el programador debe creer que el usuario no respetará la sintaxis de la URL [6].

Con base en las vulnerabilidades que un sistema web presenta, se agrupan los tipos de inyección SQL como los siguientes.

- Cadenas mal filtradas
- Incorrecta manipulación de tipo
- Blind SQL injection

Las cadenas mal filtradas, se refieren a las cadenas de datos no analizadas que los usuarios ingresan o modifican, y que se interpretan como instrucciones SQL. Estas cadenas son visibles en formularios, en los parámetros utilizados en funciones javascript, en los valores de HTTP o datos almacenados de cookies [7], estas cadenas generan ataques del tipo modificación.

La incorrecta manipulación de tipo, se refiere a los datos que no están validados en tipo, longitud y formato. El ingreso a la base de datos no validados puede incurrir en la integridad de la base de datos o generar un estado de error en el sistema [7].

La blind SQL injection, se basa en ataques a ciegas, es decir, el atacante ingresa instrucciones y caracteres reconocidos como operadores en SQL, esperando afectar la base de datos o al sistema web [7].

1.8 Análisis de riesgo del Sistema Web Educativo

Una de las vulnerabilidades que se presentaron tanto en la etapa uno como en la etapa dos sistemas web educativos, fue el uso de los campos de usuario y contraseña, quienes permitían insertar sentencias de SQL válidas que el gestor de base de datos ejecutaba y realizaba la acción solicitada. La Figura 1-1 muestra un ejemplo de la pantalla de usuario y contraseña, este corresponde a un sistema web elegido al azar, debido a que el sistema web educativo es de carácter confidencial. En esta Figura 1-1 se indica la parte vulnerable del sistema que corresponde a la caja de texto de usuario (usuario:) o en la caja de texto de contraseña (password:).

Figura 1-2 Contraseña con vulnerabilidad SQL [6]

En la caja de texto del usuario y contraseña se ingresan caracteres válidos de SQL o palabras reservadas de SQL, si no se tienen los controles de seguridad de la información adecuados para evitar este incidente en la seguridad de la información, el sistema entra en un estado de error, no permitiendo el flujo normal de la información. En el peor de los casos, se provoca la modificación, el borrado de la información o el esquema de la base de datos y el acceso no autorizado al Sistema Web Educativo.

Algunos controles de seguridad de la información que se pueden utilizar para evitar esta vulnerabilidad son las validaciones de las entradas de los usuarios, limitar el tipo y número de palabras recibidas por el usuario, entre otras.

Figura 1-3 Contraseña con vulnerabilidad SQL [6]

Otra vulnerabilidad detectada en el sistema web educativo, es el campo de la URL. Mediante la URL se escribe palabras reservadas del lenguaje SQL o cualquier carácter que reconozca el gestor como sentencia válida. La Figura 1-4 ilustrar el lugar donde se puede llevar a cabo el ataque, cabe resaltar que es la pantalla de un sistema web al azar.

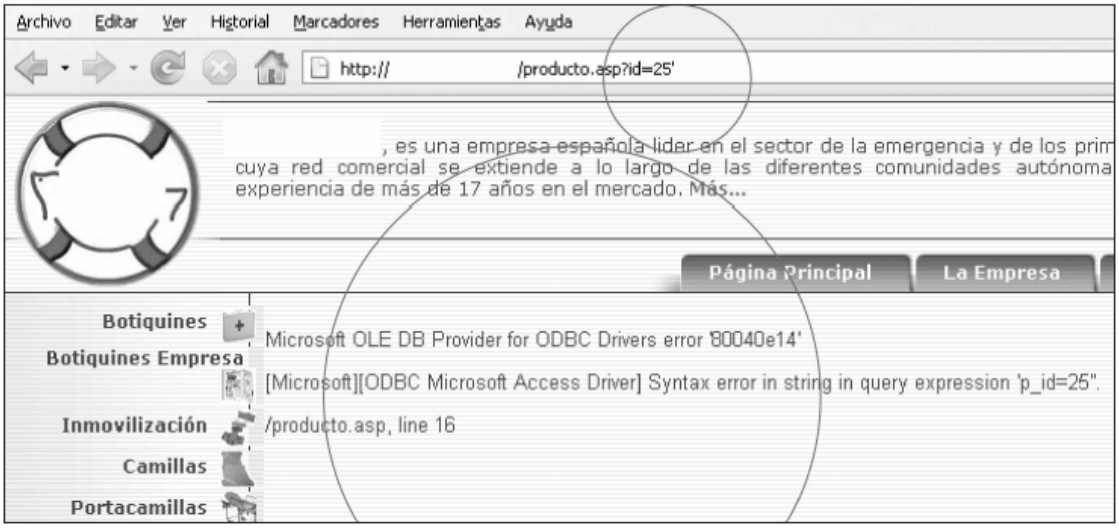


Figura 1-4 Vulnerabilidad inyección SQL en la URL [6]

Como se puede observar en Figura 1-4, se puede ingresar comillas o cualquier palabra reservada del lenguaje SQL y se puede alterar, borrar o consultar información de la base de datos. Por otro lado, se puede generar un error en la base de datos y por consecuencia en el sistema. Los controles que se pueden aplicar para disminuir la probabilidad de ataque por inyección SQL, es filtrar las URL del Sistema Web y negar todas las peticiones de usuario con palabras reservadas y caracteres reconocidos como operadores de SQL.

La inyección SQL se puede evitar considerando los siguientes puntos.

- Validación de entrada de datos de usuario: agregar validaciones a todas las entradas de los usuarios, esto es, limitar la longitud, tipo (sea numérico, alfanumérico, fecha, etc.) y formato de los datos (sea un patrón o expresión regular que modele las entradas de datos). Un atacante esperará que el sistema no tenga validaciones de entrada de datos de usuario y buscará ingresar datos con un formato no autorizado o una longitud que sobrepase a la especificada en la base de datos, con lo cual, el sistema entrará en un estado de error [8].

- Filtrar la entrada de datos: independientemente de la fuente de donde se generen los datos hacia la base de datos, se debe filtrar eliminando caracteres indeseados y palabras reservadas de los lenguajes utilizados y reconocidos por el sistema y servidor web [8].

1.9 Descripción de la norma ISO/IEC 27001:2005

La norma ISO/IEC 27001:2005 es un estándar internacional que ha sido preparado para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) [1].

Este estándar internacional recomienda utilizar y adoptar un enfoque del proceso. El enfoque del proceso para la gestión de la seguridad de la información que recomienda este estándar internacional, permite que los usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles de seguridad de la información para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño y la efectividad del SGSI.
- Mejoramiento continuo con base en la medición del objetivo, las características de la empresa y los recursos con los que cuenta.

Este estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La Figura 1-5 muestra el modelo que el estándar acepta, recomienda y adopta.

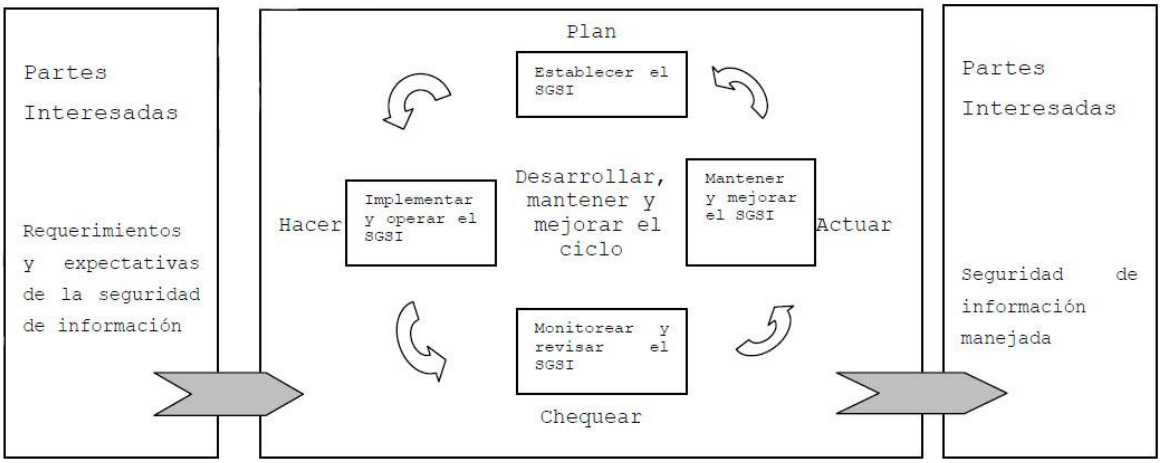


Figura 1-5 Modelo PCDA [1]

1.10 Sistema de Gestión de la Seguridad de la Información

Para una correcta gestión de la seguridad en la información, la norma ISO/IEC 27001:2005 sugiere implementar un Sistema de Gestión de Seguridad de la Información SGSI como parte del sistema gerencial, basado en un enfoque de tratamiento de riesgos. Se puede componer de normas, políticas, planeación, prácticas, procedimientos y recursos. Cabe recalcar que la implementación de un SGSI es decisión de la alta gerencia, esta debe decidir el alcance y los objetivos para implementarlo [1].

Un SGSI se compone de las siguientes partes, las cuales son descritas a continuación y se muestra el diagrama en la Figura 1-5:

- Establecer el SGSI
- Implementar y operar el SGSI
- Monitorear y revisar el SGSI
- Mantener y mejorar el SGSI.

Establecer el SGSI: en esta parte se definen el alcance y los límites del SGSI, dependiendo de las características de negocio, organización, almacenamiento de la información y la tecnología que se ocupa en la organización o empresa [1].

- Se definen políticas para el SGSI; esto incluye marco referencial; requerimientos legales, comerciales y obligaciones de seguridad contractual.
- Se define el enfoque de evaluación de riesgo de la organización.
- Se analizan y se evalúan los riesgos.
- Se identifican y evalúan las opciones para el tratamiento de riesgos.
- Se seleccionan los controles para el tratamiento de riesgos.
- Por último, la gerencia debe aceptar el SGSI para su posterior implementación.

Implementar y operar el SGSI: en esta parte se diseñan y analizan los controles de seguridad de la información para el tratamiento de riesgos [1].

- Se formula un plan de tratamiento de riesgos que decida la gerencia para manejar los riesgos de seguridad de la información.
- Se implementa el plan de tratamiento de riesgos para lograr los objetivos que se establecieron con respecto al SGSI en proceso.
- Se implementan los controles seleccionados que se establecieron y que satisfagan los objetivos establecidos en el SGSI en proceso.
- Se define cómo se medirá la eficacia de los controles establecidos para producir resultados comparables y reproducibles.
- Se implementan los programas de capacitación.
- Se manejan las operaciones y recursos del SGSI.
- Se implementan controles adicionales para el manejo de incidentes en la seguridad de la información.

Monitorear y revisar el SGSI: en esta parte se prueban los controles de seguridad de la información implementados. Se detectan fallos en los controles y procedimientos implementados y se detectan otros incidentes en la seguridad [1].

- Se deben ejecutar procedimientos de monitoreo y revisión.
- Se deben realizar revisiones periódicas de la efectividad del SGSI en donde se puede comprobar los resultados de revisiones y auditorias anteriores.
- Medir la efectividad de los controles establecidos y que se haya cumplido con los objetivos establecidos en el SGSI en proceso.
- Actualizar el análisis de riesgos de la seguridad de la información.
- Realizar auditorías internas al SGSI. También se puede recurrir a entidades externas para una auditoría más objetiva y directa.
- Actualizar los planes de seguridad de la información.
- Se deben registrar las acciones y eventos que impacten al SGSI y la información.

Mantener y mejorar el SGSI: En esta parte se implementan las mejoras al SGSI que se identificaron de acuerdo a los resultados que se obtuvieron de las auditorías internas, externas y el monitoreo del SGSI [1].

- Se implementan las mejoras identificadas en el SGSI.
- Se toman las acciones correctivas y preventivas adecuadas.
- Se comunican los cambios a las partes interesadas con el detalle apropiado para que los comprendan.
- Se asegura que las mejoras logren sus objetivos señalados y satisfagan los requerimientos en la seguridad de la información definidos por las partes interesadas o la alta gerencia.

Basado en las mejores prácticas y los controles de la seguridad propuestos en la norma ISO/IEC 27001:2005 para la implementación de un SGSI, se acordó para este reporte de aplicación de conocimientos, la implementación de algunos controles de la seguridad de la información para satisfacer los requerimientos de las partes interesadas, y así proteger el sistema web educativo, logrando, además, una mayor calidad en el producto final.

Capítulo 2 . Implementación de un Sistema de Seguridad para el Sistema Web Educativo

En este capítulo, se describe las actividades desarrolladas a lo largo del proyecto y que competen al tema de seguridad de la información. El rol de las partes interesadas en la seguridad de la información lo desempeña el grupo de desarrolladores del sistema web, quienes establecieron los requerimientos mínimos para la seguridad de la información tomando en cuenta el alcance y las limitaciones de sus recursos y las características de la empresa.

2.1 Justificación de Herramientas Utilizadas

Las normas y metodologías MAGERIT [2], ISO 27001:2005 [1] e ISO 17799 [4]; utilizadas para la realización de las actividades con respecto a la seguridad de la información, se eligieron debido a que son de libre acceso, es decir, la documentación requerida se puede encontrar en internet u otros medios y se puede utilizar sin ninguna restricción o pago de alguna licencia para su uso e implementación. Existen otras como COBIT pero que no son de libre acceso y la documentación adquiere un costo.

2.2 Estimación de riesgos Cualitativo

Basado en el análisis de riesgo cualitativo, mediante tablas del libro tres de MAGERIT [3], que determina cómo se debe realizar un análisis de riesgos, las características de la empresa y los recursos de las partes interesadas, se identificó los activos relevantes, se determinó el valor de cada activo y se calculó su degradación con relación a su valor y el impacto o perdida que representa para la empresa debido a un ataque resultado de un incidente en la seguridad de la información. Con este análisis, se determinó los requerimientos de seguridad de la información. La escala,

sugerida por el libro tres de MAGERIT [3], utilizada fue la presentada en la sección 1.2:

La Tabla 2-1 muestra los indicadores obtenidos, se agregó la columna justificación para determinar el valor y la degradación del activo, note que la justificación indica el impacto o perdida que se tendría por un ataque dirigido a cada activo y que se utilizó para decidir la ponderación de la degradación del activo.

Tabla 2-1 Estimación de impacto

Número	Activo	Valor	Degradación	Impacto	Justificación
1	Claves de usuario y sistema	A	100%	A	El programa podría mostrar información no autorizada o entrar en estado de error.
2	Estructura de base de datos	MA	100%	MA	Se podría modificar la estructura de la base de datos degradando todas las propiedades de la seguridad de la información.
3	Información de la base de datos	A	10%	M	La integridad y disponibilidad de la información se podría afectar.
4	Módulos del sistema web educativo	A	10%	M	La disponibilidad podría verse afectada.
5	Usuarios del sistema web educativo	A	10%	M	Las leyes gubernamentales exigen proteger y utilizar los datos personales de forma controlada.
6	Tecnología donde se montará la aplicación y base de datos	B	1%	MB	Se dejó fuera la infraestructura donde se montará la aplicación y la base de datos debido a falta de recursos.
7	Instalaciones que alojarán	B	1%	MB	Se dejó fuera las instalaciones donde

Número	Activo	Valor	Degradación	Impacto	Justificación
	la tecnología.				se montará la aplicación y la base de datos debido a falta de recursos.

Basado en la guía técnica del libro tres de MAGERIT [3] y el resultado de las pruebas de funcionalidad de las partes interesadas, se calculó el riesgo y la probabilidad de ocurrir un incidente en la seguridad de la información.

La probabilidad se determina por medio de la exposición o disponibilidad de las vulnerabilidades a los atacantes o usuarios, en este caso; la URL, el Login de usuario y las cajas de texto, son accesibles por cualquier usuario o atacante; por lo que aumenta considerablemente la probabilidad de incidencias en la seguridad de la información. Con esta ponderación se determinó el tipo de control de la seguridad de la información y la prioridad con la que debían ser implementados al sistema web educativo.

La Tabla 2-2 muestra los resultados obtenidos. El riesgo se determina de la relación entre la degradación del activo y la probabilidad de que un incidente en la seguridad de la información se ejecute por cada activo identificado.

Tabla 2-2 Estimación de Riesgo

No. Activo	Impacto	Probabilidad	Riesgo
1	A	MA	MA
2	MA	MA	MA
3	M	MA	A
4	M	A	A
5	M	M	M
6	MB	B	MB
7	MB	B	MB

Con base en la Tabla 2-1 y la Tabla 2-2, se determinó el valor de las propiedades de la seguridad que corresponden al sistema web educativo, basados en la siguiente Tabla 2-3 que muestra la escala y el promedio de los valores asignados.

Tabla 2-3 Escala para valoración de propiedades de Seguridad

Indicador	Ponderación	Descripción
MB	10	Muy bajo: Propiedad con probabilidad de riesgo muy baja
B	8	Bajo: Propiedad con probabilidad de riesgo baja
M	6	Medio: Propiedad con probabilidad de riesgo media
A	4	Alto: Propiedad con probabilidad de riesgo muy alta
MA	2	Muy Alto: Propiedad con probabilidad de riesgo muy alta

La Tabla 2-4 muestra la ponderación de las propiedades de la seguridad de la información basándose en la Tabla 2-3, definida mediante el promedio de los valores obtenidos del análisis de riegos obtenido. En escala de 1 a 10, siendo 10 un valor satisfactorio, se determinó que los valores encontrados para las propiedades de la seguridad de la información eran deficientes para el sistema web educativo.

Tabla 2-4 Ponderación de Propiedades de Seguridad

Propiedad	Ponderación
Disponibilidad	5
Confidencialidad	5
Integridad	5
Autenticidad	5

2.3 Análisis de Soluciones de la Seguridad de la Información

Una vez determinada la estimación de riesgos y la estimación de impacto de los activos de la información identificados por las partes interesadas, se propuso los siguientes controles para satisfacer los requerimientos en la seguridad de la información:

- Cambiar los métodos que se usan para enviar la información. En este caso se considera el método Post.
- Utilizar variables de sesión que no son visibles para el usuario y se utilizan únicamente en el servidor.

Las soluciones mencionadas anteriormente permiten tener mayor manejo de la seguridad de la información en el sistema web educativo, sin embargo, podían impactar en el funcionamiento del sistema, debido a la modificación del código que representaba una mayor inversión de tiempo en pruebas exhaustivas para determinar que el sistema funcionara correctamente con estas modificaciones y que ya se había realizado las pruebas correspondientes.

Por las razones anteriormente expuestas, estos controles de seguridad no se implementaron ya que fueron rechazadas por el equipo de desarrollo y las partes interesadas, debido al tiempo de escritura de código, realización de pruebas de funcionalidad y mantenimiento del sistema web educativo.

Para solucionar la vulnerabilidad correspondiente a la inyección de código SQL se propuso lo siguiente:

- Dar formato a las URL con ayuda de archivos *.htaccess* para lograr una presentación amigable, de tal forma, que el valor de las variables se adjuntara en forma de directorios, tratando de ocultar al usuario las variables, encapsulándolas como una ubicación o directorio.
- Validar la URL por medio del lenguaje de programación PHP empleado para programar el sistema web educativo.

Para la primera opción, seguía presentando el incidente en la seguridad de la información, por lo que se optó por denegar las palabras reservadas de SQL. La segunda solución al problema se descartó debido a que se ejecuta primero la URL antes que la validación escrita en PHP, es por ello que la mejor solución es utilizar directivas para el servidor web por medio de archivos *.htaccess,* es decir, enfocadas a otro uso.

En resumen, se optó por los controles que impactaran lo menos posible en el funcionamiento y los tiempos de desarrollo del sistema web educativo

evitando alargar el tiempo de pruebas, corrección de errores y escritura de código adicional.

2.4 Alcance y limitaciones de la solución de la Seguridad de la Información

Los controles de seguridad en la información implementados en el sistema web educativo, permite proteger al sistema contra código malicioso SQL, acceso no autorizado a perfiles o privilegios y proporciona la validación de entrada de datos de manera lógica para preservar la autenticidad, integridad y confidencialidad de las claves de usuario y de la información.

No se implementa algún control de seguridad física, debido a la limitante en los recursos con los que contaba las partes interesadas, por lo que no se protege contra fallos eléctricos, el mal funcionamiento de los dispositivos y el hardware o fallas en la red. Es responsabilidad de la empresa hacer el debido análisis de riesgos de la seguridad de la información para implementar los controles de la seguridad de la información restantes y recomendados por las normas y estándares como COBIT o ISO/IEC 27001:2005.

La ingeniería social es otra limitante de la solución, pues no controla a los usuarios y sus capacidades, además de su ética al momento de compartir su información con otras personas.

Los controles y mecanismos implementados están sujetos a la evolución de la tecnología y de las herramientas desarrolladas para explotar las vulnerabilidades de los sistemas web, es decir, pueden quedar obsoletos o su efectividad puede verse degradada. Es por esto que se recomienda hacer auditorias periódicas al sistema web educativo.

2.5 Establecimiento de los Requerimientos de la Seguridad de la Información

Las partes interesadas deciden implementar la seguridad de la información de acuerdo a sus necesidades, limitaciones, características y los recursos con los que se cuenta. Para el desarrollo de este reporte de aplicación de conocimiento, tanto la empresa como los desarrolladores, acordaron que

los controles de seguridad de la información se implementaran a nivel Software.

A continuación se presentan los requerimientos identificados en el Sistema Web Educativo:

- Se integran a la URL claves o identificadores de algunas entidades que se utilizan para arrojar una consulta a la base de datos, de tal forma que si son modificadas ya sea intencionalmente o accidentalmente, el sistema presenta dos comportamientos.
    - El primero, regresa una consulta con información no autorizada al usuario
    - El segundo, el sistema entra en un estado de error de consulta.

  Las partes interesadas identificaron la necesidad de un control de seguridad para autentificar las claves (identificadores). La solución que se presenta para este requerimiento, es la implementación de *firmas digitales* utilizando el lenguaje de programación PHP y basado en el uso de un método *hash* para autentificar el origen y contenido de las claves y ejecutar las medidas correctivas adecuadas.

- Se identificó que en algunas cajas de texto que componen el sistema, era posible introducir sentencias de SQL válidas de cualquier tipo, por lo que la integridad de la base de datos estaba comprometida, permitiéndole modificar, insertar o borrar alguna tabla del esquema. De ahí la necesidad de implementar un control de seguridad para evitar la inyección SQL.

  La solución que se propuso para esta vulnerabilidad, fue una validación para verificar la entrada de datos que el usuario ingresara antes de enviarla a ejecución, rechazando aquellas que en su contenido se encontraran palabras reservadas del lenguaje SQL y ejecutar las medidas correctivas adecuadas.

- En los campos de la URL, también era posible insertar sentencias SQL, por lo se implementó un archivo *.htaccess* que modifica el comportamiento del servidor web mediante las directivas contenidas en este, la directiva evita que cualquier URL que contenga palabras

reservadas del lenguaje de SQL se ejecuten y se realiza las medidas correctivas acordadas.

- Finalmente, existían archivos fuentes del sistema web educativo, que no contenían los métodos establecidos para verificar permisos y eran accedidos por perfiles no autorizados. Las partes interesadas identificaron que se debía incluir el método definido para cada perfil a cada archivo del sistema web educativo. La solución consistió en incluir en todos los archivos el método de verificación de permisos definido para cada archivo dependiendo del perfil que tiene autorizado el acceso.

2.6 Análisis de la solución Implementada

Con base en un análisis de los archivos y el número de líneas que requerían un mantenimiento del sistema web educativo, se definieron los controles de seguridad a implementar.

Se utilizó un Modelo Vista y Controlador, que permitió identificar los archivos que están expuestos a las vulnerabilidades de claves enviadas a través de la URL, identificando las líneas de código vulnerables y sus variables correspondientes, a estos se les aplico un mantenimiento o control de seguridad de la información, para evitar la inyección SQL.

Por otro lado, se identificaron los archivos vulnerables a los permisos de usuarios, y se aplicaron las medidas de control de seguridad correspondiente para disminuir el riesgo de incidentes en la seguridad de la información.

Los controles de seguridad de la información implementados que se adaptaron a las necesidades del sistema web educativo son:

- Firma Digital
- Uso de directivas del servidor para el tratamiento de la URL
- Validación para entradas de texto de usuarios evitando la inyección SQL
- Inclusión de validación de permisos

Para la implementación de estos controles de seguridad de información, se realizó el análisis de estimación de tiempo y recursos requeridos para realizar el mantenimiento correspondiente. La Tabla 2-5 muestra los valores calculados.

Tabla 2-5 Tabla de Análisis de tiempo y recursos

Control de seguridad de la información	Tiempo Unitario	Tiempo Total aproximado
Controles para la URL	20 minutos por línea en la implementación. En promedio 4 líneas por archivo.	22 días
Controles de permisos	10 minutos por archivo.	2 semanas
Directivas para servidor web	Una semana para el diseño de expresiones regulares Implementación, un día	1 semana
Validación de entradas SQL	Diseño, una semana Implementación, un día	1 semana

2.7 Implementación de los controles de Seguridad

Los controles de seguridad de la información implementados son presentados a continuación. Se eligieron con base en el análisis de los archivos y líneas que debían ser modificados y considerando el impacto que resultaría al implementarlos en el Sistema Web Educativo.

La característica principal de los controles implementados, es que no demandan mayor modificación en el código original, por lo que, la funcionalidad del sistema web educativo no se ve degradada. Sin embargo, en cualquier caso, los controles pueden ser desactivados por medio de una modificación al método principal, en caso de falla o en caso de que la empresa decida implementar otro tipo de controles en un futuro.

Firma digital

Las partes interesadas aceptaron implementar un control de seguridad basado en firma digital, está permite verificar la autenticidad de las claves

que se agregan a la URL y que sirven para llevar a cabo las consultas a la base de datos.

El método consiste en calcular una firma digital a partir del contenido de la clave. Dentro del sistema web se envía la clave y su respectiva firma a través de la URL para su operación. En otra parte del sistema, se calcula un nuevo valor de firma digital a partir del contenido de la clave recibida. Ambas firmas digitales, la nueva y la capturada en la URL son comparadas para validar su autenticidad, gracias a ello se puede detectar un cambio ilegal en el contenido de la firma o en el contenido de la clave para ejecutar las medidas correctivas respectivas. El método para calcular la firma corresponde a un método basado en *hash* llamado MD5, y corresponde a un método simétrico de cifrado.

Un *método de cifrado simétrico* utiliza un método matemático simétrico, que consiste en utilizar una llave o clave única para cifrar y descifrar el contenido de un mensaje. Particularmente en el caso de los métodos basados en funciones *hash*, no es posible obtener el mensaje a partir del valor *hash* [9].

MD5 se basa en el método *hash* que utiliza un bloque de 128 bits para calcular el valor *hash* del mensaje. Esté se utiliza para comprobar la integridad del contenido de un documento o como un método de autenticación e integridad de los datos de las claves en la URL. El lenguaje PHP contiene una implementación segura de MD5. Sin embargo, la desventaja de utilizar métodos de cifrado basados en *hash* es que en un momento dado puede generar una colisión cuando dos mensajes corresponden a un valor *hash*, no óbstate, entre más grande es la llave única de cifrado más difícil será generar una colisión.

Como dato adicional que justifica la utilidad de este método, los sistemas UNIX/Linux utilizan MD5 para cifrar las claves de los usuarios. Cabe destacar que en estos sistemas se puede modificar el método de cifrado de las claves de usuario, ya que, no es el único método que se puede utilizar para verificar la autenticidad e integridad de un documento o usuario.

En la Figura 2-1, se presenta un ejemplo de una función genérica que puede utilizarse en cualquier sistema web para la implementación de controles tipo firma digital.

```
function generaLlave()
{
    //Contiene todos los caracteres permitidos para generar
la llave
    $array = array("A", "B", "C",
"D","E","F","G","H","I","J","K","L","M","N","O","P","Q","R"
,"S","T","U","V","W","X","Y","Z"

,"a","b","c","d","f","g","h","i","j","k","l","m","n","o","p
","q","r","s","t","u","v","w","x","y","z"

,"1","2","3","4","5","6","7","8","9","0","@","%","*","#");
    //Tamaño que tendrá la llave
    $tamPalabra =10;
    $llave="";
     for($x=0;$x <=$tamPalabra;$x++)
     {
         $llave= $llave.$array[rand(1,60)];
     }
     return $llave;
}
```

Figura 2-1 Función que genera llave

Para ello primeramente está función debe generar la llave única con la cual se calcula el valor *hash* para cada clave que se pasa a través de la URL a otras páginas del mismo sistema. Cada vez que un usuario se firma, se genera una nueva llave única, de esta forma, si el usuario obtiene la llave única, la próxima vez que ingrese al sistema o se firme con otro usuario, no podrá generar un incidente en la seguridad de la información.

Para este ejemplo en particular, la llave tiene una longitud de 10 caracteres para evitar la colisión de valores *hash*. Se recomienda que esté método se utilice una vez en todo el programa y se ejecute en la parte donde se construye la sesión de usuario.

Posteriormente se debe generar la firma *hash* a partir de la llave generada con anterioridad. La Figura 2-2 muestra un ejemplo genérico de una función para generar la firma digital en cualquier sistema web.

```
//Función para firmar una clave o variable
function generaFirma($variable)
{
        //Se llamar al método para generar la llave
     aleatoria y firmar una variable
         session_start();
         $llave = $_SESSION["llave"];
         $firmaVariable = md5($llave . $variable);
         return $firmaVariable;
}
```

Figura 2-2 Función que genera firma

Está función debe recibir el valor de la clave, con la cual se genera una firma digital, se recupera la llave única y se aplica el método de MD5 implementado en PHP al valor de la clave. Esta firma digital es única para cada valor de una clave. Este método debería utilizarse en cada parte del sistema web donde se deba direccionar a otra página del mismo sistema, adjuntando las claves y se adiciona a la URL la firma digital obtenida.

Para verificar los valores de las firmas digitales implementadas en cualquier sistema web, es necesario comparar la firma digital generada con la nueva firma digital que proviene de una página del sistema. Para ello podemos apoyarnos en la función general de verificación de firma presentada en la Figura 2-3. Cabe mencionar que todas estas funciones presentadas son genéricas para cualquier sistema web, no corresponden a las utilizadas en el sistema web educativo, ya que poner el código de las funciones implementadas para el sistema web educativo, pondría en riesgo la confidencialidad de la empresas, por lo que se optó en ilustrar la generación de la firma digital, con funciones genéricas que pueden implementarse en cualquier sistema web.

```
//Función que verificara la firma
function verificaFirma($variable,$firmaActual)
{
    //Aquí se vuelve a calcular el hash para verificar que
la variable no fue modificada
    $firma = generaFirma($variable);
    //comparar las firmas y sino son iguales, la firma o la
variable fue modificada
    if ($firma!=$firmaActual)
    {
        //Acción correctiva para la violación de la
seguridad
        header('Location: /index.php' );
    }
}
```

Figura 2-3 Función que verifica firma

Con estos controles de firma digital, si el usuario no conoce la llave única, no es posible que genere firmas digitales válidas para insertar otros valores a las claves con los cuales pueda obtener información no autorizada de la base de datos. Este procedimiento se ejecuta cada que se desea verificar si la clave no ha sido alterada por el usuario u otro atacante al sistema web.

Para ilustrar el funcionamiento de este módulo de firmas digitales, se muestra la Figura 2-4 con un diagrama de secuencia que describe el proceso que se lleva a cabo al utilizar este módulo.

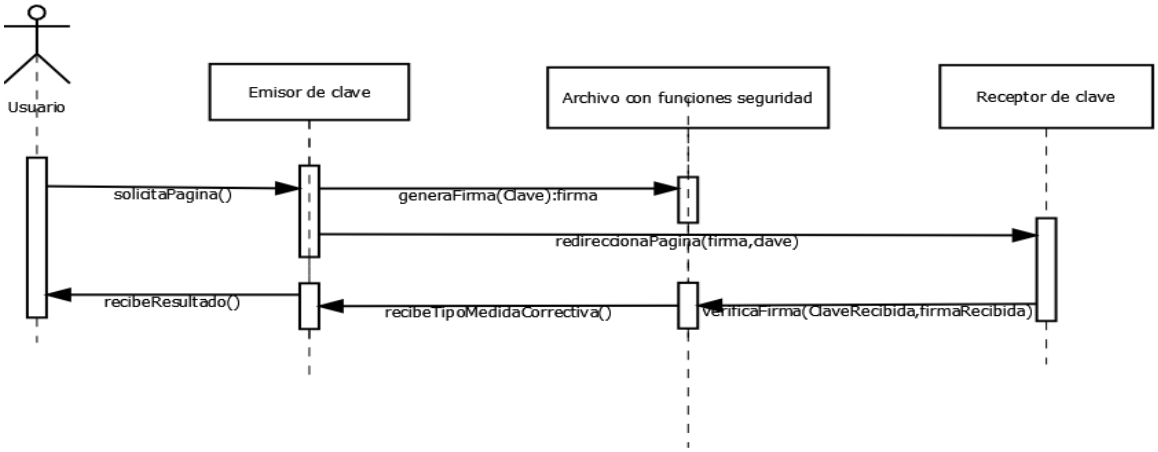


Figura 2-4 Diagrama de secuencias de Firma Digital

El emisor de clave es una página web que es parte del sistema que va a direccionar en alguna otra página del sistema, agregando a la URL una clave y una firma para su uso y verificación; en la página emisora se debe generar la firma digital que corresponde al valor de la clave que se enviará. El receptor de clave es una página web a la cual se está re-direccionando desde un emisor de clave y que debe capturar una clave y una firma para hacer las operaciones para la cual se desarrolló. En esta página se debe verificar la integridad de la clave para garantizar la autenticidad en la información. Se calcula un nuevo valor de firma para la clave recibida y se compara con el valor de la firma recibida, si no coinciden, las acciones correctivas serán ejecutadas.

Uso de Directivas de Servidor para la entrada de datos por la URL

Para evitar la inyección código SQL mediante la URL, las partes interesadas aceptaron utilizar un archivo *.htaccess* que contiene directivas de configuración para el servidor y se coloca en el directorio donde se quiere aplicar estas directivas.

Las directivas tienen la forma de expresiones regulares, lo que facilita formar modelos que se apliquen a varios casos. Se utilizan

principalmente para implementar controles de autentificación de usuarios, archivos, crear URL amigables para el usuario y rescribir reglas para detectar un incidente en la seguridad de la información y realizar las acciones correctivas correspondientes [10].

En el caso del sistema web educativo, se utiliza para restringir las palabras reservadas del lenguaje de SQL e incidentes en la seguridad de la información del tipo inyección SQL mediante la URL, ya que en este era posible insertar sentencias SQL válidas que comprometían la integridad de la información y la estructura de la base de datos.

Este método de filtrado de URL se puede utilizar en cualquier otro sistema web que utilice, como forma de almacenamiento, base de datos relaciones basadas en el lenguaje SQL.

A continuación, la Figura 2-5 muestra un ejemplo genérico de las líneas que pueden existir en un archivo *.htaccess*. La línea “RewriteEngine On” indica que se permite rescribir las reglas del servidor con la instrucción de las líneas que se encuentren debajo de esta.

```
RewriteEngine On

#Esta parte es para evitar las sentencias sql en la URL
#Condición que revisa el contenido de una palabra reservada
#Si encuentra la palabra reservada indica que no existe esa
pagina
RewriteCond %{THE_REQUEST}
^.*(i|I)(n|N)(s|S)(e|E)(r|R)(t|T)\b.*$
RewriteRule .* - [L,R=404]
RewriteCond %{THE_REQUEST}
^.*(s|S)(e|E)(l|L)(e|E)(c|C)(t|T)\b.*$
RewriteRule .* - [L,R=404]
RewriteCond %{THE_REQUEST}
^.*(c|C)(r|R)(e|E)(a|A)(t|T)(e|E)\b.*$
RewriteRule .* - [L,R=404]
RewriteCond %{THE_REQUEST} ^.*(d|D)(r|R)(o|O)(p|P)\b.*$
RewriteRule .* - [L,R=404]
RewriteCond %{THE_REQUEST}
^.*(d|D)(e|E)(l|L)(e|E)(t|T)(e|E)\b.*$
RewriteRule .* - [L,R=404]
RewriteCond %{THE_REQUEST}
^.*(u|U)(p|P)(d|D)(a|A)(t|T)(e|E)\b.*$
RewriteRule .* - [L,R=404]
RewriteCond %{THE_REQUEST}
^.*(a|A)(l|L)(t|T)(e|E)(r|R)\b.*$
RewriteRule .* - [L,R=404]
```

Figura 2-5 Directivas de servidor

Las líneas del tipo “RewriteCond %{THE_REQUEST}” indican que la URL objetivo será analizada y se buscará en ella el caso que describa la línea que se encuentre debajo de está. Las líneas del tipo “^.*(i|I)(n|N)(s|S)(e|E)(r|R)(t|T)\b.*$” se utilizan para buscar una palabra por medio de una expresión regular.

Las líneas del tipo “RewriteRule”, indican que si se suscita el evento que no cumpla con la regla de la línea anterior, se aplicará la medida correctiva. Con este método se evita la inyección de código SQL por medio de la URL.

La Figura 2-6 describe el proceso que se lleva a cabo al usar las directivas del archivo *.htaccess* para evitar la inyección de código SQL por medio de la URL. En cuando se inicia una petición para solicitar que se muestre una página del sistema, el servidor ejecuta el archivo *.htaccess* y sobre-escribe las reglas con las directivas contenidas en el archivo *.htaccess*. Si no se encuentra un incidente en la seguridad de la información, cargará la página solicitada en la petición, en otro caso, mostrará el estado de error “Página no encontrada” y se da por terminada la petición.

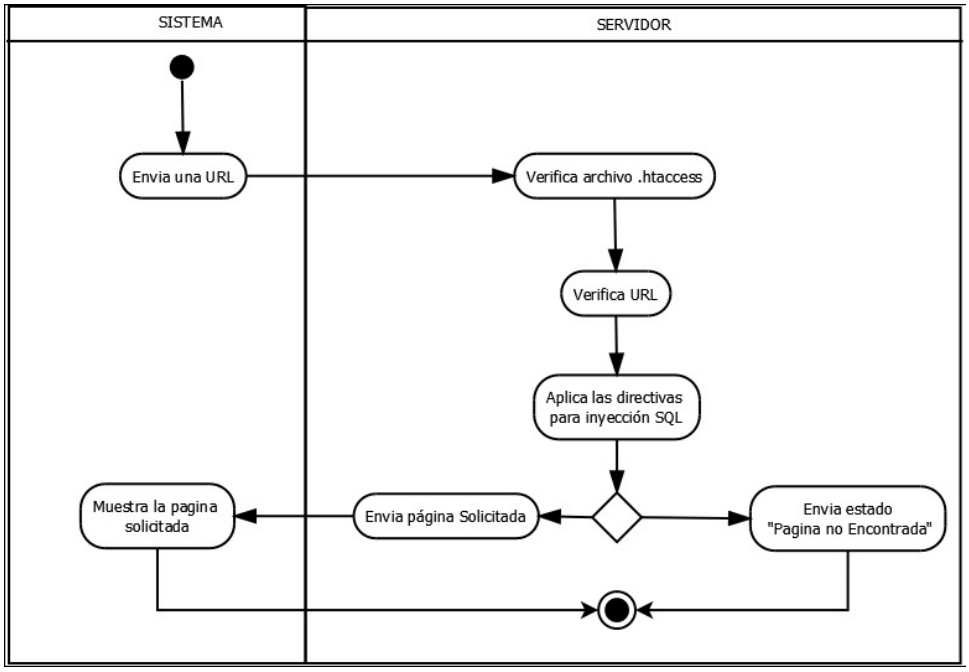


Figura 2-6 Diagrama de actividades Directivas de Servidor

Validación para entradas de texto de usuarios

Para la validación de las entradas de texto que los usuarios ingresan al sistema web educativo, mediante las cajas de texto, tales como el *login*, se agregó una función para validar que no existieran palabras reservadas del lenguaje SQL o caracteres reconocidos por el gestor de la base de datos, evitando la ejecución de estos y proteger la integridad de la base de datos.

La Figura 2-7 describe el funcionamiento que debe ejecutarse para filtrar las palabras SQL provenientes de las cajas de textos para los usuarios del sistema web educativo. El usuario puede ser cualquiera de los perfiles definidos para el sistema web educativo. El receptor de entrada se entiende como una página del sistema web educativo que recibe una entrada de texto del usuario y que debe ser analizada antes de ser ejecutada o enviada a la base de datos. El usuario envía una entrada de texto a un receptor de mensaje del sistema web educativo, el receptor filtrar las palabras reservadas de SQL que puedan comprometer la integridad de la información y la estructura de la base de datos. El archivo Funciones de Seguridad, actúa como controlador, siendo este, el que hace el procesamiento de la petición de la vista.

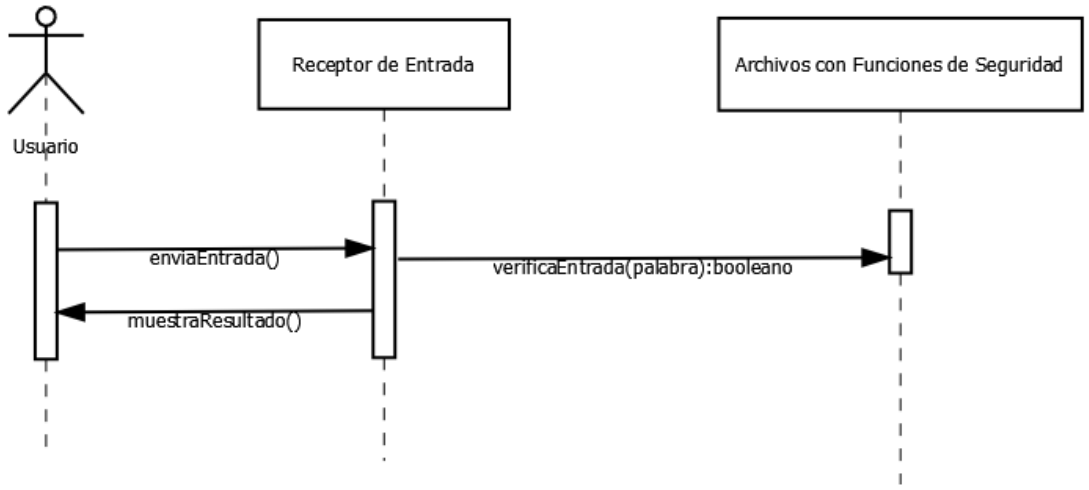


Figura 2-7 Diagrama de Actividades de validación para inyección SQL

Inclusión de validación de permisos en cada archivo

La implementación de los métodos correspondientes a cada tipo de perfil para verificar los permisos de usuario se realizó previamente a implementación de los controles de seguridad de la información. Cuando se

evaluó la efectividad de la validación de permisos, se presentó el siguiente problema: al realizar constantes llamadas al método en una misma página del sistema web educativo, el sistema entra en un estado cíclico infinito.

Para evitar el estado cíclico infinito, se discriminaron los archivos que requerían la inclusión de la validación de los permisos, dejando una vulnerabilidad en la restricción de permisos sobre estos, permitiendo su acceso no autorizado por otros perfiles o atacantes de la seguridad de la información. Por falta de tiempo, y por acuerdo de las partes interesadas no se pudo desarrollar eficientemente otro método para tratar esta excepción. Sin embargo, se recomienda la creación de un archivo donde se especifique el nivel de permisos de cada rol de usuario y se consulte cuando sea necesario.

2.8 Análisis de desempeño de los controles de seguridad implementados

Los controles de seguridad con referencia a archivos *.htacces* y validaciones de palabras SQL se probaron en un servidor con dirección IP pública y bajo flujo de información. Se revisó que funcionaran recreando nuevamente los ataques a las vulnerabilidades en el sistema web educativo, se encontró que esta solución es satisfactoria a los requerimientos de la seguridad de la información establecidos por las partes interesadas.

El control de firmas digitales se probó en un servidor *offline* y con bajo flujo de información. Con base en los resultados arrojados por las pruebas realizadas, se encuentra satisfactorio el resultado y se pronostica el mismo comportamiento cuando se implemente al sistema web educativo y se encuentre de manera online y con un flujo de información mayor.

Debido a la cercanía de los tiempos de entrega de producto final y el cierre del proyecto con CONACYT, no fue posible implementar el control de firmas digitales sobre una versión estable del sistema web educativo, por lo cual no se tiene una respuesta a la efectividad de este control por las partes interesadas y de la empresa.

En resumen, la solución se encuentra satisfactoria para los requisitos de la seguridad de la información establecidos por las partes

interesadas bajo las limitaciones establecidas como el tiempo de pruebas y de escritura de código.

2.9 Análisis de la propuesta implementada

La firma digital es un mecanismo eficiente para verificar la autenticidad e integridad de la información, sin embargo, la efectividad de este control de la seguridad de la información depende del método de cifrado que se utilice. En la literatura se menciona que expertos en cifrado han logrado colisionar y vulnerar el algoritmo MD5, con lo cual baja la efectividad del control implementado para el sistema web educativo [11].

Las directivas del servidor para el tratamiento de la URL son un control de seguridad en la información efectiva, aplica expresiones regulares que se adaptan a diferentes casos de la URL y es independiente del sistema web al que se implemente. Se logra filtrar las principales palabras reservadas del lenguaje SQL que permiten consultar y modificar la información, sin importar su escritura o la ubicación en la URL. Se presentan en pocas líneas, sin impactar en la funcionalidad o el código del sistema web educativo, lo cual lo hace un control rápido de implementar, probar y desactivar.

La validación para entradas de texto de usuarios para evitar la inyección de código SQL, es un control indispensable que se debe implementar. No se puede confiar en el usuario y su ética al momento de utilizar el sistema web educativo. Este control se aplicó únicamente a las cajas de texto correspondiente a la clave del usuario (*login*), se recomienda aplicar las validaciones a todas las entradas de texto de los usuarios y construcciones de sentencias SQL.

La inclusión de la validación de los permisos no es un control propiamente estable, por ello, sugiere encontrar otro tipo de control de seguridad de la información para verificar los permisos de los usuarios.

Los controles de seguridad aquí dispuestos evitan tiempos de pruebas y de escritura de código e impactan lo menos posible la funcionalidad del sistema web educativo, pero pueden no ser los

adecuados ante atacantes con herramientas más sofisticadas y automatizadas para explotar las vulnerabilidades del sistema.

2.10 Adecuaciones de la Propuesta del SGSI para mejorar su desempeño

Para obtener mejoras en los resultados y garantizar la seguridad del sistema web educativo, se propone implementar otros controles de seguridad de la información para lograr satisfacer los mismos requerimientos de seguridad de la información de una manera óptima.

Para las claves añadidas a la URL se recomienda utilizar otros métodos para mantener disponibles esta información, sin que el usuario u otras amenazas tengan acceso a estas claves. Para ello se sugiere implementar el método *post* para ocultar esta información al usuario. Adicionalmente, se puede hacer uso de las variables de sesión para mantener globales las claves y puedan ser utilizadas en cualquier parte del sistema sin que el usuario u otras amenazas tengan acceso a estas y conocerlas.

Se debe implementar validaciones de entrada de datos apropiadas, es decir, se deben verificar las entradas de datos de todas las transacciones realizadas en el sistema web educativo, tales como nombre, direcciones, teléfonos, referencias de los usuarios, entre otras. Se recomienda realizar controles de seguridad de la información que verifiquen los datos de entrada contra valores fuera de rango, caracteres inválidos, exceder el límite de volumen de datos, control de datos no autorizados o inconsistentes. Se recomienda hacer una revisión periódica de las claves o archivos de datos para confirmar su integridad.

Por otro lado, añadir seguridad física y seguridad en el servidor es sumamente conveniente. Para ello se debe implementar firewalls o listas de acceso, estos impiden el acceso no autorizado al sistema de personas o amenazas que pretendan robar información o comprometer la integridad de la misma.

A continuación, se proyecta una propuesta para implementar un adecuado SGSI, basándose en la norma ISO/IEC 17799 [4] que describen las mejores prácticas sobre los requerimientos de gestión, métricas,

medición, lineamiento e implementación de un SGSI utilizando el esquema de numeración de la norma ISO/IEC 27001:2005 [4].

El primero paso para implementar un SGSI adecuado consiste en determinar los activos de información que se requiere proteger y su valor, evaluar los riesgos de seguridad de la información y definir las características de la organización o empresa. Para ello la norma ISO 17799 sugiere que la alta gerencia compare los objetivos de la empresa u organización con los requerimientos legales de la seguridad de la información que tiene que satisfacer para estar en cumplimiento con las normas, leyes y regulaciones a los que está sujeta [4].

En México la ley que obliga a las empresas y organizaciones a mantener seguridad en la información de los usuarios, es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares LFPDPP, que regula el tratamiento legítimo, controlado e informado de los datos personales, con el objeto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas [12].

Como segundo paso, la empresa debe establecer el plan de tratamiento de riesgos para implementar los controles de seguridad de la información y los métodos de recuperación de errores. La norma ISO/IEC 17799 [4], sugiere que después de hacer el análisis y evaluación de riesgos, la empresa decida si puede aceptar los riesgos de seguridad de la información o decide ignorarlos o traspasarlos.

Las opciones posibles para el tratamiento de riesgos son las siguientes.

- Aplicar los controles de la seguridad de la información apropiados o recomendados para reducir los riesgos identificados en la etapa anterior.
- Aceptar los riesgos consciente y objetivamente, tomando en cuenta las características de la empresa y los recursos con los que se cuenta, además de cuidar que los controles y mecanismos de seguridad de la información que se necesiten implementar cumplen con la visión y los objetivos de la empresa
- Transferir los riesgos en la seguridad de la información que la empresa no pueda mitigar y contrarrestar, en particular, lo que refieren a terceras entidades como son proveedores.

Una vez, decidido cuales riesgos serán aceptados por la empresa, se deberán decidir los controles de la seguridad de la información que serán implementados tomando en cuenta los siguientes puntos.

- Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales.
- Los objetivos y visión de la empresa.
- Los requerimientos y limitaciones operacionales de la empresa.
- Los costos de la implementación en relación con los riesgos. El costo de implementar un control en la seguridad de la información no debe sobrepasar el costo total que representa la pérdida o daño del activo, en este caso, la información.

Apoyándose en la norma ISO/IEC 17799 [4], los controles básicos que se sugiere implementar son los siguientes:

- Diseñar e implementar una política de seguridad que proporcione a la empresa, la dirección y el soporte para la seguridad de la información en relación con los requerimientos de la empresa y las leyes regulatorias de privacidad de los datos.
- Diseñar e implementar un esquema que permita la organización de la información para un adecuado control, tratamiento y acceso. Esto incluye asignar responsabilidades en la seguridad de la información, es decir, las personas responsables de la información, sus privilegios y sus roles; definir métodos de procesamiento de la información que eviten su perdida y permita su recuperación.
- Establecer contratos con las terceras partes para la protección de datos personales, antes de permitir a los usuarios y al personal el acceso a la información. En caso de fallar al convenio de la protección de los datos, aplicar las medidas correctivas acordadas o aplicar la ley vigente de privacidad de datos.
- Se recomienda implementar seguridad física en las instalaciones donde se alojan servidores y bases de datos. Particularmente, se recomienda implementar seguridad de redes. Implementar un sistema de respaldo de la información es indispensable para

garantizar la disponibilidad, integridad de la información y recuperación contra pérdidas y errores.

- Realizar constantes auditorías al sistema web educativo y evaluar las propiedades de la seguridad de la información, así como realizar el registro de actividades e incidente de seguridad que se presenten en el sistema web educativo y los recursos relacionados a este.
- Utilizar un sistema de monitoreo para vigilar el flujo de información y la infraestructura de red que se ocupa para el sistema, la empresa no debe olvidar restringir el uso de estas herramientas de sistema de monitoreo de flujo de información, ya que pueden ser utilizadas para obtener acceso a los flujos de información de formar no autorizada. Implementar herramientas basadas en el Protocolo Simple de Administración de Red SNMP [13] es recomendable.
- Establecer políticas para el control de acceso a los medios, al sistema y los recursos del mismo, definiendo claramente privilegios, usuarios y roles. En el sistema se tiene definido los perfiles, pero los permisos no son muy claros, se puede hacer énfasis en este aspecto.
- Implementar controles de acceso a la red como listas de acceso, mecanismos de autenticación, etc. Algunos equipos, como los routers CISCO ya proporcionan esta facultad [13].
- Implementar un control de acceso y autentificación de usuario donde se indique la actividad del usuario. Implementar un log que registre todas las transacciones y operaciones que cada usuario realiza.
- Implementar protocolos seguros de servicios de redes, como HTTPS o SMTPS, además de la implementación de certificados de autenticidad SSL. Lo último es muy importante para comprobar la identidad y ubicación del servidor de la empresa.

Estos son los controles de la seguridad de la información mínimos que se recomienda implementar, para garantizar que las propiedades de la seguridad de la información se protejan y cumplan con los requerimientos de la empresa y los requerimientos legales de la región. Para más detalle e información sobre otros controles de la seguridad de la información más

especializados o específicos a cada requerimiento de la empresa se puede consultar la norma ISO/IEC 177799 [4].

Como tercer paso, el sistema web educativo se debe someter a las pruebas que se acordó con las partes interesas y los encargados de la seguridad de la información y pruebas, para ello, en la norma ISO/IEC 177799 [4] se recomienda:

- Ocupar flujos de información operacional que se asemejen a las cargas reales para observar el comportamiento del sistema web educativo y se puedan detectar vulnerabilidades en la seguridad de la información y otros errores de funcionalidad y diseño.
- Se debe realizar pruebas donde se reproduzcan varios escenarios a los que puede estar expuesto el sistema web educativo.
- El código fuente y el recurso o infraestructura del sistema web educativo debe estar debidamente restringido y sólo el personal autorizado debe tener acceso a éste para evitar la introducción de procedimientos o funciones no autorizadas.
- Las pruebas deben ser registradas, además de registrar todos los incidentes de seguridad de la información ocurridos.
- Se debe identificar todo el código, entidades, bases de datos y hardware que requiera mantenimiento. Posteriormente realizar las medidas correctivas que la empresa requiera y apruebe.
- Realizar pruebas de recuperación técnica, puede ser de errores o de información. Como es la restauración de la base de datos y documentar el procedimiento que se lleve a cabo para su implementación.
- Por último, se debe tener un registro detallado de todos los cambios que se harán en el sistema y la infraestructura del mismo y la empresa debe aceptar los cambios para que sean realizados

El último paso, consiste en establecer un control riguroso, de tal forma que se debe documentar debidamente todo cambio hecho en el sistema web educativo. Esto puede implicar hacer un nuevo análisis y evaluación de riesgos para medir los riesgos y el impacto que se tendrá debido a los

cambios que se efectuarán en el sistema web educativo y la infraestructura del mismo. Para ello la norma ISO/IEC 17799 [4] sugiere lo siguiente.

- Los cambios deben ser presentados a los usuarios autorizados. Por ejemplo, el equipo de desarrollo.
- Asegurarse que la integridad y la funcionalidad del sistema web educativo no se vean degradados por los cambios efectuados.
- Actualizar toda la documentación del sistema al realizar y completar cada cambio y la documentación anterior se archive o elimine.
- Mantener un control de las versiones del sistema web educativo de forma detallada describiendo los cambios realizados.
- Realizar y mantener un registro de auditoria del sistema web educativo con todas las recomendaciones y anomalías encontradas para realizar las medidas correctivas competentes.
- Notificar con tiempo a todas las partes involucradas en el sistema web educativo, sobre los cambios a realizar y el tiempo que durará el mantenimiento.
- Asegurarse que la implementación de los cambios se realice sin interrumpir el flujo normal de trabajo del sistema web educativo y que no interrumpa las actividades de los usuarios.

Estas son las recomendaciones que se hacen con base en la norma ISO/IEC 177799 [4] y la norma ISO/IEC 27001:2005 [1], sin embargo, se puede consultar estas normas para más detalle o consultar otras recomendaciones o buenas practicas más específicas, además que existen otros marcos referenciales en los cuales se puede basar para un correcto mantenimiento y mejoramiento del sistema.

Los controles propuestos anteriormente son los recomendados para cumplir con los requerimientos básicos de seguridad de la información. De esta forma se logra cumplir con las regulaciones y leyes impuestas en México, como la ley de protección a los datos confidenciales de los usuarios. Además, se logra proteger los procesos del sistema web educativo ante errores y se permite la recuperación correcta de estos, se permite la detección de incidencias de seguridad de la información para poder tomar las acciones correctivas adecuadas a cada caso particular.

Por otro lado, la empresa debe estar completamente comprometida con la implementación de seguridad de la información para que se puedan adicionar dichos controles, en caso contrario, es difícil o nula la posibilidad de desarrollar e implementar un SGSI adecuado y debería aceptar los riesgos y responsabilidades de no hacerlo. Cabe destacar que estos controles están basados en normas ISCO/IEC 27001 e ISO/IEC 17799 y que existen otros estándares, metodologías y normas para ayudar a lograr objetivo de la seguridad de la información, como lo es COBIT que tiene un apartado dedicado a la gestión de la seguridad.

La empresa debe realizar correctamente el análisis y evaluación de riesgos, además de estar consciente de sus recursos para adoptar esta u otra metodología o marco de referencia para la implementación de la seguridad de la información.

En este proyecto se recomiendan las normas conocidas y señaladas como las adecuadas para lograr alcanzar los objetivos de las partes interesadas, basándose en el tiempo de entrega del producto y el recurso económico de esta.

En resumen, los controles propuestos son para proteger los activos de la empresa, en este caso, la información como recurso de un valor importante tanto para la empresa como para los usuarios y terceras partes.

Capítulo 3 . Resultados

En este capítulo, se describen los resultados obtenidos de acuerdo a los escenarios y las condiciones en donde se llevó a cabo la implementación de la solución propuesta para alcanzar el objetivo del reporte de aplicación de conocimientos.

El entorno en el cual se probaron los controles de seguridad de la información implementados en el sistema web educativo cuenta con las siguientes características:

- Entorno controlado
- Entorno *offline*
- El flujo de datos es bajo flujo
- Un solo usuario
- Uso de herramientas especializadas para la detección de inyección SQL y otras vulnerabilidades en la seguridad de la información.

En la Tabla 3-1 se resumen las condiciones con las cuales se realizaron las pruebas para la solución propuesta descrita en la sección 2.7 y el resultado obtenido.

Tabla 3-1 Resultado de pruebas de control de seguridad en un sistema off-line

Control de seguridad	**Condición**	**Resultado**
Firma digital	El valor de la clave y el valor de la firma digital no se modifican por un usuario.	Las acciones correctivas no se ejecutan como se espera.
Firma digital	El valor de la clave se modifica con un valor no autorizado por un usuario o atacante.	Las acciones correctivas se ejecutan, el sistema regresa a la página principal.
Firma Digital	El valor de la clave se modifica con un valor, que	Las acciones correctivas se ejecutan, el sistema regresa a la

Control de seguridad	Condición	Resultado
	existe en la base de datos, pero no está autorizado a su acceso, por un usuario o atacante.	página principal.
Firma Digital	El valor de la clave se borra, es decir, apunta a nulo, por un usuario o atacante.	Otra validación se encarga de ejecutar las acciones de recuperación, regresa a la página principal cuando una clave se encuentra en nulo.
Firma Digital	El valor de la firma se modifica por un usuario o atacante.	Las acciones correctivas se ejecutan, el sistema regresa a la página principal.
Firma Digital	El valor de la firma se borra, es decir, apunta a nulo por un usuario o atacante.	Las acciones correctivas se ejecutan, el sistema regresa a la página principal.
Firma Digital	El valor de la firma y el valor de la clave son borrados, es decir, apuntan a un nulo.	Otra validación que se encarga de ejecutar las acciones de recuperación cuando una clave se encuentra en nulo.
Directivas para servidor mediante el archivo *.htaccess*	Se escribe un carácter o una palabra reservada o reconocida de SQL mediante la URL del sistema web educativo por un usuario o atacante.	Las acciones correctivas se ejecutan mostrando un estado de error del sistema, se despliega por el servidor “Pagina no encontrada”.
Validación de palabras SQL en las entradas de usuario	Se escribe un carácter o una palabra reservada o reconocida de SQL mediante las cajas de texto de la página de login por un usuario o atacante.	Las acciones correctivas se ejecutan, el sistema vuelve a cargar la página de login indicando que el usuario o la contraseña están incorrectos.
Inclusión de validación de permisos de usuario	Se ingresa con perfiles autorizados a una página web del sistema educativo por un usuario.	El sistema permite el acceso al usuario y hacer uso del contenido de la página web.
Inclusión de validación de permisos de	Se ingresa con perfiles no autorizados a una página web del sistema web	El sistema aplica la acción correctiva, el sistema regresa a la página de login indicando que no

Control de seguridad	Condición	Resultado
usuario	educativo.	se tiene privilegio para consultar esa página.

Una vez realizada las pruebas en el sistema web educativo bajo las condiciones mencionadas en la Tabla 3-1, se determinó nuevamente el análisis de riesgos para determinar las ponderaciones de las propiedades de seguridad del sistema web educativo.

La Tabla 3-2 muestra los valores obtenidos de la estimación de riesgos posteriores a la implementación y prueba de los controles de seguridad de la información en el sistema web educativo.

Tabla 3-2 Estimación de Riesgos Posterior

No.	Activo	Valor	Degradación	Impacto	Justificación
1	Claves de usuario y sistema	A	10%	M	El sistema verifica la integridad de las claves.
2	Estructura de base de datos	MA	1%	M	El sistema niega las sentencias no autorizadas.
3	Información de la base de datos	A	1%	B	El sistema no permite el acceso a información no autorizada.
4	Módulos del sistema web educativo	A	1%	B	Se protegieron contra entradas y valores no autorizados.
5	Usuarios del sistema web educativo	A	1%	B	Su información no es revelada a otros usuarios y se almacena en una base de datos restringida.
6	Tecnología donde se montará la aplicación y base de datos	B	1%	MB	Se dejó fuera la infraestructura donde se montará la aplicación y la base de datos debido a falta de recursos.
7	Instalaciones que alojarán la tecnología.	B	1%	MB	Se dejó fuera las instalaciones donde se montará la aplicación y

No.	Activo	Valor	Degradación	Impacto	Justificación
					la base de datos debido a falta de recursos.

Utilizando los valores de las tablas Tabla 3-1 y la Tabla 3-2, se re-calcula la estimación de impacto para evaluar la efectividad de los controles de seguridad del sistema web educativo. La Tabla 3-3 muestra los valores determinados.

Tabla 3-3 Estimación de Impacto Posterior

No. de Activo	Impacto	Probabilidad	Riesgo
1	M	MA	A
2	M	MA	A
3	B	MA	M
4	B	A	M
5	B	M	B
6	MB	B	MB
7	MB	B	MB

Se ponderó en una escala de 1 a 10, las propiedades de la seguridad de la información donde MB=- 10, B=- 8, M=- 6, A= - 4, y MA=-2.

Para los valores posteriores de las propiedades de la seguridad de la información nuevamente se saca el promedio de los valores obtenidos en la estimación de impacto de la Tabla 3-3. En la Tabla 3-4 se compara los valores obtenidos antes y después de aplicar los controles de seguridad de la información descritos en la sección 2.7.

Tabla 3-4 Ponderación de Propiedades de Seguridad

Propiedades de Seguridad	Valor anterior	Valor final
Disponibilidad	5	7
Confidencialidad	5	7
Integridad	5	7
Autenticidad	5	7

En la Figura 3-1 se muestra una gráfica con los valores obtenidos del análisis de las propiedades de seguridad de la información, antes y después de implementar los controles de seguridad de la información, con lo cual se ilustra la mejora obtenida en estas propiedades, aumentando de esta forma la seguridad en la información y por ende la calidad de producto final.

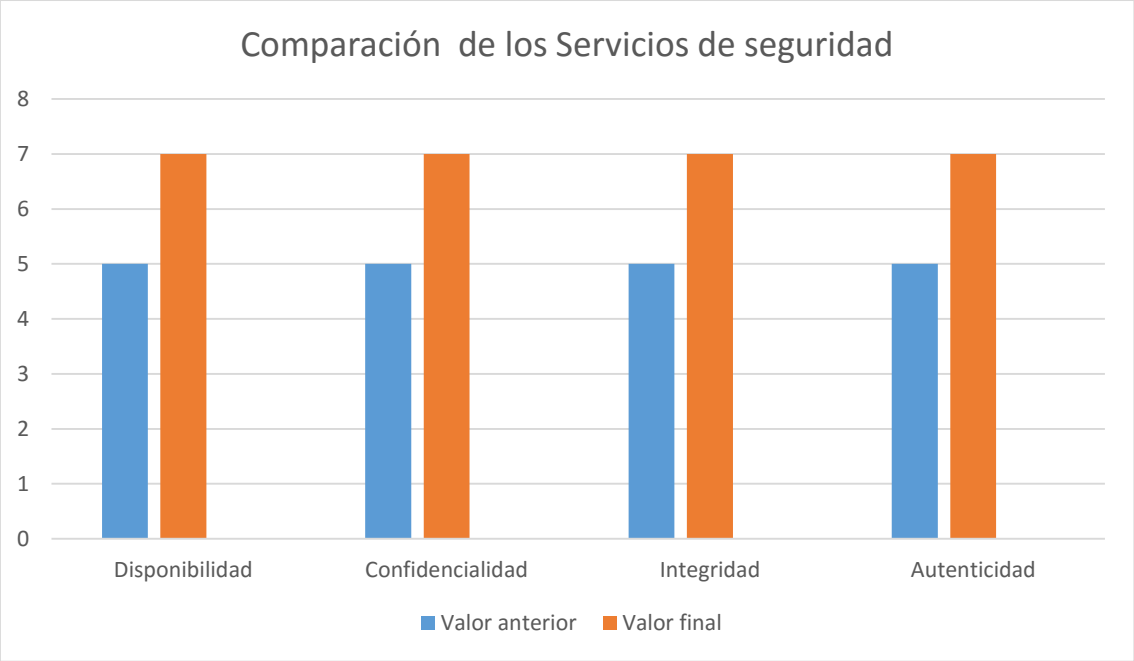


Figura 3-1 Gráfica comparativa de propiedades de seguridad

Mediante los controles de seguridad de la información implementados en el sistema, se cubrieron vulnerabilidades importantes como inyección de código SQL y el acceso no autorizado a información que comprometen la integridad, autenticidad y confidencialidad de la información del sistema web educativo. Las partes interesadas logran el objetivo principal de la implementación de los controles de seguridad aumentando la calidad del producto entregable.

Debido al tiempo de entrega del producto final, no se pudieron realizar las pruebas en una versión estable del sistema web educativo online con mayor flujo de información, es por ello que estas se realizaron en un entorno offline, sin embargo, con base a los resultados obtenidos se puede concluir que, al implementar estas medidas de seguridad, el sistema

web educativo será seguro y fiable, es decir que la información contenida en él estará protegida de intrusos no deseados.

Conclusiones

La seguridad de los datos es importante para proteger la información, considerada como uno de los activos más importantes de la empresa u organización, además es importante e indispensable la implementación de un SGSI definido de acuerdo a los requerimientos de la empresa y de las leyes de la región para evitar problemas legales y pérdidas económicas.

Con base a los resultados obtenidos durante el desarrollo de este proyecto podemos concluir lo siguiente.

- Es importante investigar y adoptar un marco referencial sobre las mejores prácticas para el desarrollo de sistemas, antes de comenzar el desarrollar un sistema web.
- Es necesario hacer un análisis y evaluación de riesgos para implementar controles de seguridad de la información, con la finalidad de planificar los tiempos y determinar los requerimientos de desarrollo de un sistema, considerando la implementación de la seguridad de la información desde el inicio del desarrollo del software.
- Resulta indispensable agregar validaciones y controles de recuperación que protejan el sistema web ante fallos en la disponibilidad, independiente del sistema de seguridad de la información que se adapte.
- No se debe asumir que el usuario usará correcta y éticamente el sistema. Puede cometer errores al ingresar sus datos o puede jugar el rol de atacante y provocar un incidente de la seguridad de la información.
- Finalmente, de acuerdo con el resultado de la segunda y última etapa de desarrollo del proyecto, se concluye que los objetivos y requerimientos en la seguridad de la información fueron cubiertos adecuadamente, al no tener una respuesta negativa por parte de la empresa.

Referencias

[1] ISO/IEC (2005). *Norma ISO/IEC 27001:2005.*

[2] Consejo Superior de Administración Electrónica (2012). *Libro 1. Método*. Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V6jQ8_l97IU

[3] Consejo Superior de Administración Electrónica (2012). *Libro 3. Gua Técnica*. Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V6jQ8_l97IU

[4] ISO/IEC (2005). *Norma ISO/IECO 17799.*

[5] W. Stallings (2004). *Fundamentos de Seguridad en Redes. Aplicaciones y Estándares*. Madrid: Pearson Edicación.

[6] C. Tori (2008). *Hacking Ético*. Buenos Aires: Argetina.

[7] M. Mijail (2013). *SQL Inyection*. Obtenido de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100017&script=sci_arttext&tlng=en.

[8] Microsoft (2016). Inyección de código SQL. Obtenido de https://technet.microsoft.com/es-es/library/ms161953(v=sql.105).aspx.

[9] J. D. Chávez (2015). *Principios Basicos de la Seguridad en Bases de Datos*. Obtenido de https://www.researchgate.net/publication/279983428_Principios_Basicos_de_Seguridad_en_Bases_de_Datos.

[10] Apache (2016). Apache HTTP Server Tutorial: .htaccess files. Obtenido de https://httpd.apache.org/docs/2.4/howto/htaccess.html.

[11] X. W. y. H. Yu (2005). *How to break MD5 and Other Hash Functions*. Obtenido de http://download.springer.com/static/pdf/55/chp%253A10.1007%252F11426639_2.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F11426639_2&token2=exp=1456714810~acl=%2Fstatic%2Fpdf%2F55%2Fchp%25253A10.1007%25252F11426639_2.pdf%3ForiginUrl%3Dh.

[12] IFAI (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

[13] CISCO (2015). *Trampas de SNMP (Protocolo simple de gestión de redes) compatibles con IOS de Cisco y cómo configurarlas*. Obtenido de http://www.cisco.com/cisco/web/support/LA/102/1025/1025299_snmp_traps.pdf.