UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

"Trabajo de grado previo a la obtención del Título de Ingeniero en Sistemas y Computación."

TRABAJO DE GRADUACIÓN

Título del proyecto

ANÁLISIS DE VULNERABILIDADES DE SOFTWARE PARA MEJORAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS.

CASO PRÁCTICO: SISTEMA INFORMÁTICO PARA EL CEMENTERIO MUNICIPAL DE RIOBAMBA

AUTORES:

Jessica Janneth Valle Padilla

Marco Vinicio Gavidia Villacrés

Directora: Ing. Ana Congacha

Riobamba – Ecuador

2015

PÁGINA DE REVISIÓN

Los miembros del Tribunal de Graduación del proyecto de investigación de título "Análisis de vulnerabilidades de software para mejorar la seguridad en los sistemas informáticos. **Caso práctico:** sistema informático para el Cementerio Municipal de Riobamba" presentado por: Jessica Janneth Valle Padilla y Marco Vinicio Gavidia Villacrés, dirigida por: Ing. Anita Congacha.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Fernando Molina
Presidente del Tribunal

.....
Firma

Ing. Ana Congacha
Directora del Proyecto

.....
Firma

Ing. Danny Velasco
Miembro del Tribunal

.....
Firma

AUTORÍA DE LA INVESTIGACIÓN

"La responsabilidad del contenido de este Proyecto de Graduación, corresponde exclusivamente a los Srs. Jessica Janneth Valle Padilla y Marco Vinicio Gavidia Villacrés (autores) y del Ing. Ana Congacha (directora); y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.

Autora:

……..

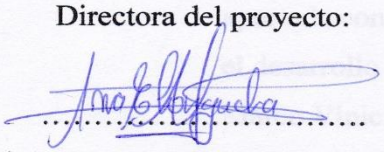
Jessica Janneth Valle Padilla

Autor:

……..

Marco Vinicio Gavidia Villacrés

Directora del proyecto:



……..

Ing. Anita Congacha

AGRADECIMIENTO

Agradezco a Dios porque él ha permitido culminar la carrera de la mejor manera a través de sus bendiciones, agradecimiento a mis padres y hermanos por brindarme siempre su apoyo y ejemplo de superación, agradezco también a todos mis amigos y compañeros de la promoción 2013-2014 de Ingeniería en Sistemas de la Universidad Nacional de Chimborazo por su apoyo intelectual y emocional ,a los estimados docentes de la Carrera de Ingeniería en Sistemas que han cumplido con su labor profesional sino también como amigos.

Un agradecimiento muy especial al Ing. Fernando Molina por su pertinente guía y apoyo, también a la Ingeniera Lady Espinoza Tutora del presente trabajo de investigación quien ha dirigido y aportado con tiempo y conocimientos para el desarrollo de este proyecto.

Marco Vinicio Gavidia Villacrés

DEDICATORIA

Dedico este trabajo de investigación fruto de mi esfuerzo a Dios porque la profesión que posee servirá para honrarlo y cumplir con su palabra, a mi esposa Carmita por el amor que me ha brindado, mi hija Emily, a mi Padre Julio, por su apoyo, a mi madre Gloria por el estímulo que me ha dado, a mis hermanas Myriam , Gabriela, Jacqueline y mis hermanos Fabián, Cristian quienes no solo han sido de ejemplo de vida sino que además han sido de motivación por brindarme su apoyo alegría, fortaleza y cada uno de mis amigos en especial Efraín, Daniel, Juan Carlos, Fabián, Luis, Juan Pablo, Gabriela Richard, Patty, que a través de sus palabras y experiencias han transmitidos

Marco Vinicio Gavidia Villacrés

AGRADECIMIENTO

Agradezco principalmente a Dios por haberme guiado por el camino de la felicidad, a mi director de esta tesis la Ing. Ana Congacha, por la dedicación y apoyo que ha brindado a este trabajo, por el respeto a mis sugerencias e ideas y por el rigor que ha facilitado a las mismas. También a mis Abuelitos, Margarita y Miguel por ser los mejores, a mis Padres Elvia y Enrique por haber estado conmigo, apoyándome en los momentos difíciles, por dedicar tiempo y esfuerzo para ser una mujer de bien, y darme excelentes consejos en mi caminar diario. A mis hermanos Alexandra y Wilmer que con su ejemplo y dedicación me han instruido para seguir adelante en mi vida profesional.

Jessica Janneth Valle Padilla

DEDICATORIA

El presente trabajo de tesis dedico principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A la UNIVERSIDAD NACIONAL DE CHIMBORAZO por darme la oportunidad de estudiar y ser un profesional. A mi madre Elvia, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones. A mis Abuelitos Margarita y Miguel, a pesar de la distancia siento que están conmigo siempre y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido tan especial para ustedes como lo es para mí. A mis hermanos Alexandra y Wilmer por haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Por último a mi familia porque a depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad.

Jessica Janneth Valle Padilla

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este proyecto consiste en el desarrollo de un sistema seguro para el Cementerio Municipal de Riobamba, mediante el estudio de tres vulnerabilidades más comunes que afectan las aplicaciones web: Inyección SQL, Secuencia de comandos cruzados (XSS) y la falsificación de sitios cruzados (CSRF). En primer lugar se ha realizado el análisis de diez vulnerabilidades de software que nos presentó la organización OWASP (Te Open Web Aplicación Security Project) sobre el análisis y la seguridad de las aplicaciones web.

El Cementerio Municipal de la ciudad de Riobamba maneja toda la información de catastro de: bóvedas particulares, bóvedas institucionales, nichos, mantenimiento de bóvedas y nichos de forma manual, la cual provoca una gran pérdida de tiempo al momento de registrar, buscar y modificar la información de alguna persona fallecidas, demás dicha búsqueda no siempre es exitosa. De igual forma conlleva a la confusión o pérdida de información al momento de trascribir los todos datos a una hoja de Excel.

Se estudian las vulnerabilidades según las características más comunes y peligrosas en el mundo para las cuales se implementó mecanismo de protección para disminuir el impacto en el sistema para el Cementerio Municipal de Riobamba.

Para el desarrollo del sistema se utilizó la metodología XP por ser la más adecuada para la ingeniería de software y las tecnologías de desarrollo web, los programas seleccionados fueron PHP y mysql por ser de código libre.

SUMARY

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CENTRO DE IDIOMAS

Lic. Geovanny Armas

19 de Marzo del 2015

SUMARY

This project is involved in the development of a safe system for the Municipal Cemetery of Riobamba by means of the study of three vulnerabilities which are the most common ones affecting web applications: SQL Injection, Cross Command Sequence (XSS) and cross site forgery (CSRF). First, the analysis of ten software vulnerabilities has been developed; it was presented by OWASP (Open Web Application Security Project) on analysis and security of web applications.

The Municipal Cemetery of Riobamba handles all registry information about: private vaults, institutional vaults, niches, manual maintenance of vaults and niches; this causes a huge waste of time when registering, searching and modifying information about a deceased person, and this search is not always successful. Similarly it leads to confusion or loss of information when transcribing all data to an Excel spreadsheet.

Vulnerabilities are studied according to the world's most common and dangerous characteristics for which a protection mechanism was implemented in order to reduce the impact on the system for the Municipal Cemetery of Riobamba.

For developing this system, some XP methodology was used because this is the most suitable for software engineering and web development technologies, the selected programs were PHP and MySQL since they are from open source.

OWASP ZAP testing tool is performed to check the existing vulnerabilities in the system and apply the mechanisms of protection for each of them.

In addition, with the development of the SGCMR system, it was possible to improve the registry and information management for the Municipal Cemetery of Riobamba.

CENTRO DE IDIOMAS

COORDINACION

INTRODUCCION

El proyecto está enfocado en el análisis de tres vulnerabilidades que se encuentran desarrollados en los siguientes capítulos.

Capítulo I.-Manifiesta el marco referencial del proyecto en el cual se muestra los problemas, su sistematización y la importancia de la investigación, para la cual se plantean objetivos que ayudan a alcanzar la solución del mismo.

Capítulo II.- Analiza la descripción actual de las vulnerabilidades de software. Para ello se da a conocer brevemente lo que es sistemas informáticos, seguridad informática, proyecto de seguridad de aplicaciones web abiertas (OWASP) como aporte principal de la investigación y las normas de seguridad.

Capítulo III.-Contempla el análisis para la selección de las vulnerabilidades más comunes que se toman en cuenta el nivel de riesgo que estos provocan en los sistemas informáticos.

Se desarrolla los mecanismos de protección ante las vulnerabilidades analizadas para reducir el nivel de riesgo que provocan estos.

También en este capítulo se contempla la selección de la metodología de desarrollo de software más adecuada para realizar el sistema para el Cementerio Municipal de Riobamba.

Capítulo IV.- Se desarrolla las metodologías de investigación donde se especifica que procedimientos se ha seguido para dar a conocer y aplicar la información recopilada.

Capitulo V.-Se presenta la recopilación, análisis y tabulación los datos para que puedan ser comprobarlos estadísticamente y de esa forma aceptar o rechazar la hipótesis.

Capítulo VI.- Se presentan las conclusiones y recomendaciones resultantes de la investigación con información muy importante y relevante así como también propuestas para mejorar el estudio y problema planteado.

Capítulo VII.-Se propone una alternativa de solución para la investigación la cual está sustentada teóricamente y para ser evaluada.

Capítulo VIII.- Se indica las fuentes bibliográficas ya sean estos libros, revistas, publicaciones o documentos web que sustentan la presente investigación.

El desarrollo del Sistema de Gestión para el Cementerio Municipal de Riobamba (SGCMR) permite realizar los procesos realizados en la institución de manera automatizada y con la seguridad ante vulnerabilidades que en la actualidad ponen en riesgo la confiabilidad e integridad de los sistemas informáticos o aplicaciones web.

CAPÍTULO I

MARCO REFERENCIAL

1.1 TÍTULO DEL PROYECTO

ANÁLISIS DE VULNERABILIDADES DE SOFTWARE PARA MEJORAR LA SEGURIDAD EN LOS SISTEMAS INFORMATICOS.
CASO PRÁCTICO: SISTEMA INFORMÁTICO PARA EL CEMENTERIO MUNICIPAL DE RIOBAMBA.

PROBLEMATIZACIÓN

La evolución de las Tecnologías de la Información y la Comunicación (TIC) ha sido un elemento clave para que exista un sin número de amenazas y riesgos, tanto en la web como en los Sistemas Informáticos.

En si la mayoría de empresas e instituciones poseen Sistemas Informáticos los cuales son afectados en el funcionamiento de sus activos como en la vulnerabilidad de su sistema por no tener implementadas herramientas, políticas y normas de seguridad .

El análisis de vulnerabilidades nos ayudará a la identificación de las distintas amenazas y riesgos de la información que posee un sistema, con el objetivo de implementar los controles necesarios para la seguridad de la información en disponibilidad, confidencialidad e integridad.

Además en la actualidad existe problemas con la seguridad web entre los más importantes son: Inyección Sql, Pérdida de Autenticación y Gestión de Sesión, Secuencia de Comandos en Sitios Cruzados (Mss.), Referencia Directa Insegura a Objetos, Configuración Defectuosa de Seguridad, La Exposición de Datos Sensibles, Falta Nivel de Función de Control de Acceso, Falsificación de Peticiones en Sitio Cruzado, Utilización de Componentes con Vulnerabilidades Conocidas, Sin Validar Redirecciones y Reenvíos no Validados.

IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA

La constante evolución tecnológica, el acceso a la información por medios informáticos inducen a escoger una sistemática adecuada que pueda resolver problemas que además cuente con la debida seguridad informática especialmente para los activos más importantes como son Software y Datos.

Desde el punto de vista del usuario, cuando se descubre una vulnerabilidad del software, lo más importante es saber cómo protegerse. En este sentido, son fundamentales las actualizaciones y parches de seguridad publicadas generalmente por los creadores de los programas informáticos.

Esto se ha considerado en el desarrollo de un sistema informático que cuente con las debidas seguridades en la parte de software principalmente para que el manejo de toda la información además de automatizarse sea seguro y confiable cómo será el caso en el desarrollo del sistema informático para el Cementerio Municipal de Riobamba.

1.1.1 ANÁLISIS CRÍTICO

Las empresas actualmente y constantemente son amenazadas en sus activos, para ello es necesario combatirlos y defenderlos de posibles ataques a la información.

La amenaza es como un escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático.

Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y el sistema informático esté en riesgo.

Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños cualitativos y cuantitativos, y esto se llama 'impacto'.

Al Integrar este análisis se puede decir “un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema, produce un impacto sobre él.

Si se quiere eliminar las vulnerabilidades del sistema informático o disminuir el impacto que puedan producir sobre él, se ha de proteger el sistema mediante una serie de medidas, las cuales se implementan en el sistema informático para el Cementerio Municipal de Riobamba.

1.1.2 PROGNOSIS

En la actualidad la mayor parte de las Instituciones del Gobierno necesitan automatizar sus procesos con el fin de mejorar la atención a la ciudadanía.

Con la implementación de un Sistema Informático para el Cementerio Municipal de Riobamba se podrá: tener el registro de la información de las personas fallecidas, registro de representantes legales, conocer la fecha exacta de las personas fallecidas, conocer el número de bóveda, nicho o sepultura.

El Sistema Informático tendrá la debida seguridad en software y estará protegido ante vulnerabilidades que son más comunes.

El sistema estará alojado en la internet junto con un sitio web sé que brindara información de importancia de la mencionada institución para el beneficio de la ciudadanía.

1.1.3 DELIMITACIÓN

La investigación para el desarrollo de software se limita al estudio de las siguientes vulnerabilidades que están enfocadas a los entornos web las mismas que se describen a continuación:

- ✓ Inyección Sql
- ✓ Pérdida de Autenticación y Gestión de Sesión
- ✓ Secuencia de Comandos en Sitios Cruzados (Mss.)
- ✓ Referencias Directa Insegura a Objetos
- ✓ Configuración Defectuosa de Seguridad
- ✓ La Exposición de Datos Sensibles
- ✓ Falta Nivel de Función de Control de Acceso
- ✓ Falsificación de Peticiones en Sitio Cruzado

- ✓ Utilización de Componentes con Vulnerabilidades Conocidas
- ✓ Sin Validar Redirecciones y Reenvíos no Validados.

De las vulnerabilidades mencionadas se va a seleccionar 3 vulnerabilidades para la investigación.

Las tecnologías de desarrollo que se va a utilizar para el nuevo sistema son:

- ✓ PHP
- ✓ Mysql

Este proyecto se desarrolla en el Cementerio Municipal de Riobamba que se encuentra ubicada en la Av. Nueve de Octubre y Santa Isabel la misma que no presenta ningún inconveniente en el acceso a sus instalaciones.

La construcción del Sistema Informático realizará los siguientes controles:

- ✓ Registro de la información de las personas fallecidas
- ✓ Registro de representantes legales
- ✓ Fecha exacta en que falleció
- ✓ Numero de bóveda, nicho o mausoleo en la que se encuentra sepultado.

Para pruebas del sistema en lo que se refiere a la seguridad se utilizaran herramientas de hacking, y para verificar los datos se va a ingresará el 10% del total de las personas fallecidas.

1.1.4 FORMULACIÓN DEL PROBLEMA

¿En qué forma las vulnerabilidades de software inciden en la seguridad del sistema informático para el Cementerio Municipal de Riobamba?

JUSTIFICACIÓN

La inseguridad en Tecnologías de la Información ha evolucionado en los últimos tiempos, en que los errores en los programas son los responsables de la inmensa mayoría de los incidentes de seguridad informática.

Por esta razón se pretende analizar las vulnerabilidades y escoger la más adecuada para resolver la seguridad Informática en el sistema del Cementerio Municipal de Riobamba.

Hoy en día todas las entidades gubernamentales necesitan proteger sus sistemas informáticos ya que son susceptibles de ser atacadas por hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella.

El Cementerio Municipal de Riobamba no cuenta con un sistema adecuado para el registro de toda la información de las personas fallecidas lo que imposibilita dar una mejor atención a la ciudadanía optimizar recursos.

Por eso se considera, importante generar un Sistema Informático vinculado a la Web, a través del cual se pueda acceder con facilidad a la información que necesite el usuario.

Por estas razones resulta necesario consolidar el sistema de información mediante un enfoque orientado hacia las autoridades, los técnicos, y todos aquellos usuarios que requieran esta información, con el apoyo del fortalecimiento y desarrollo institucional.

OBJETIVOS

1.1.5 GENERAL

Analizar las vulnerabilidades de Software para mejorar la seguridad en los Sistemas Informáticos.

1.1.6 ESPECÍFICOS

- ✓ Analizar las vulnerabilidades de los Sistemas Informáticos a nivel de Software
- ✓ Implementar los Mecanismos de Seguridad para las vulnerabilidades identificadas.
- ✓ Desarrollar un Sistema Informático seguro en el Cementerio Municipal de Riobamba.

CAPITULO II

FUNDAMENTACIÓN TEÓRICA

2.1 SEGURIDAD INFORMÁTICA

2.1.1 CONCEPTO

En la Real Academia Española el término seguro se refiere estar libre y exento de todo peligro, daño o riesgo. Este es el concepto que es aplicado a sistemas de información y sistemas informáticos.

Purificación Aguilera menciona que la seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. (Aguilera, 2010)

A pesar de las medidas de seguridad aplicadas siempre hay un margen de riesgo además para establecer dichas medidas es necesario hacerse ciertas interrogantes y tener conocimientos de lo siguiente:

- ✓ Cuáles son los elementos que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
- ✓ Cuáles son los peligros que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.
- ✓ Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico de revisión y actualización las medidas adoptadas. (Aguilera, 2010)

Todo elemento que posee un sistema informático puede ser afectado por fallos de seguridad y a los datos, por ello el software es un el factor más vulnerable.

2.1.2 TIPOS DE SEGURIDAD INFORMÁTICA

ACTIVA

(Aguilera, 2010) Menciona que el tipo de seguridad activa comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

PASIVA

(Aguilera, 2010) Concreta que el tipo de seguridad pasiva hace referencia a la integridad, confidencialidad y disponibilidad de los datos, estas son las propiedades que debe tener un sistema para considerarlo seguro.

Está formada por las medidas que se implantan para cuando se produce el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; para tener siempre al día copias de seguridad de los datos.

2.1.3 PROPIEDADES DE UN SISTEMA DE INFORMACIÓN SEGURO

Los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización.

Su origen puede ser:

Fortuito. Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistema, catástrofes naturales...

Fraudulento. Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

Se considera seguro un sistema que cumple con las propiedades de integridad, confidencialidad y disponibilidad de la información.

2.1.3.1 INTEGRIDAD

Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.

Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto.

2.1.3.2 CONFIDENCIALIDAD

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como: "el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada."

Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

2.1.3.3 DISPONIBILIDAD

La información está disponible para los usuarios autorizados cuando la necesiten.

El programa **MAGERIT**[1] es una metodología de análisis y gestión de riesgos de los sistemas de información**,** define a la disponibilidad como grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.

Situación que se produce cuando se puede acceder a un sistema informático en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información.

[1] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

2.1.4 SEGURIDAD DE LAS APLICACIONES WEB

La seguridad es un aspecto importante para proteger la integridad y privacidad de los datos y recursos de su aplicación Web. Debería designar una estrategia de seguridad para su aplicación Web, que use soluciones de seguridad de eficacia probada, e implementar métodos de autenticación, autorización y validación de datos, para proteger la aplicación de una serie de amenazas. (Resources.arcgis.com, 2010)

2.1.5 ISO/IEC 27032

La norma ISO/IEC 27032 fue publicada el 16 de Julio de 2012, facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo, ayuda a prepararse, detectar, monitorizar y responder a los ataques de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad. (ISO, 2014)

La ISO / IEC 27032 se centra en la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio". El "ciberespacio" se conoce como "el entorno complejo que resulta de la interacción de las personas, software y servicios a través de Internet por medio de dispositivos de tecnología y redes.

La gran variedad de riesgos de seguridad de la información están conectados con "el ciberespacio; tales como redes, la piratería del sistema, spyware, malware, cross-site scripting, inyección SQL, la ingeniería social, además de los problemas de seguridad de información, etc. (GoDaddy.com, 2014)

2.1.6 OWASP

Te Open Web Aplicación Security Project (OWASP) es una organización que proporciona un conjunto de conocimientos, técnicas y directrices sobre el análisis de la seguridad de las aplicaciones web. OWASP fue fundada en diciembre de 2001 y alcanzó en EE.UU. un estatus de organización benéfica sin fines de lucro en 2004. "Es un gran recurso para el aprendizaje y la fijación de la seguridad de la aplicación web.
El proyecto OWASP Top Ten ha sido un sub-proyecto de la fundación OWASP desde 2004. Las vulnerabilidades encontradas se han elegido a través de un consenso por los miembros del proyecto y expertos en seguridad a nivel mundial. La lista Top Ten es utilizado por un gran número de organizaciones comerciales y se ha convertido en un estándar para la seguridad de las aplicaciones web.

OWASP APPLICATION SECURITY VERIFICATION STÁNDAR (ASVS)

El objetivo principal de la Aplicación de Verificación de Seguridad Estándar del OWASP (ASVS) es la normalización de la gama de la cobertura y el nivel de rigor en el mercado cuando se trata de realizar la verificación de la seguridad de aplicaciones Web se utiliza un estándar abierto comercialmente viable.
El estándar proporciona una base para probar los controles de aplicación técnica de seguridad, así como todos los controles técnicos de seguridad en el medio ambiente, que se basó en proteger vulnerabilidades como Cross-Site Scripting (XSS) y la inyección de SQL. Esta norma se puede utilizar para establecer un nivel de confianza en la seguridad de las aplicaciones Web.
OWASP Top 10 es un proyecto dedicado a seleccionar las vulnerabilidades más riesgosas para la seguridad de aplicaciones web, mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones.

2.2 VULNERABILIDAD

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquier elemento de una computadora, tanto en el hardware, el sistema operativo, como en el software.

La vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una Amenaza sobre dicho Activo. La vulnerabilidad es una propiedad de la relación entre Activo y una Amenaza.

2.2.1 VULNERABILIDADES DE SOFTWARE

El término 'vulnerabilidad' se refiere a la violación de una política de seguridad. Esto puede deberse a reglas de seguridad inadecuadas o a problemas dentro del mismo software. En teoría, todos los sistemas de ordenadores tienen vulnerabilidades, cuya seriedad depende que sean o no usados para causar un daño al sistema.

Una vulnerabilidad universal es un estado en un sistema de ordenadores o un grupo de sistemas que:

- ✓ Permite que un atacante ejecute órdenes como otro usuario
- ✓ Permite que un atacante tenga acceso a los datos de acceso restringido
- ✓ Permite que un atacante hacerse pasar por otra entidad
- ✓ Permite que un atacante conduzca una denegación de servicio.

Una exposición es un estado en un sistema de ordenadores (o grupo de sistemas) que no es una vulnerabilidad universal, pero:

- ✓ Permite que un atacante reúna información sobre las actividades del sistema
- ✓ Permite que un atacante disimule sus actividades

2.2.2 TIPOS DE VULNERABILIDADES DE SOFTWARE

A1 – Inyección SQL: Corresponde a la inyección de código y es una de las más comunes.

A2 –P*érdida de Autenticación y Gestión de Sesión*: Corresponde al mal manejo de las sesiones en diferentes aplicaciones.

A3 –Secuencia de Comandos en Sitios Cruzados: Ocurre cuando existe validación de la información ingresada por el atacante.

A4 – Referencia Directa Insegura a Objetos: Ocurre cuando un desarrollador expone información la cual puede ser manipulada por un atacante que puede acceder a datos que no están autorizados.

A5 – Configuración de Seguridad Incorrecta : Corresponde a configuraciones no adecuadas que pueden impactar en la seguridad de la propia aplicación.

A6 – Exposición de Datos Sensibles: Se refiere a la protección incorrecta de datos críticos tales como: números de tarjetas de crédito, contraseñas, entre otros las cuales pueden ser remplazadas, modificadas o robas.

A7 – Ausencia de Control de Acceso a Funciones: Corresponde a la falta de controles desde el servidor, para permitir un posible atacante, acceder a funciones a las que no está autorizada.

A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF): Permite a un atacante generar peticiones sobre una aplicación vulnerable a partir de la sesión de la víctima.

A9 - Utilización de Componentes con Vulnerabilidades Conocidas: Corresponde a la explotación de librerías, framework y otros componentes vulnerables por parte de un atacante con el fin de obtener acceso o tener un impacto grave en el servidor.

A10 – Redirecciones y Reenvíos no Validados: Ocurre cuando los atacantes aprovechan el uso de redirecciones de sitios web a otros sitios en el momento de utilizar información no confiable para redirigir a las víctimas a sitios de phishing o que contienen malware.

Tabla 1. Actualización de vulnerabilidades 2010 a 2013

OWASP TOP 10 -2010 (ANTERIOR)	OWASP TOP 10 -2013 (NUEVO)
A1 - Inyección (inyección sql)	A1-injection (inyección sql)
A3 - Broken Authentication and Session Management Pérdida de Autenticación y Gestión de Sesión	A2 - Broken Authentication and Session Management Pérdida de Autenticación y Gestión de Sesión
A2 - Cross-Site Scripting (xss) Secuencia de comandos en Sitios Cruzados	A3 - Cross-Site Scripting - Secuencia de Comandos en Sitios Cruzados
A4 – Insecure Direct Object References - Referencias directa insegura a objetos	A4 – Insecure Direct Object References - Referencias Directa Insegura a Objetos
A6 – Security Misconfiguration - Configuración Defectuosa de Seguridad	A5 – Security Misconfiguration - Configuración Defectuosa de Seguridad
A7 - Insecure Cryptographic Storage – Fusionada con a9 →	A6 - Sensitive Data Exposure - Exposición de Datos Sensibles
A8 – Failure to Restrcict Url Access – ampliado en →	A7- Missing Functionlevel Access Control - Falta de función que controla el nivel de acceso.
A5 – Cross-Site Request Forgery (CSRF) Falsificación de Peticiones de Sitios Cruzados	A8 – Cross-Site Request Forgery (CSRF) Falsificación de Peticiones de Sitios Cruzados
<enterrado en A6:Security Misconfiguration - - Configuración Defectuosa de Seguridad >	A9 – Using Known Vulnerable Components
A10 - Unvalidated Redirects and Forwards - Redirecciones y Destinos Inválidos	A10 - Unvalidated Redirects and Forwards - Redirecciones y Destinos Inválidos
A9-Insufficeint Transport Layer Protection insuficiente protección de la capa de transporte	Funcionada con 2010-A7 en un nuevo 2013-A6

Fuente: OWASP. (2013). Owasp Top 10-2013 rcl.

Adaptado por: Gavidia Marco & Jessica Valle

2.2.2.1 INYECCIÓN SQL

Definición

"SQL Injection" es el ataque contra un Gestor de Bases de Datos Relacional que aprovecha la vulnerabilidad de una aplicación cliente del mismo.

La finalidad del ataque es realizar tareas sobre la base de datos y de ser posible sobre host mismo, tener resultados indeseables e inesperados que van desde la alteración de un dato hasta apoderarse del servidor.

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

La inyección de código implica la explotación de una vulnerabilidad causada por el procesamiento de datos no válidos, y puede ser utilizada para cambiar un comportamiento o flujo de ejecución. Para realizar estos ataques, es común emplear un proxy local que capture las transacciones entre el navegador y el servidor web, para que puedan ser manipuladas antes de salir del sistema.

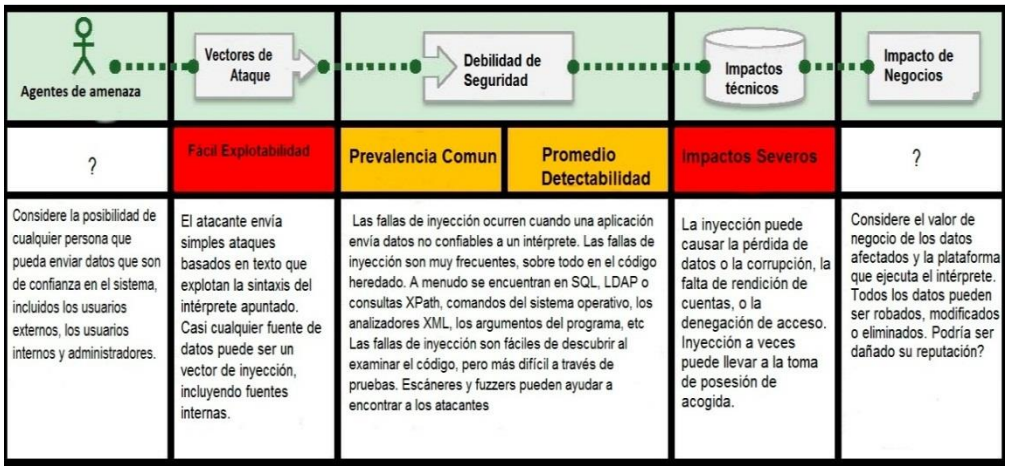


Figura 1.Características de la Vulnerabilidad de Inyección SQL

Fuente: OWASP (2013).Imagen de las características de inyección sql en sitios cruzados de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ La mejor manera de saber si una aplicación es vulnerable a la inyección Sql se debe utilizar variables **bind** (sentencias de control de SQL) en todas las sentencias preparadas y procedimientos almacenados, para evitar consultas dinámicas.
- ✓ La comprobación del código es una forma rápida y precisa para ver si la aplicación es segura. Las herramientas de análisis de código pueden ayudar a realizar pruebas de penetración, que confirman la vulnerabilidad. Los scanners no siempre pueden llegar al código para detectar si existe inyección sql.
- ✓ La gestión pobre de errores hace que los errores de inyección sean fáciles de descubrir. (OWASP, Owasp Top 10-2013 rcl, 2013, pág. 8)

RECOMENDACIONES (Publica, 2012)

- ✓ Para evitar este tipo de ataques se basa en la regla máxima sobre seguridad: Nunca confiar en los datos recibidos por el usuario.
- ✓ La modificación de parámetros de entrada por URL puede mostrar errores pero no descriptivos acerca de datos técnicos, es decir, se debe notificar al usuario de los errores producidos pero mediante mensajes personalizados.
- ✓ Los parámetros de entrada por URL serán correctamente filtrados y al modificarlos con texto en formato SQL no permitirá alterar la funcionalidad original.
- ✓ La modificación de parámetros de formularios puede mostrar errores, es decir, se debe notificar al usuario de los errores producidos mediante mensajes personalizados.
- ✓ Los parámetros de entrada en formularios serán correctamente filtrados y al modificarlos con texto en formato SQL no permitirá alterar la funcionalidad original.
- ✓ Cualquier parámetro recibido, ya sea por método GET o POST (u otro si se usan más comandos HTTP) debe ser filtrado para, eliminar caracteres

especiales o rechazar completamente su contenido si se detecta un contenido potencialmente peligroso.

- ✓ Se deberá filtrar todos los caracteres especiales que puedan ser tratados de forma diferente en lenguajes Java Script, SQL o cualquiera que se es va a utilizar para el funcionamiento del portal.
- ✓ Si los datos recibidos pueden ser devueltos al usuario en formato HTML se deberán filtrar los caracteres "<" y ">" o si es posible eliminar completamente o filtrar todas las etiquetas HTML que contenga el texto a excepción de las de formato de mensaje.
- ✓ Se recomienda igualmente aplicar las características propias del motor de los lenguajes aplicados al portal, para activar el escape de caracteres.
- ✓ Si los datos recibidos pueden ser almacenados, aunque sea de forma temporal en una base de datos se deberán filtrar los caracteres de comillas simples y dobles y posiblemente alguno más en función del gestor de base de datos utilizado. Es recomendable utilizar la documentación del gestor de base de datos que siempre suelen acompañar una información al respecto del juego de caracteres soportado.
- ✓ Los parámetros de entrada por URL serán correctamente filtrados y al insertar texto en formato script (como Java Script) no se mostrará de vuelta en la página.
- ✓ Los parámetros de entrada en formularios serán correctamente filtrados y al insertar texto en formato script (como Java Script) no se muestra de vuelta en la página.
- ✓ Para evitar potenciales problemas con el Java Script (u otros lenguajes de script), se deberán filtrar los caracteres "<" y ">" o si es posible eliminar completamente o filtrar todas las etiquetas HTML que contenga el texto a excepción de las de formato de mensaje.

2.2.2.2 PÉRDIDA DE AUTENTICACIÓN Y GESTIÓN DE SESIÓN

DEFINICIÓN

Esta vulnerabilidad se preocupa de la seguridad a los usuarios. Se puede permitir que un atacante suplante la información de un determinado usuario, se puede llegar a obtener una cuenta de administración que le permita sabotear los controles de autorización y registro de la aplicación.

La autenticación de usuario en la web que normalmente implica el uso de un ID, incluso hasta el cambio de contraseña, olvidado mi contraseña, recordar mi contraseña, actualización de cuenta, y otras funciones relacionadas. (OWASP, OWASP Top Ten 2013 Proyect, 2013)

Los tokens de sesión no están debidamente protegidos, un atacante puede secuestrar una sesión activa y asumir la identidadde un usuario.

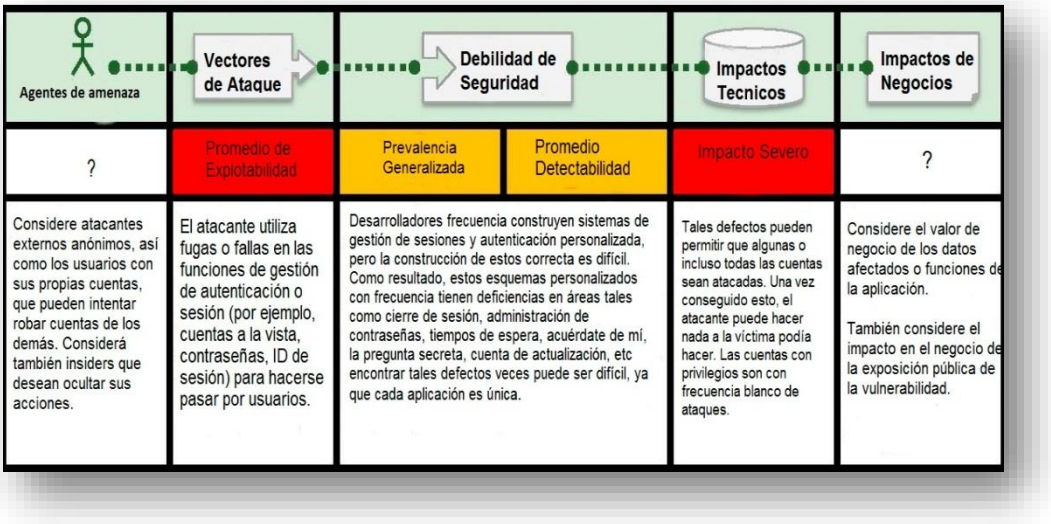


Figura 2. Características pérdida de autenticación-gestión de sesión

Fuente: *OWASP(2013).*Imagen de las características de perdida y autenticación y gestión de sesión de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ Credenciales de autenticación de usuario no están protegidos cuando se almacena un hash o cifrado.
- ✓ Identificadores de sesión se exponen en la URL (por ejemplo, la reescritura de URL).
- ✓ Identificadores de sesiones de usuario o tokens de autenticación, no se invalidan correctamente durante la sesión.

RECOMENDACIONES (Publica, 2012)

- ✓ No habrá referencias a identificadores de sesión en la URL.
- ✓ Iniciar sesión, por defecto su validez debe ser como máximo hasta el cierre del navegador (o la duración que haya especificado el usuario).
- ✓ Se debe iniciar sesión, siempre mediante conexiones seguras y cifradas (protocolo HTTPS).
- ✓ Para iniciar sesión, dos sesiones independientes deben tener identificadores distintos y no relacionados entre sí.

Las sesiones deben ser tratadas con el máximo cuidado posible. El secuestro de sesiones mediante el filtrado de las comunicaciones es un ataque bastante común de consecuencias muy graves ya que permite la suplantación completa de un usuario con los mismos roles de seguridad y permisos de acceso que tuviese el usuario legítimo.
Su creación, a través de la autenticación de credenciales procedentes del usuario debe realizarse siempre al utilizar un canal seguro para evitar la interceptación de las comunicaciones, como por ejemplo HTTPS y el uso de certificados de confianza.

A partir de ese momento, toda la identificación del usuario frente al portal debe reducirse a la mínima expresión, es recomendable tener un único identificador aleatorio alfanumérico almacenado en una cookie de forma que sea transparente para el usuario. Dicha cookie debe cumplir que:

- ✓ Sea lo suficientemente larga y aleatoria para que sea imposible averiguar el algoritmo de creación y secuestrar sesiones.

- ✓ Normalmente su generación está delegada según la tecnología que se vaya a utilizar (PHP, Java, ASP...) pero se suele poder reforzar la modificación de la semilla para la generación de números aleatorios.
- ✓ Su caducidad debe ser a nivel de sesión a menos que se habilite una opción para especificarla. En ese último caso los valores recomendados no deberían superar las 3 horas de inactividad del usuario excepto en casos justificados.
- ✓ La finalización de la sesión debe destruir cualquier cookie que se haya generado en el inicio de la misma, independientemente de la caducidad que se haya marcado.
- ✓ Debe estar marcada mediante los atributos "secure" y "http Only" para que los navegadores modernos lo interpreten correctamente y añada opciones de seguridad extra para que las cookies sensibles tengan el mínimo riesgo.

2.2.2.3 SECUENCIA DE COMANDOS EN SITIOS CRUZADOS (XSS)

Los ataques de cross- site scripting (XSS) ocurren cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario diferente. (OWASP, OWASP Top Ten 2013 Proyect, 2013).

Un atacante puede utilizar XSS para enviar un script malicioso a un usuario desprevenido.

El navegador del usuario final no tiene manera de saber que el script no es de confianza, y este se ejecutará.

Porque piensa que el script llegó de una fuente confiable, el script malicioso puede tener acceso a las cookies, los tokens de sesión u otra información sensible. Estos scripts pueden incluso volver a escribir el contenido de la página HTML. (Asesoriait.com, 2013).

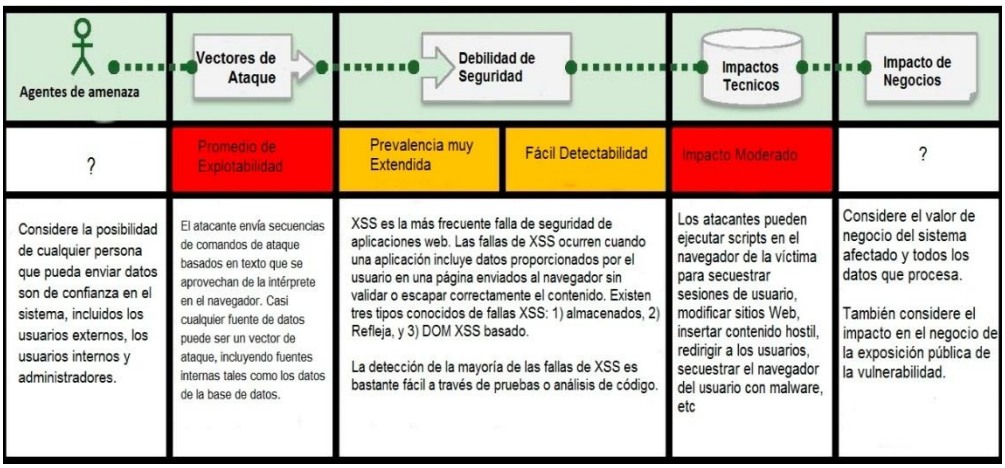


Figura 3. Vulnerabilidad de Secuencia de comandos en sitios cruzados

Fuente: *OWASP(2013).*Imagen de las características pérdida de secuencia de comandos en sitios cruzados de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ Las herramientas Automatizadas pueden encontrar algunos problemas XSS automáticamente. Sin embargo, cada aplicación genera páginas de salida diferente y utiliza diferentes intérpretes del lado del navegador, tales como Java Script, ActiveX, Flash, y Silverlight, lo que hace difícil la detección automatizada.
- ✓ Por lo tanto, la cobertura completa requiere una combinación de revisión de código manual y pruebas de penetración, además de métodos automatizados.
- ✓ Tecnologías de la Web2.0, como AJAX, hacen XSS mucho más difícil de detectar través de herramientas automatizadas. (OWASP, Owasp Top 10-2013 rcl, 2013, pág. 10)

RECOMENDACIONES (Publica, 2012)

- ✓ Los parámetros de entrada por URL serán correctamente filtrados y al insertar texto en formato script (como Java Script) no se mostrará de vuelta en la página.

- ✓ Los parámetros de entrada en formularios serán correctamente filtrados y al insertar texto en formato script (como Java Script) no se muestra de vuelta en la página.
- ✓ Al igual que con los fallos de tipo inyección, los problemas derivados de XSS se pueden evitar con un correcto filtrado de todos los datos de entrada procedentes de los usuarios.
- ✓ Para evitar potenciales problemas con el Java Script (u otros lenguajes de script), se deberán filtrar los caracteres "<" y ">" o si es posible eliminar completamente o filtrar todas las etiquetas HTML que contenga el texto a excepción de las de formato de mensaje.
- ✓ También es posible mostrar los caracteres problemáticos con una codificación equivalente en entidades mediante su correspondiente código como &#xxxx; o & en lugar de &.
- ✓ Se recomienda el uso de cortafuegos de aplicaciones web (WAF), que además sea capaz de generar una respuesta activa frente a posibles ataques. Dicha respuesta, debe incluir en todo caso la posibilidad de excluir las direcciones IP's correspondientes a la conexión originaria del ataque.

2.2.2.4 REFERENCIAS DIRECTA INSEGURA A OBJETOS

DEFINICIÓN

Las referencias directa insegura a objetos es cuando el acceso a los datos / activos sensibles no está totalmente protegidos y objetos de datos son expuestos por la aplicación con el supuesto de que el usuario siempre seguirá las reglas de aplicación.

La identificación de esta vulnerabilidad es un poco más difícil el uso de herramientas de automatización que otros puntos vulnerables porque para aprovechar esta vulnerabilidad no sólo es necesario identificar los defectos de la interfaz, sino también es necesario predecir el patrón para identificar un objeto seguro como los ficheros, etc.

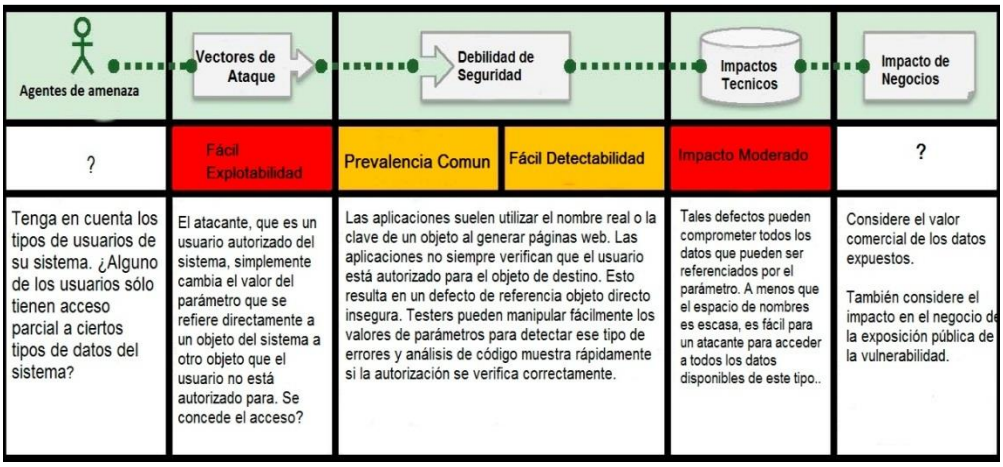


Figura 4. Características-vulnerabilidad de referencias directas inseguras a objetos

Fuente: *OWASP(2013).*Imagen de las características-vulnerabilidad de referencias directas inseguras a objetos de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ Para las referencias directas, la aplicación necesita verificar el usuario que está autorizado para acceder a los recursos exactos que han solicitado.
- ✓ Si la referencia es una referencia indirecta, la asignación a la referencia directa debe limitarse a los valores autorizados para el usuario actual.
- ✓ La revisión de código de la aplicación se puede verificar rápidamente si uno u otro enfoque se implementa de forma segura.
- ✓ Las pruebas también son eficaces para la identificación de las referencia a objetos directos y si son seguros. Las herramientas automatizadas normalmente no buscan ese tipo de errores porque no pueden reconocer lo que requiere protección o lo que es seguro o inseguro. (OWASP, Owasp Top 10-2013 rcl, 2013, pág. 11)

RECOMENDACIONES (Publica, 2012)

- ✓ Si hay valores personales de usuario por URL, su cambio no debe permitir visualizar datos de otros usuarios.
- ✓ Si hay valores personales de usuario por "cookies", su cambio no debe permitir visualizar datos de otros usuarios.
- ✓ A la hora de realizar el diseño de un portal es recomendable aplicar siempre la directriz de denegación por defecto.
- ✓ El acceso a cualquier recurso estará prohibido a menos que se autorice explícitamente a un usuario que pueda visualizarlo. De este modo se oculta mucha información a un posible atacante y es más robusto frente a errores humanos que pudiesen desvelar datos sensibles.

2.2.2.5 CONFIGURACIÓN DEFECTUOSA DE SEGURIDAD

DEFINICIÓN

Una mala configuración de seguridad puede ocurrir a cualquier nivel de un conjunto de aplicaciones, incluyendo la plataforma, servidor web, servidor de aplicaciones, el marco y el código personalizado.

Los desarrolladores y los administradores de red deben trabajar juntos para asegurar que toda la pila está correctamente configurada.

Los escáneres automáticos son útiles para detectar los parches faltantes, errores de configuración, el uso de las cuentas por defecto, los servicios innecesarios, etc. (Cyberintruder.com, 2013).Esto sucede principalmente cuando el administrador de sistema, administradores de bases de datos y los desarrolladores dejan agujeros de seguridad en la configuración de los sistemas informáticos.

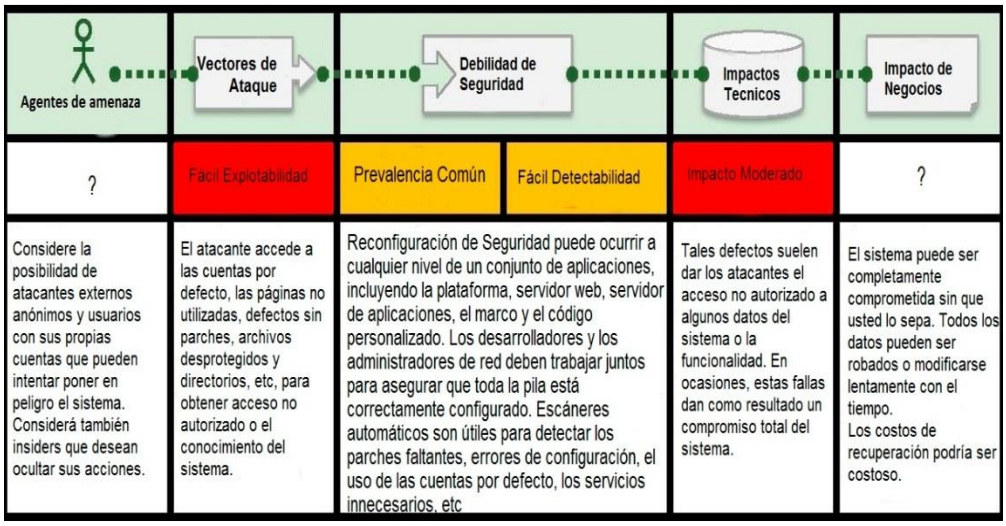


Figura 5. Configuración defectuosa de seguridad

Fuente: *OWASP(2013).*Imagen de las configuración defectuosa de seguridad de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ No realizar el adecuado refuerzo de la seguridad en toda la pila de aplicaciones.
- ✓ No tener un proceso para mantener todo el software actualizado. Esto incluye el IOS, Web / App Server, DBMS, las aplicaciones y las bibliotecas de código.
- ✓ Tener todo innecesariamente deshabilitado, eliminado o no instalado (por ejemplo, puertos, servicios, páginas, cuentas, privilegios.
- ✓ Tenerlas contraseñas de cuentas por defecto, cambiadas o desactivadas.
- ✓ Tener el tratamiento de errores configurado para evitar seguimientos de pila u otros y dejar que se escape mensajes de error demasiado informativos.
- ✓ No tener ajustes de seguridad en su desarrollo de framework (por ejemplo, Struts, Spring, ASP.NET) y bibliotecas entendidas además configurados incorrectamente.
- ✓ Se requiere un proceso tenso-repetible para desarrollar y mantener una correcta configuración de seguridad de aplicaciones. (OWASP, Owasp Top 10-2013 rcl, 2013, pág. 12)

RECOMENDACIONES (Publica, 2012)

- ✓ Sólo serán accesibles los servicios relevantes en los puertos del servidor para ofrecer la funcionalidad deseada.
- ✓ Sólo serán accesibles los servicios relevantes por URL en el servidor para ofrecer la funcionalidad deseada.
- ✓ Tan importante es el desarrollo como el software sobre el que se apoya, tanto en librerías que ofrecen funcionalidades adicionales como con los servidores a los que accede. Es recomendable leer la documentación de todos aquellos programas adicionales que se utilicen para realizar una configuración de seguridad efectiva ya que la mayoría ofrecen por defecto unos valores pobres. Por ejemplo, el servidor de base de datos MySQL no tiene asociada una contraseña para su usuario administrador.
- ✓ Del mismo modo, para aquellas librerías o módulos de los que haga uso la aplicación deberán estar correctamente actualizados. Es común que se encuentren vulnerabilidades en ellas y sean corregidas con diligencia por los responsables de las mismas.
- ✓ Es responsabilidad del equipo de desarrollo hacer uso de las últimas versiones de dichas librerías y adaptar la aplicación a cada nueva versión correctiva que aparezca.
- ✓ Se recuerda que deben aplicarse, al menos, las reglas bastionado de un servidor, a saber: mínimos privilegios posibles, mínimo punto de exposición, y defensa en profundidad.

2.2.2.6 LA EXPOSICIÓN DE DATOS SENSIBLES

DEFINICIÓN

Sistemas de TI suelen guardar la información personal de un usuario de base de datos como contraseñas, números de tarjetas de crédito, dirección de casa', número de teléfono, el número de identificación, etc.

Cuando el sistema no está protegido del acceso no autorizado efectivamente existe una alta probabilidad de que un hacker podría explotar esta vulnerabilidad y robar esa información. Esa vulnerabilidad es "la exposición de información confidencial".

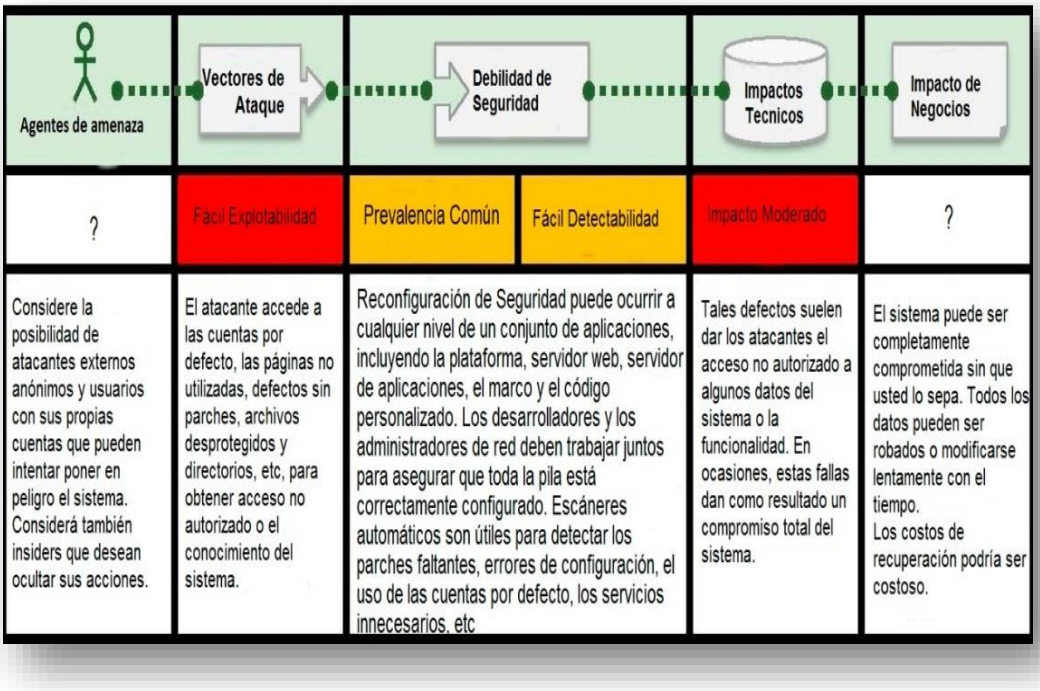


Figura 6. Características de la vulnerabilidad de exposición de datos sensibles

Fuente: *OWASP (2013).*Imagen de las características de la vulnerabilidad de exposición de datos sensibles de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ Cifrar toda cosa que se almacene a largo plazo, incluyendo copias de seguridad de estos datos.
- ✓ Encriptar contraseñas tanto interna como externamente. Todo el tráfico de internet debe ser encriptado.
- ✓ Algoritmo fuerte de cifrado se utilizan para todos lo script o claves criptográficas fuertes son generadas, y gestión de claves es correcta en el lugar, incluyendo la rotación de claves.

- ✓ Dar directivas de navegador adecuados las establezcan cabeceras para protegerlos datos confidenciales proporcionado para enviar al navegador. (OWASP, Owasp Top 10-2013 rcl, 2013, pág. 13)

RECOMENDACIONES (Publica, 2012)

- ✓ En caso de permitir inicio de sesión a los usuarios, la recuperación de la contraseña no expone ningún dato personal como dirección de correo y sólo permite modificarla sin poder conocer su valor original.
- ✓ Cualquier información sensible que se encuentre almacenada en el sistema deberá estar cifrada. Si se trata únicamente de datos de comprobación, es decir, que no van a ser transmitidos a ninguna otra entidad o sistema como puede ser una contraseña de acceso, deberá ser cifrada con un algoritmo hash preferiblemente SHA1.
- ✓ Si se trata de datos sensibles pero necesarios para interactuar con otras aplicaciones o servicios como puede ser un número de tarjeta de crédito, deberán estar correctamente cifrados al utilizar algún sistema de criptografía simétrica convenientemente implementado para que la clave secreta nunca salga de la aplicación

2.2.2.7 FALTA DE FUNCIÓN QUE CONTROLA EL NIVEL DE ACCESO

DEFINICIÓN

Prácticamente todas las aplicaciones web verifican los derechos de acceso de nivel de la función antes de que la funcionalidad visible en la interfaz de usuario. Sin embargo, las aplicaciones tienen que realizar las mismas comprobaciones de control de acceso en el servidor cuando se accede a cada función. Si no se verifican peticiones, los atacantes serán capaces de forjar peticiones con el fin de acceder a la funcionalidad no autorizada.

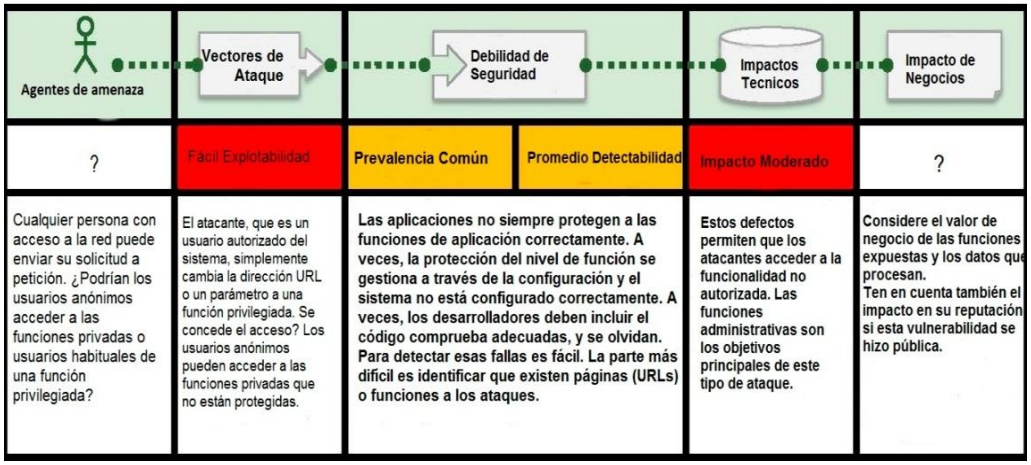


Figura 7. Vulnerabilidad de Falta de función que controla el nivel de acceso

Fuente: *OWASP (2013).*Imagen de las vulnerabilidad de vulnerabilidad de Falta de función que controla el nivel de acceso de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

La mejor manera de saber si una aplicación no ha logrado restringir adecuadamente la función de nivel de acceso es verificar todas las funciones de la aplicación:

- ✓ Que muestra el interfaz de usuario de navegación funciones no autorizadas.
- ✓ Que sea adecuada la comprobación de autenticación.
- ✓ Que sea adecuada la comprobación de autorización.
- ✓ Que los controles efectuados en el servidor no tengan que depender de la información proporcionada por el atacante.
- ✓ El uso de un proxy, navegar por la aplicación con un papel privilegiado. A continuación, volver a las páginas restringidas mientras está conectado como un papel menos privilegiado.
- ✓ También puede comprobar la aplicación de control de acceso en el código. Trate de seguir una única solicitud privilegiado a través del código
- ✓ Verificar el patrón de autorización.

PREVENCIÓN SEGÚN OWASP

Su aplicación debe tener un módulo de autorización coherente y fácilmente analizables que se invoca desde todas sus funciones comerciales.

Con frecuencia, esta protección es proporcionada por uno o más componentes externos al código de la aplicación.

- ✓ Se debe pensar en el proceso de gestión de derechos y asegurarse de que se puede actualizar y auditar fácilmente. Sin codificar.
- ✓ El mecanismo de aplicación (s) se debe negar el acceso de forma predeterminada, lo que requiere otorgamientos explícitos a las funciones específicas de acceso a todas las funciones.
- ✓ Si la función está involucrada en un flujo de trabajo, se debe comprobar que las condiciones estén en el estado adecuado para permitir el acceso.

2.2.2.8 FALSIFICACIÓN DE PETICIONES EN SITIO CRUZADOS

DEFINICIÓN

La forma más común y eficaz para prevenir un ataque CSRF es integrar un código secreto, que llamo un csrf token, única para cada sesión, en todas sus formas y en cada botón. Cualquier solicitud que entra tiene que tener ese código o sino será rechazado.
No hay manera de que un script de otro sitio para obtener el código, más de lo que puede obtener de la sesión, debido a la política de mismo origen (same-origin policy (SOP)) forzada por el navegador, el que impide que el código de un sitio de lectura de salida de otro. (Marc, 2013, pág. 197)

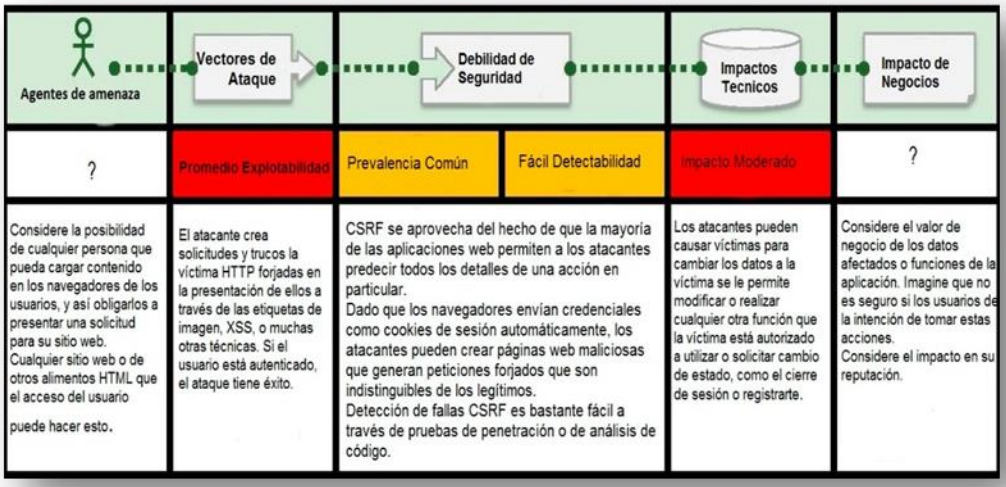


Figura 8. Vulnerabilidad de falsificación de peticiones en sitio cruzados

Fuente: *OWASP (2013).*Imagen de las vulnerabilidad de falsificación de peticiones en sitio cruzados de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ Debe centrarse en los vínculos y formas que invocan funciones estatales cambiantes, ya que esos son los objetivos más importantes de CSRF.
- ✓ Usted debe verificarlas operaciones de varios pasos, ya que no son intrínsecamente inmunes. Los atacantes pueden falsificar fácilmente una serie de peticiones con múltiples etiquetas o posiblemente de Java Script.
- ✓ Tenga en cuenta que las cookies de sesión, direcciones IP de origen, y otra información enviada automáticamente por el navegador no cuenta ya que esta información también se incluye en las solicitudes falsificadas. (OWASP, Owasp Top 10-2013 rcl, 2013, pág. 15)

RECOMENDACIONES (Publica, 2012)

- ✓ No se crearán peticiones por URL que realicen una acción funcional completa.
- ✓ No se crearán peticiones por formulario que realicen una acción funcional completa.
- ✓ Esta clase de ataques de invocación de peticiones fraudulentas es muy común y sencillo de explotar y por desgracia rara vez los portales se encuentran protegidos contra él.
- ✓ Es necesario poder distinguir entre una petición legítima del usuario y una fraudulenta de un atacante realizada en nombre del usuario. La medida de prevención más simple, aunque no muy efectiva, es la comprobación del origen de la petición a través de las cabeceras HTTP que envían los navegadores. Lamentablemente dicho origen también es fácilmente suplantable.
- ✓ La solución ideal consiste en crear "tokens" de petición de modo que cualquier acción, ya sea en enlace o en solicitud contra el portal, incluya un "token" generado dinámicamente y que el portal al recibirla sea capaz de comprobar su validez y autenticidad.
- ✓ Existen múltiples maneras de implementar una solución como ésta, pero la más sencilla es mantener en un sistema de almacenamiento como una base de datos, una caché de "tokens" generados aleatoriamente en tiempo de ejecución asociados a cada petición que se muestre al usuario, de forma que pueda comprobarlo fácilmente una vez recibidos. Evidentemente los token serían de un único uso y desechables.
- ✓ El escenario ideal sería que no se pudiera invocar ninguna acción desde un entorno ajeno al portal, pero las de consulta no serían peligrosas a menos que estén en combinación con otro fallo de seguridad de inyección o XSS.

2.2.2.9 UTILIZACIÓN DE COMPONENTES CON VULNERABILIDADES CONOCIDAS

DEFINICIÓN

Componentes, tales como bibliotecas, marcos, y otros módulos de software, casi siempre se ejecutan con privilegios completos. Si se explota un componente vulnerable, como un ataque puede facilitar la pérdida de datos importantes o toma de control del servidor.

Las aplicaciones que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de aplicación y permitir una serie de posibles ataques e impactos.

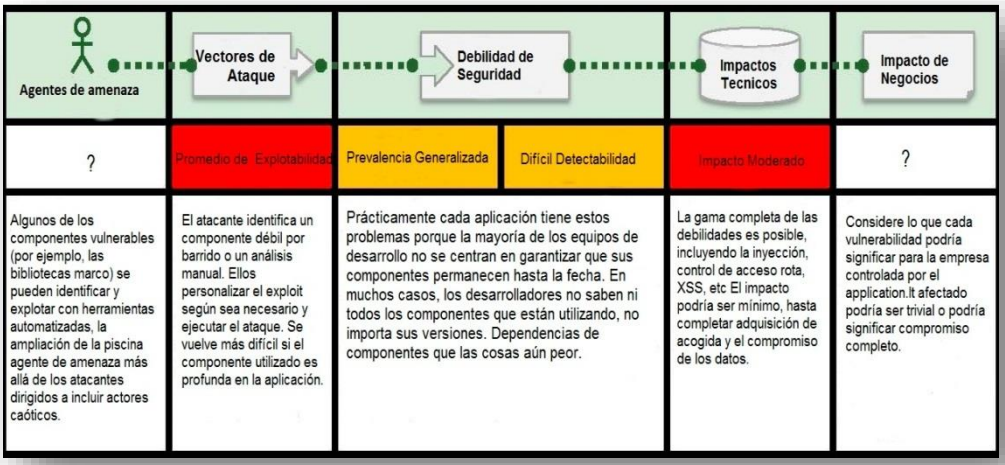


Figura 9. Utilización de componentes con vulnerabilidades conocidas

Fuente: *OWASP (2013).*Imagen de las vulnerabilidad utilización de componentes con vulnerabilidades conocidas de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

PREVENCIÓN SEGÚN OWASP

Muchos proyectos de código abierto (y otras fuentes de componentes) no crean parches de vulnerabilidad para las versiones antiguas. En su lugar, la mayoría simplemente solucionar el problema en la próxima versión.

Los proyectos de software deben tener un proceso para:

- ✓ Identificar los componentes y sus versiones, incluyendo todas las dependencias. (por ejemplo, el plug-inversiones).
- ✓ Velar por la seguridad de estos componentes en bases de datos pública, lista de correo del proyecto, y las listas de correo de seguridad y mantenerlos al día.
- ✓ Establecer políticas de seguridad que rigen el uso de componentes, como la exigencia de ciertas prácticas de desarrollo de software, pasar por las pruebas de seguridad, y las licencias aceptables.

RECOMENDACIONES (Publica, 2012)

- ✓ Todas las comunicaciones que contengan datos sensibles para el usuario deberán hacer uso de cifrados como SSL (HTTPS).
- ✓ Todas las cookies de sesión tienen el atributo "secure" activado de forma que el navegador nunca las transmita en claro.
- ✓ El certificado de seguridad del servidor será legítimo, firmado por una autoridad de certificación reconocida, con validez vigente y que cubra todos los nombres de dominio utilizados por la aplicación.
- ✓ La interceptación de las comunicaciones es un riesgo muy real y más habitual de lo que se puede pensar. Debe presuponer en el desarrollo de una aplicación web que cualquier dato que el usuario envíe o que se envíe hacia el usuario puede ser observado por un posible atacante.
- ✓ El escenario ideal y la configuración por defecto debería ser cifrar todas las comunicaciones, ya no sólo para los datos personales procedentes del usuario, sino también porque la información consultada puede estar sujeta a restricciones de visibilidad.
- ✓ Se recomienda actualizar regularmente el software de cifrado SSL, para evitar de esta forma ser objeto de ataques basados en vulnerabilidades de software conocidas y/o errores en la implementación del sistema de cifrado (Ejemplo: vulnerabilidades conocidas de versiones antiguas de "openssl").
- ✓ En caso de ser posible, se debe forzar siempre la conexión y la navegación HTTPS.

2.2.2.10 REDIRECCIONES Y REENVÍOS NO VALIDADOS

DEFINICIÓN

Las aplicaciones Web frecuentemente redirigen y reenviar los usuarios a otras páginas o sitios web con datos no confiables.

Sin la correcta validación, los atacantes pueden redirigir a las víctimas a sitios de malware o phishing, o utilizar delante para acceder a páginas no autorizadas. (Owasp Top 10-2013 rcl, 2013)

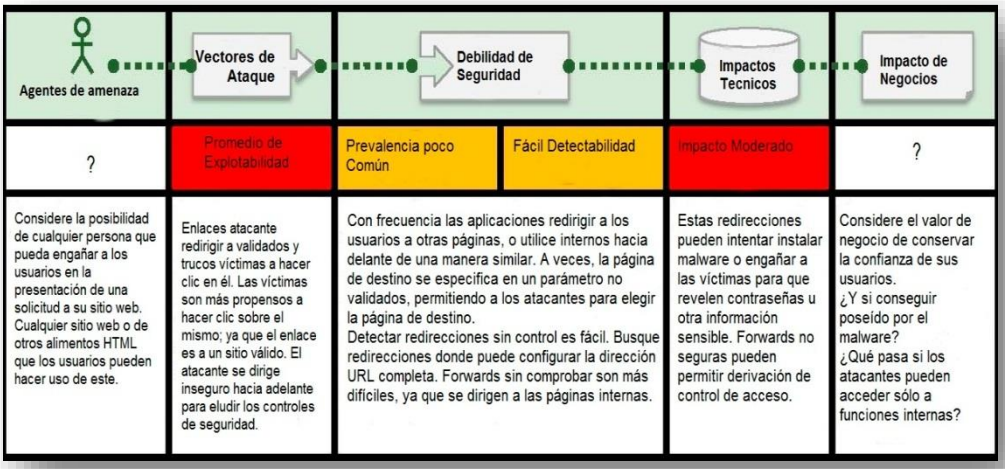


Figura 10. Características vulnerabilidad -redirecciones y destinos inválidos

Fuente: *OWASP (2013).*Imagen de las vulnerabilidad características vulnerabilidad -redirecciones y destinos inválidos de OWASP TOP 10.

Adaptado por: Gavidia Marco & Jessica Valle

CONDICIONES PARA QUE EXISTA LA VULNERABILIDAD

- ✓ Revise el código antes de redirigir o reenviar (llamado transferencia de. NET).
- ✓ Identifique si la URL de destino se incluirá en todos los valores de los parámetros.
- ✓ Verifique el sitio para ver si genera redirecciones (códigos de respuesta HTTP 300 a 307, por lo general 302).
- ✓ Revisar los parámetros proporcionados antes de la redirección para ver si parece ser un URL de destino o un pedazo desea URL.

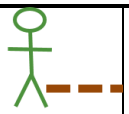
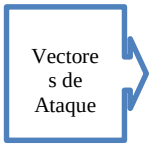
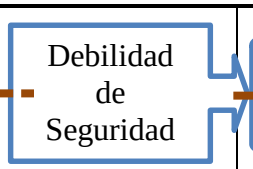
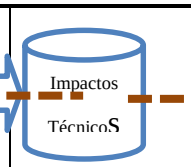
- ✓ Se debe cambiar la URL de destino y observar si el sitio redirige a la nueva.
- ✓ Si el código no está disponible, compruebe todos los parámetros para ver si se ven como parte de una redirección o enviar URL de destino.

RECOMENDACIONES (Publica, 2012)

- ✓ En caso de que la aplicación realice redirecciones por URL, éstas no deberán admitir cualquier nombre o destino a menos que su funcionalidad así lo requiera explícitamente

2.2.3 RESUMEN DE VULNERABILIDADES

Tabla 2. Resumen de Vulnerabilidades 1

					
A1 **INYECCIÓN SQL**	Considere la posibilidad de cualquier persona que pueda enviar datos que son de confianza en el sistema, incluidos los usuarios externos, los usuarios internos y administradores.	El atacante envía simples ataques basados en texto que explotan la sintaxis del intérprete apuntado. Casi cualquier fuente de datos puede ser un vector de inyección, incluyendo fuentes internas.	Ocurre cuando una aplicación envía datos no confiables a un intérprete. Son muy frecuentes, sobre todo en el código heredado. A menudo se encuentran en SQL, LDAP o consultas XPath, comandos de sistema operativo, los analizadores XML, argumentos del programa, etc. Son fáciles de descubrir al examinar el código, pero más difícil a través de pruebas. Escáneres y fuzzers ayudan a encontrar a los atacantes	La inyección puede causar la pérdida de datos o la corrupción, la falta de rendición de cuentas, o la denegación de acceso. Inyección a veces puede llevar a la toma de posesión de acogida.	Considere el valor de negocio de los datos afectados y la plataforma que ejecuta el intérprete. Todos los datos pueden ser robados, modificados o eliminados. Podría ser dañado su reputación?

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 3. Resumen de Vulnerabilidades 2

A2 **PÉRDIDA DE AUTENTICACIÓN Y GESTIÓN DE SESIÓN**	Considere atacantes externos anónimos, así como los usuarios con sus propias cuentas, que pueden intentar robar cuentas de los demás. Considera también incide que desean ocultar sus acciones.	El atacante utiliza fugas o fallas en las funciones de gestión de autenticación o sesión (por ejemplo, cuentas a la vista, contraseñas, ID de sesión) para hacerse pasar por usuarios.	Desarrolladores frecuencia construyen sistemas de gestión de sesiones y autenticación personalizada, pero la construcción de estos correcta es difícil. Como resultado, estos esquemas personalizados con frecuencia tienen deficiencias en áreas tales como cierre de sesión, administración de contraseñas, tiempos de espera, acuérdate de mí, la pregunta secreta, cuenta de actualización, etc. encontrar tales defectos veces puede ser difícil, ya que cada aplicación es única.	Tales defectos pueden permitir que algunas o incluso todas las cuentas sean atacadas. Una vez conseguido esto, el atacante puede hacer nada a la víctima podía hacer. Las cuentas con privilegios son con frecuencia blanco de ataques.	Considere el valor de negocio de los datos afectados o funciones de la aplicación. También considere el impacto en el negocio de la exposición pública de [la vulnerabilidad.
A3 **SECUENCIA DE COMANDOS EN SITIOS CRUZADOS**	Considere la posibilidad de cualquier persona que pueda enviar datos son de confianza en el sistema, incluidos los usuarios externos, los usuarios internos y administradores.	El atacante envía secuencias de comandos de ataque basados en texto que se aprovechan de la intérprete en el navegador. Casi cualquier fuente de datos puede ser un vector de ataque, incluyendo fuentes internas tales como los datos de la base de datos.	XSS es la más frecuente falla de seguridad de aplicaciones web. Las fallas de XSS ocurren cuando una aplicación incluye datos proporcionados por el usuario en una página enviados al navegador sin validar o escapar correctamente el contenido. Existen tres tipos conocidos de fallas XSS: 1) almacenados, 2) Refleja, y 3) DOM XSS basado.	Los atacantes pueden ejecutar scripts en el navegador de la víctima para secuestrar sesiones de usuario, modificar sitios Web, insertar contenido hostil, redirigir a los usuarios, secuestrar el navegador del usuario con malware, etc.	Considere el valor de negocio del sistema afectado y todos los datos que procesa. También considere el impacto en el negocio de la exposición pública de la vulnerabilidad.
A4 **REFERENCIAS DIRECTA INSEGURA A OBJETOS**	Tenga en cuenta los tipos de usuarios de su sistema. ¿Alguno de los usuarios sólo tienen acceso parcial a ciertos tipos de datos del sistema?	El atacante, que es un usuario autorizado del sistema, simplemente cambia el valor del parámetro que se refiere directamente a un objeto del sistema a otro objeto que el usuario no está autorizado para. Se concede el acceso?	Las aplicaciones suelen utilizar el nombre real o la clave de un objeto al generar páginas web. Las aplicaciones no siempre verifican que el usuario está autorizado para el objeto de destino. Esto resulta en un defecto de referencia objeto directo insegura. Testers pueden manipular fácilmente los valores de parámetros para detectar ese tipo de errores y análisis de código muestra rápidamente si la autorización se verifica correctamente.	Tales defectos pueden comprometer todos los datos que pueden ser referenciados por el parámetro. A menos que el espacio de nombres es escasa, es fácil para un atacante para acceder a todos los datos disponibles de este tipo.	Considere el valor comercial de los datos expuestos. También considere el impacto en el negocio di la exposición pública de [la vulnerabilidad.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 3. Resumen de Vulnerabilidades 3

A5 **CONFIGURACIÓN DEFECTUOSA DE SEGURIDAD**	Considere la posibilidad de atacantes externos anónimos y usuarios con sus propias cuentas que pueden intentar poner en peligro el sistema. Considera también inside que desean ocultar sus acciones.	El atacante accede a las cuentas por defecto, las páginas no utilizadas, defectos sin parches, archivos desprotegidos y directorios, etc., para obtener acceso no autorizado o el conocimiento del sistema.	Reconfiguración de Seguridad puede ocurrir a cualquier nivel de un conjunto de aplicaciones, incluyendo la plataforma, servidor web, servidor de aplicaciones, el marco y el código personalizado. Los desarrolladores y los administradores de red deben trabajar juntos para asegurar que toda la pila está correctamente configurado.	Tales defectos suelen dar los atacantes el acceso no autorizado a algunos datos del sistema o la funcionalidad. En ocasiones, estas fallas dan como resultado un compromiso total del sistema.	El sistema puede ser completamente comprometido sin que usted lo sepa. Todos los datos pueden ser robados o modificarse lentamente con el tiempo. Los costos de recuperación podrían ser costoso.
A6 **LA EXPOSICIÓN DE DATOS SENSIBLES**	Considere la posibilidad de atacantes externos anónimos y usuarios con sus propias cuentas que pueden intentar poner en peligro el sistema. Considera también insiders que desean ocultar sus acciones.	El atacante accede a las cuentas por defecto, las páginas no utilizadas, defectos sin parches, archivos desprotegidos y directorios, etc. para obtener acceso no autorizado o el conocimiento del sistema.	Reconfiguración de Seguridad puede ocurrir a cualquier nivel de un conjunto de aplicaciones, incluyendo la plataforma, servidor web, servidor de aplicaciones, el marco y el código personalizado. Los desarrolladores y los administradores de red deben trabajar juntos para asegurar que toda la pila está correctamente configurado.	Tales defectos suelen dar los atacantes el acceso no autorizado a algunos datos del sistema o la funcionalidad. En ocasiones, estas fallas dan como resultado un compromiso total del sistema.	El sistema puede ser completamente comprometido sin que usted lo sepa. Todos los datos pueden ser robados o modificarse lentamente con el tiempo. Los costos de recuperación podrían ser costoso.
A7 **FALTA DE FUNCIÓN QUE CONTROLA EL NIVEL DE ACCESO**	Considere la posibilidad de cualquier persona que pueda cargar contenido en los navegadores de los usuarios, y así obligarlos a presentar una solicitud para su sitio web. Cualquier sitio web o de otros alimentos HTML que el acceso del usuario puede hacer esto.	El atacante crea solicitudes y trucos la de victima HTTP forjadas en la presentación de ellos a través de las etiquetas de imagen, XSS, o muchas otras técnicas. Si el usuario está autenticado, el ataque tiene éxito.	CSRF se aprovecha del hecho de que la mayoría de las aplicaciones web permiten a los atacantes predecir todos los detalles de una acción en particular. Dado que los navegadores envían credenciales como cookíes de sesión automáticamente, los atacantes pueden crear páginas web maliciosas que generan peticiones forjados que son indistinguibles de los legítimos.	Los atacantes pueden causar víctimas para cambiar los datos a la víctima se le permite modificar o realizar cualquier otra función que la víctima está autorizado a utilizar o solicitar cambio de estado, como el cierre de sesión o registrarte.	Considere el valor de negocio de los datos afectados o funciones de la aplicación. Imagine que no es seguro si los usuarios de la intención de tomar estas acciones. Considere el impacto en su reputación.
A8 **FALSIFICACIÓN DE PETICIONES EN SITIO CRUZADO**	Considere la posibilidad de cualquier persona que pueda engañar a los usuarios en la presentación de una solicitud a su sitio web. Cualquier sitio web o de otros alimentos HTML que los usuarios pueden hacer uso de este.	Enlaces atacante redirigir a validados y trucos victimas a hacer clic en él. Las víctimas son más propensos a hacer clic sobre el mismo; ya que el enlace es a un sitio válido. El atacante se dirige inseguro hacia adelante para eludir los controles de seguridad.	Con frecuencia las aplicaciones redirigir a los usuarios a otras páginas, o utilice internos hacia delante de una manera similar. A veces, la página de destino se especifica en un parámetro no validado, permitiendo a los atacantes para elegir la página de destino. Detectar redirecciones sin control es fácil. Busque redirecciones donde puede configurar la dirección URL completa. Forwards sin comprobar son más difíciles, ya que se dirigen a las páginas internas.	Estas redirecciones pueden intentar instalar malware o engañar a las víctimas para que revelen contraseñas u otra información sensible. Forwards no seguras pueden permitir derivación de control de acceso.	Considere el valor de negocio de conservar la confianza de sus usuarios. ¿Y si conseguir poseído por el malware? ¿Qué pasa si los atacantes pueden acceder sólo a funciones internas?

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 4. Resumen de vulnerabilidades 4

A9 **UTILIZACIÓN DE COMPONENTES CON VULNERABILIDADES CONOCIDAS**	Algunos de los componentes vulnerables (por ejemplo, las bibliotecas marco) se pueden identificar y explotar con herramientas automatizadas, la ampliación de la piscina agente de amenaza más allá de los atacantes dirigidos a incluir actores caóticos..	El atacante envía simples ataques basados en texto que explotan la sintaxis del intérprete apuntado. Casi cualquier fuente de datos puede ser un vector de inyección, incluyendo fuentes internas.	El atacante identifica un componente débil por barrido o un análisis manual. Ellos personalizar el exploit según sea necesario y ejecutar el ataque. Se vuelve más difícil si el componente utilizado es profunda en la aplicación	Prácticamente cada aplicación tiene estos problemas porque la mayoría de los equipos de desarrollo no se centran en garantizar que sus componentes permanecen hasta la fecha. En muchos casos, los desabolladores no saben ni todos los componentes que están utilizando, no importa sus versiones. Dependencias de componentes que las cosas aún peor.	Considere lo que cada vulnerabilidad podría significar para la empresa controlada por el application.lt afectado podría ser trivial o podría significar compromiso completo.
A10 **VULNERABILIDAD DE REDIRECCIONES Y DESTINOS INVALIDOS**	Considere la posibilidad de cualquier persona que pueda engañar a los usuarios en la presentación de una solicitud a su sitio web. Cualquier sitio web o de otros alimentos HTML que los usuarios pueden hacer uso de este.	Enlaces atacante redirigir a validados y trucos victimas a hacer clic en él. Las víctimas son más propensos a hacer clic sobre el mismo; ya que el enlace es a un sitio válido. El atacante se dirige inseguro hacia adelante para eludir los controles de seguridad.	Con frecuencia las aplicaciones redirigir a los usuarios a otras páginas, o utilice internos hacia delante de una manera similar. A veces, la página de destino se especifica en un parámetro no validado, permitiendo a los atacantes para elegir la página de destino. Detectar redirecciones sin control es fácil. Busque redirecciones donde puede configurar la dirección URL completa. Forwards sin comprobar son más difíciles, ya que se dirigen a las páginas internas.	Estas redirecciones pueden intentar instalar malware o engañar a las víctimas para que revelen contraseñas u otra información sensible. Forwards no seguras pueden permitir derivación de control de acceso.	Considere el valor de negocio de conservar la confianza de sus usuarios. ¿Y si conseguir poseído por el malware? ¿Qué pasa si los atacantes pueden acceder sólo a funciones internas?

Adaptado por: Gavidia Marco & Jessica Valle

2.2.4 METODOLOGÍA DE CALIFICACIÓN DE RIESGO SEGÚN OWASP

Es importante estimar el riesgo asociado a las diferentes vulnerabilidades para ello se puede verificar durante el desarrollo, mientras que otros pueden ser descubiertos cuando la aplicación esta en producción pero a pesar de estas condiciones es posible estimar la gravedad, para ello OWASP ha creado un sistema de calificación de riegos que permitirá ahorrar tiempo y eliminar discusiones de lo que respecta a prioridades. (RRM, 2008).

Lo ideal sería tener un sistema de calificación de riesgo universal para estimar con precisión todos los riesgos para todas las organizaciones pero una vulnerabilidad puede ser importante para dicha organización mientras que para otra no, para eso se ha desarrollado un modelo simple de usar, mientras se mantienen las estimaciones de riesgos precisas a realizar.

En este paso la estimación de probabilidad y la estimación de impacto se ponen juntas para calcular el riesgo de cada vulnerabilidad. (OWASP, Owasp Top 10-2013 rcl, 2013).

Esto se hace por averiguar si la probabilidad es baja, media o alta y luego hacer lo mismo para el impacto. Los niveles para calcular la probabilidad e impacto son:

Tabla 5. Niveles de probabilidad e impacto

Niveles de probabilidad e impacto	
0 a <3	BAJO
3 a <6	MEDIO
6 a 9	ALTO

Fuente: *OWASP (2013).*Tabla de OWASP Risk Rating Methology de OWASP.

2.2.5 OWASP ZAP

El Ataque Proxy Zed (ZAP) es una herramienta fácil de usar para realizar pruebas de penetración integrada como también realizar búsqueda de vulnerabilidades en aplicaciones web.

Está diseñado para ser utilizado por personas con una amplia gama de experiencia en seguridad y, como tal, es ideal para desarrolladores y probadores funcionales que son nuevos en realización de pruebas.

ZAP ofrece escáneres automatizados, así como un conjunto de herramientas que le permiten encontrar las vulnerabilidades de seguridad de forma manual. (OWASP Z. , 2014)

Figura 11. Logo de la herramienta OWASP ZAP

Fuente: OWASP (2013).Imagen del logo de la herramienta OWASP ZAP.

USO

La facilidad de uso, lo convierte en un buscador de vulnerabilidades de aplicaciones web más famosos y tiene la facilidad de escanear dichas vulnerabilidades con solo colocar la url y hacer clic en atacar.

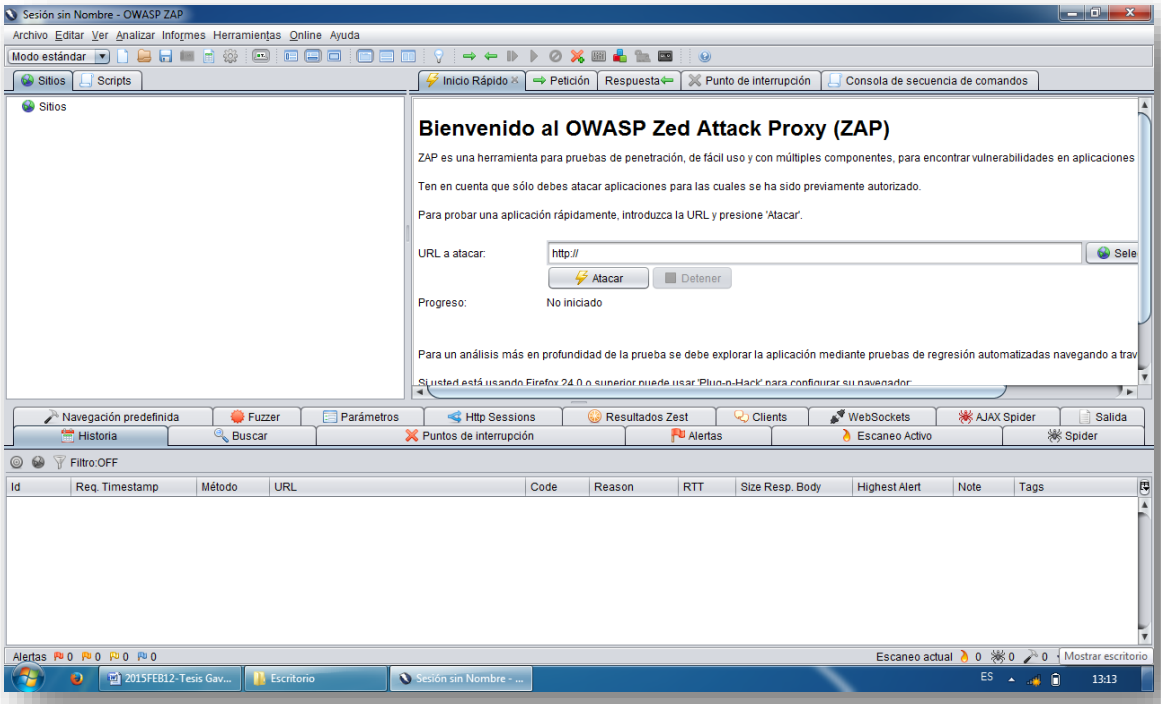


Figura 12. Pantalla de bienvenida OWASP ZAP

Fuente: OWASP (2013).Imagen del logo de la herramienta OWASP ZAP.

CAPÍTULO III

SELECCIÓN Y PROTECCIÓN DE VULNERABILIDADES.

Para la selección de las vulnerabilidades se compara las estadísticas de Owasp y otras organizaciones para lo cual se establecerá parámetros de ponderación y la prioridad que obtenga cada vulnerabilidad al ser evaluadas.

Estas comparaciones sirven para analizar el índice de riesgo de software para el desarrollo de cualquier sistema informático.

3.1.1 CRITERIOS DE SELECCIÓN DE LAS VULNERABILIDADES SEGÚN OWASP

Para comparar las vulnerabilidades se ha aplicado la fórmula de Owasp la cual consiste en: promediar los valores de explotación, la prevalencia y la detección, luego se multiplica por el impacto para obtener el valor de riesgo para cada vulnerabilidad. El resultado de la operación dará como resultado el índice.

$$\boldsymbol{Valor\ de\ Riesgo} = Promedio(explotabilidad + prevalencia + detecciòn) * impacto$$

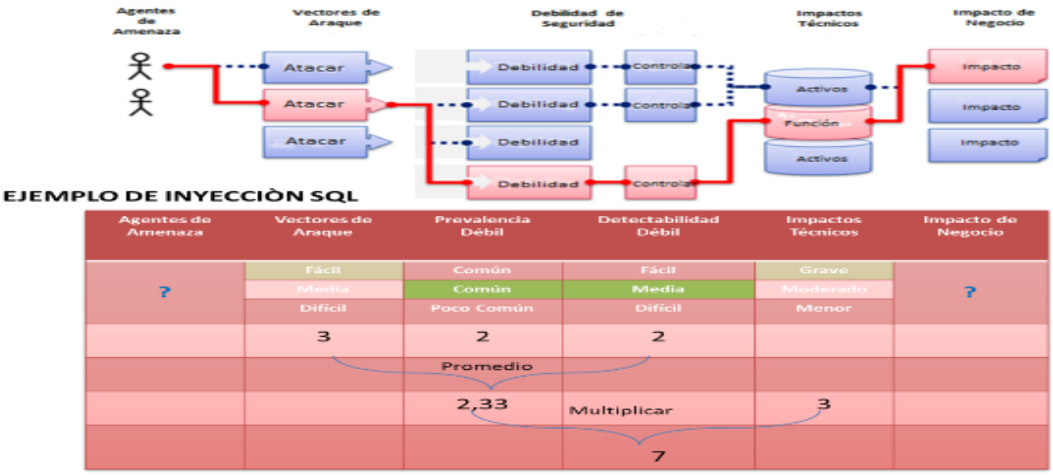


Figura 13. Evaluacion del valor de riesgo para la vulnerabilidad de Inyección SQL

Fuente: OWASP (2013).Imagen de la forma de evaluar el riesgo para cualquier vulnerabilidad

Adaptado por: Gavidia Marco & Jessica Valle

Para conocer el factor de riesgo de cada vulnerabilidad se analizaran los siguientes parámetros que se evaluarán:

- **Explotación:** Es la violación de la seguridad en los sistemas informáticos.
- **Prevalencia:** Con qué Frecuencia las vulnerabilidades se manifiestan en los sistemas Informáticos.
- **Detección:** Con qué facilidad son localizadas las vulnerabilidades en los sistemas informáticos.
- **Impacto:** Que grado de criticidad tiene cada Vulnerabilidad

Tabla 6. Resultado final del escaneo de Inyección Sql y XSS

Operaciones de Respuesta de Explotación	Valor
Difícil	1
Media	2
Fácil	3

Fuente: OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 7. Parametros de evaluación para la Prevalencia de una vulnerabilidad

Operaciones de Respuesta de Prevalencia	Valor
Poco Común	1
Común	2
Difundida	3
Muy Difundida	4

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 8. Parametros de evaluación para la Detección de una vulnerabilidad

Operaciones de Respuesta de Detección	Valor
Difícil	1
Media	2
Fácil	3

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 9. Parametros de evaluación para el Impacto de una vulnerabilidad

Operaciones de Respuesta de Impacto	Valor
Menor	1
Moderado	2
Grave	3

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

La comparación entre las 10 Vulnerabilidades es consecuencia de la investigación realizada por Owasp, de manera que puedan ser definidos los criterios de respuesta en base a la apreciación resultante de dicha investigación, como se muestra a continuación.

INYECCION

Esta vulnerabilidad tiene la explotación fácil porque el atacante envía simples cadenas de texto que explotan la sintaxis del sistema atacado, las fallas de inyección tienen una prevalencia común, son fácil de descubrir cuando se examina el código, pero más difícil a través de pruebas de testeos[2]. Los scanners[3] y fuzzers[4] pueden ayudar a los atacantes a descubrir estas fallas.

El impacto es severo o grave ya que puede resultar en perdida o corrupción de datos, falta de integridad, o negación de acceso. Una falla de inyección puede algunas veces llevar a la toma de posesión completa del servidor.

Tabla 10. Valoración de la Vulnerabilidad de Inyección

Inyección		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Media	2
Impacto	Grave	3

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

[2] Testeos es una investigación técnica que intenta revelar información de calidad acerca del producto de software con respecto al contexto en donde operará.

[3] Un scanners es una captura de una imagen, documento de texto o fotografía, y lo transfiere en bits de información, los cuales puede entender y manejar una computadora.

[4] Fuzzers es un programa que intenta descubrir vulnerabilidades de seguridad evitar arbitrariedades en una aplicación.

PÉRDIDA DE AUTENTIFICACIÓN Y GESTIÓN DE SESIONES

Esta vulnerabilidad tiene la explotación media porque el atacante envía utiliza filtraciones o vulnerabilidades en las funciones de autenticación o gestión de las sesiones para hacerse pasar por usuarios. Tiene una prevalencia difundida cuando se crean esquemas propios de autenticación o gestión de las sesiones, pero conseguir que sean correctos es complicado por ser única en cada sistema. El impacto es severo o grave ya que los atacantes permiten que algunas o todas las cuentas sean atacadas. El atacante podría realizar cualquier acción que la víctima pudiese ser involucrado en comentarios o acciones mal intencionadas. Las cuentas privilegiadas son los objetivos prioritarios.

Tabla 11. Valoración de la Pérdida de Autentificación y Gestión de Sesiones

Pérdida de Autentificación y Gestión de Sesiones		
Explotación	Media	2
Prevalencia	Difundida	3
Detección	Media	2
Impacto	Grave	3

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

SECUENCIAS DE COMANDOS DE SITIOS CRUZADOS

Esta vulnerabilidad tiene la explotación media porque el atacante envía secuencias de comando en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario o dirigir al usuario hacia un sitio malicioso. XSS es la falla de seguridad muy prevalente en aplicaciones web, ocurren cuando una aplicación incluye datos suministrados por el usuario en una página enviada al navegador sin ser el contenido apropiadamente validado o escapado.

El impacto es moderado ya que los atacantes pueden ejecutar secuencias de comandos en el navegador de una víctima para secuestrar las sesiones de usuario, destruir sitios

web, insertar código hostil, redirigir usuarios, instalar código malicioso en el navegador de la víctima, etc.

Tabla 12. Valoración de las Secuencias de Comandos de Sitios Cruzados[22]

Secuencias de Comandos de Sitios Cruzados		
Explotación	Media	2
Prevalencia	Muy Difundida	4
Detección	Fácil	3
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

REFERENCIA DIRECTA INSEGURA A OBJETOS

Esta vulnerabilidad tiene la explotación fácil porque el atacante ingresa como usuario autorizado en el sistema, simplemente modifica el valor de un parámetro que se refiere directamente a un objeto del sistema a otro objeto para el que el usuario no se encuentra autorizado. Tiene una prevalencia común ya que las aplicaciones no siempre verifican que el usuario tiene autorización sobre el objetivo. Los auditores pueden manipular fácilmente los valores del parámetro para detectar estas vulnerabilidades y un análisis de código mostraría rápidamente si la autorización se verifica correctamente.

El impacto es moderado ya que dicha vulnerabilidad puede comprometer toda la información que pueda ser referida por parámetros. A menos que el espacio de nombres resulte escaso, para un atacante resulta sencillo acceder a todos los datos disponibles de ese tipo.

Tabla 13. Valoración de la Vulnerabilidad de Referencia Directa Insegura a Objetos

Referencia Directa Insegura a Objetos		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Fácil	3
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). Owasp Top 10-2013 rcl.

Adaptado por: Gavidia Marco & Jessica Valle

CONFIGURACIÓN DEFECTUOSA DE SEGURIDAD

Esta vulnerabilidad tiene la explotación fácil porque el atacante puede utilizar cuentas predeterminadas, páginas no utilizadas, defectos en software no actualizado o no parchados, archivos o directorios no protegidos, etc. Tiene una prevalencia común cuando existe una mala configuración de seguridad puede ocurrir en cualquier capa de la aplicación, incluyendo la plataforma, el servidor web, el servidor de aplicaciones, el ambiente de trabajo, y el código personalizado. El impacto es moderado ya que permiten a los atacantes obtener acceso no autorizado a datos o funcionalidad del sistema. De forma ocasional, tales defectos resultan en un riesgo para todo el sistema

Tabla 14. Valoración de la Configuración Defectuosa de Seguridad

Configuración Defectuosa de Seguridad		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Fácil	3
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

EXPOSICIÓN DE DATOS SENSIBLES

Esta vulnerabilidad tiene la explotación Difícil porque los atacantes normalmente atacan directamente a base de datos para alterar o eliminar los datos. Como por ejemplo robar claves, robar datos de texto claros fuera del servidor, robar el tránsito desde el navegador.

Tiene una prevalencia poco común es simplemente no cifra los datos sensibles cuando se emplea una criptografía débil y la débil utilización algorítmica las soluciones de hash son particularmente débiles para proteger las contraseñas. Debilidades del navegador son muy comunes y fáciles de detectar, pero difícil de explotar. El impacto es severo o grave ya que pone en peligro con frecuencia todos los datos que deberían haber sido protegidos.

Normalmente, esta información incluye datos confidenciales, como los registros de salud, credenciales, datos personales, tarjetas de crédito.

Tabla 15. Valoración de la Vulnerabilidad de Exposición de Datos Sensibles

Exposición de Datos Sensibles		
Explotación	Difícil	1
Prevalencia	Poco Común	1
Detección	Media	2
Impacto	Grave	3

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS

Esta vulnerabilidad tiene la explotación Fácil porque los atacantes crean peticiones HTTP falsas. Engañan a la víctima al enviarlas a través de etiquetas de imágenes, XSS, o muchas otras técnicas. Si el usuario está autenticado entonces el ataque será exitoso. Tiene una prevalencia común, los CSRF aprovecha aplicaciones web que permiten a los atacantes predecir todos los detalles de una acción en particular.

Cuando los navegadores envían credenciales de autenticación automáticamente, como en el caso de las cookies de sesión, los atacantes pueden crear páginas web maliciosas las cuales generan peticiones falsas que son indistinguibles de las auténticas.

El impacto es moderado cuando los atacantes pueden cambiar cualquier dato que la víctima esté autorizado a cambiar, o acceder a cualquier funcionalidad que la víctima esté autorizada a utilizar.

Tabla 16. Valoración de la Falsificación de Peticiones en Sitios Cruzados

Falsificación de Peticiones en Sitios Cruzados		
Explotación	Fácil	3
Prevalencia	Común	2
Detección	Media	2
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

FALTA DE FUNCÓN QUE CONTROLA EL NIVEL DE ACCESO

Esta vulnerabilidad tiene la explotación Media porque los atacantes crean peticiones HTTP falsas. Engañan a la víctima al enviarlas a través de etiquetas de imágenes, XSS, o muchas otras técnicas.

Si el usuario está autenticado entonces el ataque será exitoso. Tiene una prevalencia común, los CSRF aprovecha aplicaciones web que permiten a los atacantes predecir todos los detalles de una acción en particular.

Cuando los navegadores envían credenciales de autenticación automáticamente, como en el caso de las cookies de sesión, los atacantes pueden crear páginas web maliciosas las cuales generan peticiones falsas que son indistinguibles de las auténticas.

Tabla 17. Valoración de la Falta de Función que Controla el Nivel de Acceso

Falta de Función que Controla el Nivel de Acceso		
Explotación	Media	2
Prevalencia	Común	2
Detección	Fácil	3
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

UTILIZACIÓN DE COMPONENTES CON VULNERABILIDADES CONOCIDAS

Esta vulnerabilidad tiene la explotación Media cuando el atacante identifica un componente débil o un análisis manual. Ellos personalizan el exploit según sea necesario y ejecutan el ataque. Tiene una prevalencia Difundida donde cada aplicación tiene estos problemas porque la mayoría de los equipos de desarrollo no se centran en garantizar la utilización de los componentes.

Tabla 18. Valoración de los Componentes con Vulnerabilidades Conocidas

Utilización de Componentes con Vulnerabilidades Conocidas		
Explotación	Media	2
Prevalencia	Difundida	3
Detección	Difícil	1
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

VULNERABILIDAD DE REDIRECCIÓN Y DESTINOS INVÁLIDOS

Esta vulnerabilidad tiene la explotación Media ya que el atacante redirige imágenes a forma de trucos a sus víctimas para que hagan clic sobre la imagen. Las víctimas son más propensas a hacer clic sobre el mismo; ya que el enlace es a un sitio válido. El atacante se dirige inseguro hacia adelante para eludir los controles de seguridad.

Tiene una prevalencia Poco Común a veces, la página de destino se especifica en un parámetro no validado, permitir a los atacantes elegir la página de destino. Detectar redirecciones sin control es fácil. Busque redirecciones donde puede configurar la dirección URL completa. Sin comprobación son más difíciles, ya que se dirigen a las páginas internas. El impacto es moderado ya que estas redirecciones pueden intentar instalar malware o engañar a las víctimas para que revelen contraseñas u otra información sensible.

Tabla 19. Valoración de la Vulnerabilidad de Redirección y Destinos Inválidos[29]

Vulnerabilidad de Redirección y Destinos Inválidos		
Explotación	Media	2
Prevalencia	Poco Común	1
Detección	Fácil	1
Impacto	Moderado	2

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

VALOR DE RIESGO DE LA COMPARACIÓN DE LAS VULNERABILIDADES

Tabla 20. Resultado General de la Comparación de las Vulnerabilidades

Resultado Final de las Vulnerabilidades

Criterios	A1		A2		A3		A4		A5		A6		A7		A8		A9		A10	
	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor	Resultado	Valor
Explotación	Fácil	3	Media	2	Media	2	Fácil	3	Fácil	3	Difícil	1	Fácil	3	Media	2	Media	2	Media	2
Prevalencia	Común	2	Difundida	3	Muy Difundida	4	Común	2	Común	2	Poco Común	1	Común	2	Común	2	Difundida	3	Poco Común	1
Detección	Media	2	Media	2	Fácil	3	Fácil	3	Fácil	3	Media	2	Media	2	Fácil	3	Difícil	1	Fácil	3
Impacto	Grave	3	Grave	3	Moderado	2	Moderado	2	Moderado	2	Grave	3	Moderado	2	Moderado	2	Moderado	2	Moderado	2
		7		7		6		5,33333333		5,333333333		4		4,66666667		4,66666667		4		4

Fuente: Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

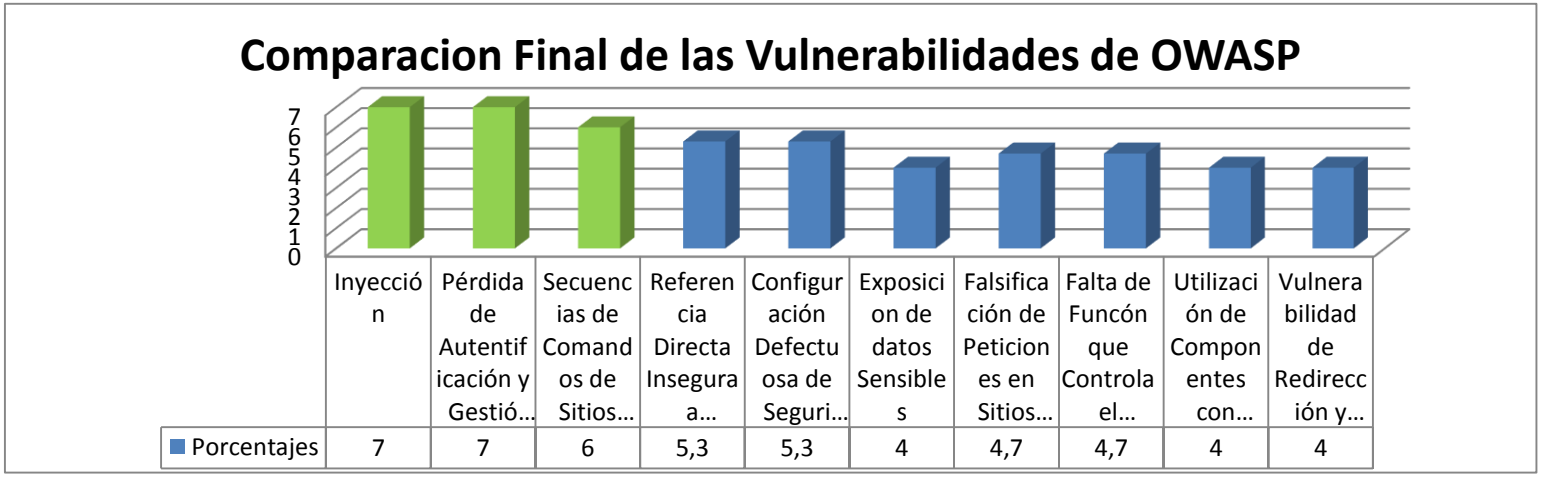


Figura 14. Comparación General de las Vulnerabilidades

.**Fuente:** Tabla de OWASP. (2013). *Owasp Top 10-2013 rcl*.

Adaptado por: Gavidia Marco & Jessica Valle

En base a las ponderaciones realizadas y de acuerdo a los parámetros planteados se puede apreciar que las vulnerabilidades de: Inyección Sql, Pérdida de Autentificación y Gestión de Sesiones, Secuencias de Comandos de Sitios Cruzados tienen un índice de riesgo mayor en comparación con las demás vulnerabilidades.

3.1.2 VULNERABILIDADES SEGÚN OTRAS ORGANIZACIONES

SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Contribuye al desarrollo de la UNAM a través de la prestación de servicios especializados en la seguridad de la información, se encarga de establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de vulnerabilidades informáticas apoyándose de las estadísticas de vulnerabilidades más comunes.

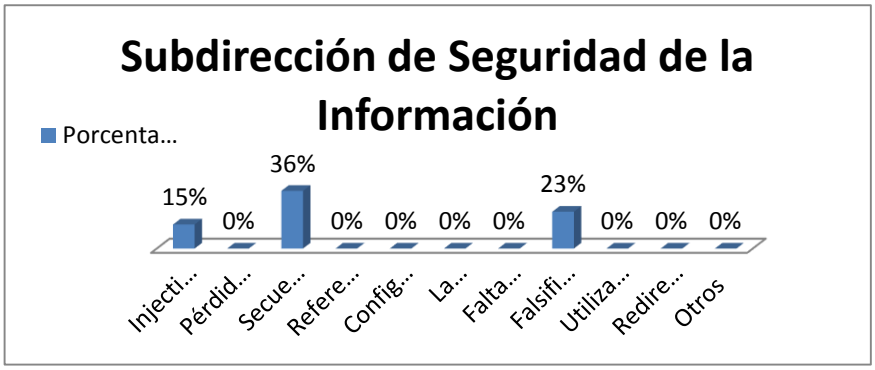


Figura 15. Subdirección de Seguridad de la Información

Fuente: Porcentajes de las vulnerabilidades que han analizado la Subdirección de Seguridad de la Información.

Adaptado por: Gavidia Marco & Jessica Valle

DEMS - Servicio de Monitoreo Externo DOSarrest

DEMS se encarga de la protección de páginas web ante alguna vulnerabilidad, las estadísticas que nos muestra esta corporación con mayores riesgos son: (Inyección Sql en un 22%, Secuencia de Comandos en Sitios Cruzados(XSS) en un 28%, y la Falsificación de Peticiones en Sitios Cruzados (CSRF) en un 67%). (DEMS, 2014)

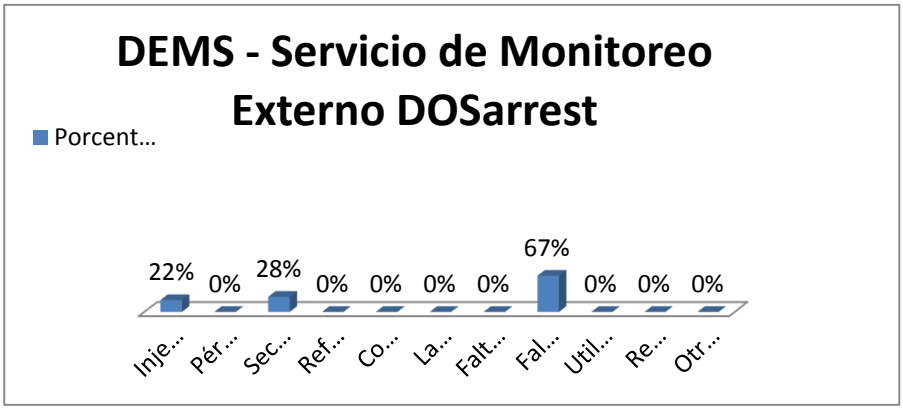


Figura 16. Servicio de Monitoreo Externo DOSarrest

Fuente: DEMS (2014)

Adaptado por: Gavidia Marco & Jessica Valle

OWASP Costa Rica

OWASP Costa Rica es una organización que proporciona un conjunto de conocimientos, técnicas sobre el análisis y la seguridad de las aplicaciones web las estadísticas que nos proporciona son: (Injection Sql en un 11%, Secuencia de Comandos en Sitios Cruzados (XSS) en un 55%, Exposición de Datos Sensibles (15%) y la Falsificación de Peticiones en Sitios Cruzados (CSRF) en un 19%). (OWASP, Owasp Day Costa Rica, 2013, pág. 34)

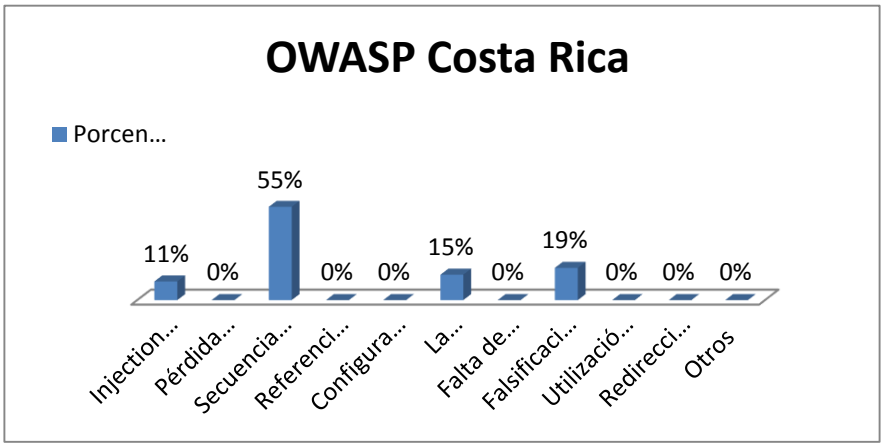


Figura 17. OWASP Costa Rica

Fuente: OWASP Costa Rica (2013).

Adaptado por: Gavidia Marco & Jessica Valle

Aspect Security

Aspect Security ayudan a las organizaciones a desarrollar prácticas y efectivos programas de seguridad de aplicaciones como muestra en las estadística las más relevantes son: (Exposición de Datos Sensibles (12%) y la Falsificación de Peticiones en Sitios Cruzados (CSRF) en un 4%). (Security A. , 2013, pág. 10).

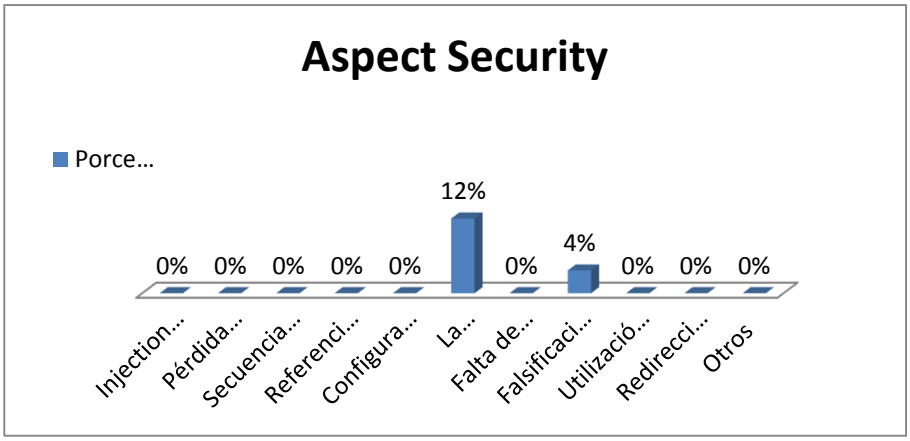


Figura 18. Aspect Security

Fuente: Aspect Security (2013).

Adaptado por: Gavidia Marco & Valle Jessica

HP Ciber Risk Report 2012

HP Enterprise Security proporciona una seguridad ante las vulnerabilidades que afecta a los organismos de inteligencia, ayuda a minimizar los riesgos de seguridad como muestra en las estadística:(Inyección Sql en un (9%), Pérdida de Autentificación y Gestión de Sesión (13%), Secuencia de Comandos en Sitios Cruzados (XSS) en un (45%), Configuración Defectuosa de Seguridad (26%) y la Utilización de omponentes con Vulnerabilidades Conocidas en un (19%)). (Cyber risk report 2013, 2013)

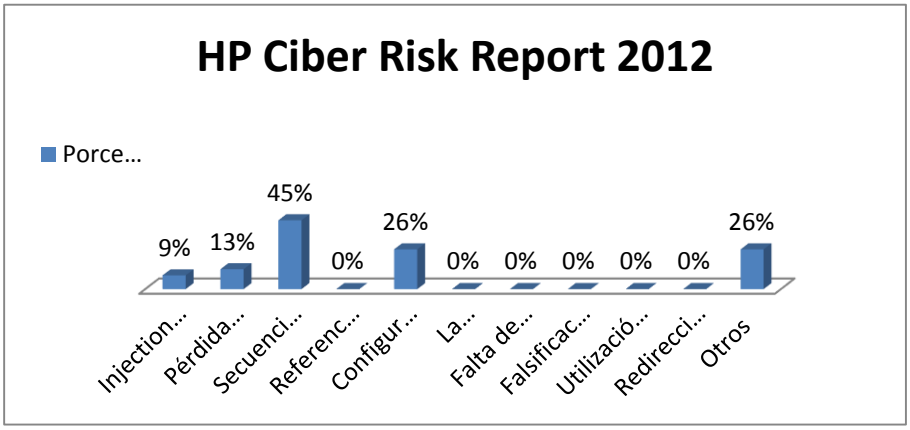


Figura 19. HP Ciber Risk Report 2012

Fuente: Minded Security (2013).

Adaptado por:Gavidia Marco & Jessica Valle

Minded Security

Seguridad Minded es la compañía global de Seguridad de Información operador centrado en la seguridad de las aplicaciones, ofrece servicios profesionales para ayudar a las empresas a crear un seguro de vida de desarrollo de software de ciclo, para ello nos muestra las estadísticas con las vulnerabilidades afectan a los sistemas y son:(Injection Sql en un (3%), Secuencia de Comandos en Sitios Cruzados (XSS) en un (11%), la Falsificación de Peticiones en Sitios Cruzados (CSRF) en un (6%) y otros tipos de Vulnerabilidades en un (52%)). (Blog, 2013, pág. 1)

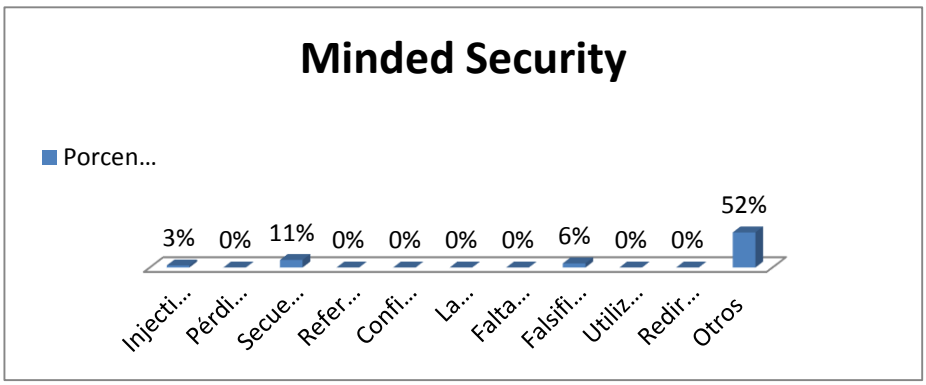


Figura 20. Minded Security

Fuente: Minded Security (2013).

Adaptado por:Gavidia Marco & Jessica Valle

Soffteck Security

Es una compañía que se encarga de la Seguridad de aplicaciones, operaciones de seguridad y gestión de riesgos. Además es responsable de la seguridad de varias empresas pequeñas, medianas y grandes. En las estadísticas las vulnerabilidades en riesgo para los sistemas son:(Injection Sql en un (18%), Pérdida de Autentificación y Gestión de Sesión en un (28%), Configuración Defectuosa de Seguridad en un (1%) y otros tipos de Vulnerabilidades en un (53%)). (Softtek, 2012)

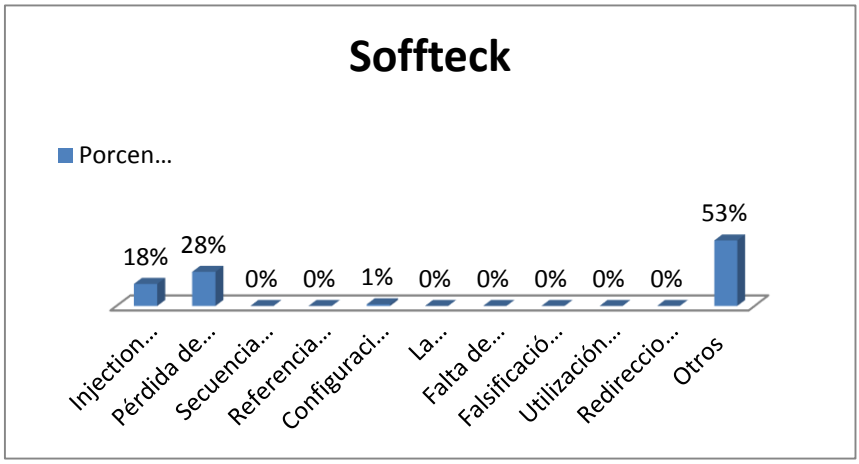


Figura 21. Estadísticas de Soffteck con las 3 vulnerabilidades estudiadas

Fuente: https://www.softtek.com/webdocs/special_pdfs/WP-State-of-the-art-2013.pdf

Adaptado por: Gavidia Marco & Jessica Valle

Trustwave SpiderLabs

La organización de Trustwave SpiderLabs se en carga de proteger los sistemas de las amenazas, sino también de identificar las vulnerabilidades inherentes a existir en los sistemas. Trustwave analizó, descubrió las principales vulnerabilidades y amenazas que tienen la mayor potencial de afectar negativamente a las organizaciones como se muestra en las estadísticas: (Injection Sql en un (11%), Secuencia de Comandos en Sitios Cruzados en un (1%), Falsificación de Peticiones en Sitio Cruzados en un (1%) y otros tipos de Vulnerabilidades en un (87%)). (MARKETO, 2013)

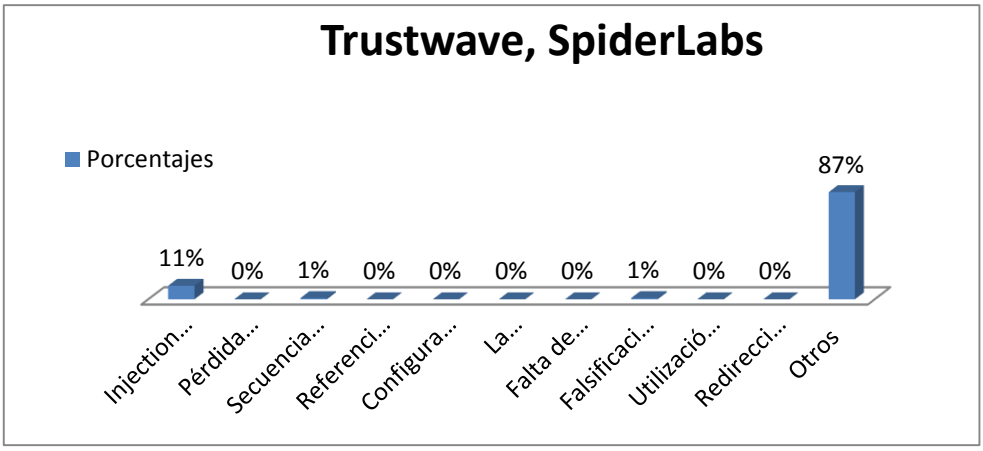


Figura 22. Trustware, SpideLabs

Fuente: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

Adaptado por: Gavidia Marco & Jessica Valle

Veracode

Veracode es una organización que proporciona la solución más rápida, más completa para mejorar la seguridad de aplicaciones de software, se basa en políticas programas de gestión de riesgos de aplicación que ayudan a identificar y erradicar numerosas vulnerabilidades como:(Injection Sql en un (3%), Secuencia de Comandos en Sitios Cruzados en un (41%) y otros tipos de Vulnerabilidades en un (56%)). (Veracode, 2011).

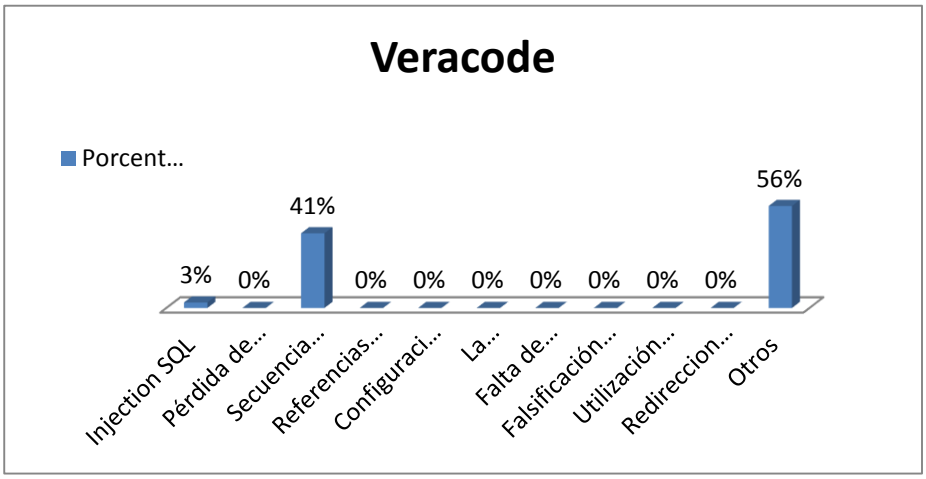


Figura 23. Veracode

Fuente: http://info.veracode.com/rs/veracode/images/VERACODE-SOSS-V4.pdf.

Adaptado por: Gavidia Marco & Jessica Valle

Whitehat Security

La seguridad de WhiteHat es una organización que se dedica a la obtención de los recursos necesarios para solucionar las vulnerabilidades que se identifican en los sistemas. Se muestra las vulnerabilidades más frecuentes que son:(Injection Sql en un (14%), Pérdida de Autentificación y Gestión de Sesión en un (6%) y Falsificación de Peticiones en Sitios Cruzados en un (41%). (Security W. , 2013)

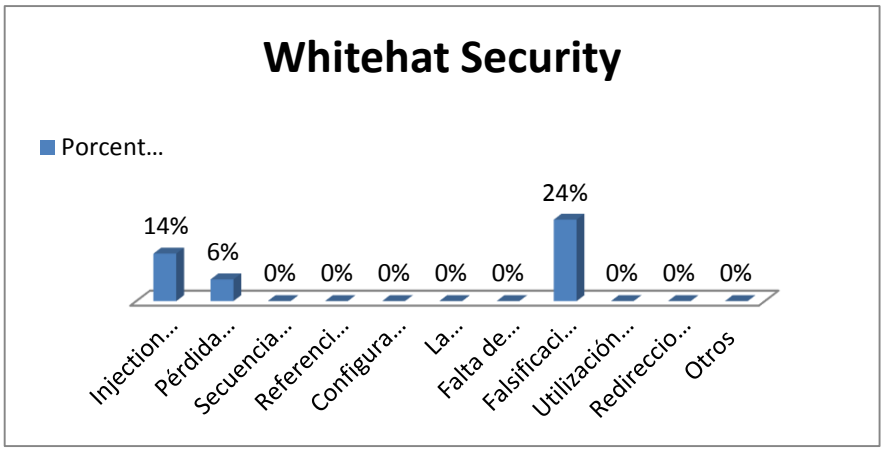


Figura 24. Whitehat Security

Fuente: http://owasptop10.googlecode.com/files/WPstats_winter11_11th.pdf

Adaptado por: Gavidia Marco & Jessica Valle

COMPARACIÓN DE LAS VULNERABILIDADES SEGÚN OTROS ORGANISMOS

Vulnerabilidades	Subdirección de Seguridad de la Información	DOSarrest	OWASP Costa Rica	Aspect Security	HP Ciber Risk Report 2012	Minded Security	Soffteck	Trustwave, SpiderLabs	PROMEDIO
Injection SQL	15%	22%	11%		9%	3%	18%	11%	12,7%
Pérdida de autenticación y gestión de sesión					13%		28%		20,5%
Secuencia de comandos en sitios cruzados (XSS)	36%	28%	55%		45%	11%		1%	29,3%
Falsificación de peticiones en sitio cruzados(CSRF)	23%	67%	19%	4%		6%		1%	20,0%
La exposición de datos sensibles			15%	12%					13,5%
Configuración defectuosa de seguridad					26%		1%		13,5%
Otros					26%	52%	53%	87%	54,5%

Figura 25. Promedio de Vulnerabilidades en las Organizaciones

Adaptado por: Gavidia Marco & Jessica Valle

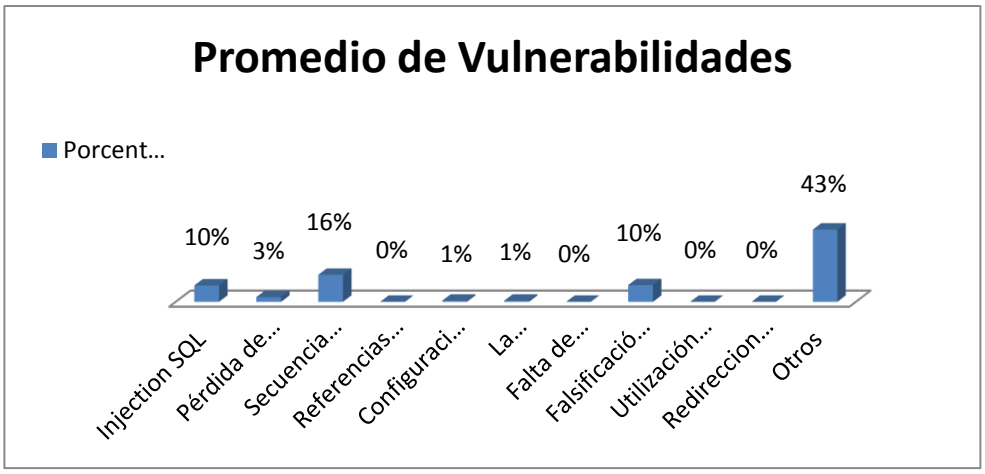


Figura 26. Vulnerabilidades según otros organismos

Fuente: OWASP. (2013). *Owasp Top 10-2013 rcl* (Create Commons ed.). (O. Foundation, Ed.) Estados Unido.

Adaptado por: Gavidia Marco & Jessica Valle

Según el índice de porcentajes de los distintos organismos nos muestra que las vulnerabilidades con más índice de riesgo son: Inyección Sql con un 10%, Falsificación de peticiones en sitios cruzados con un 10%, secuencias de comandos en sitios cruzados con un 16% y otras vulnerabilidades con un 43%.

3.1.3 COMPARACIÓN GENERAL DE VULNERABILIDADES DE OWASP CON LAS OTRAS ORGANIZACIONES

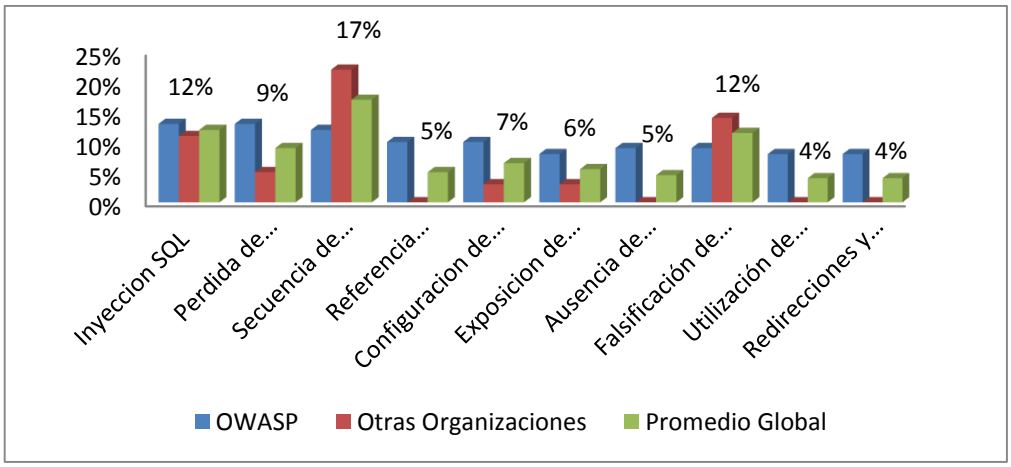


Figura 27. Comparación de vulnerabilidades de OWASP y otras organizaciones

Adaptado por: Gavidia Marco & Jessica Valle

Vulnerabilidades	Injection SQL	Pérdida de autenticación	Secuencia de com	Referencias directa i	Configuración defe	La exposición de datos sensib	Falta de función que c	Falsificación de peticiones en sitio cru	Utilización de componentes	Redirecciones y reenvíos no validados
OWASP	13%	13%	12%	10%	10%	8%	9%	9%	8%	8%
Estadisticas Totales Otras Organizaciones	11%	5%	22%	0%	3%	3%	0%	14%	0%	0%
Promedio Global	12%	9%	17%	5%	6%	5%	5%	12%	4%	4%

Figura 28. Cuadro de comparación de vulnerabilidades

Fuente: OWASP. (2013). *Owasp Top 10-2013 rcl* (Create Commons ed.). (O. Foundation, Ed.) Estados Unido.

Adaptado por: Gavidia Marco & Jessica Valle

En la figura 28 se puede apreciar los resultados obtenidos del análisis de la comparación de vulnerabilidades presentadas por OWASP comparadas con las vulnerabilidades investigadas por otros organismos, se observa que en primer lugar la vulnerabilidad de Secuencia de comandos cruzados (XSS) tiene un promedio de 17%, en segundo lugar se tiene a la falsificación de sitios cruzados (CSRF) con un promedio del 12% y la inyección SQL con un porcentaje igual del 12%.

Las siguientes vulnerabilidades con las estadísticas indicadas son muy relevantes y deben ser tomadas en consideración cuando se desea proteger un sistema informático de plataforma web.

3.1.3.1 RESULTADO DE LAS VULNERABILIDADES

Con los resultados obtenidos en:

Inyección SQL

Secuencia de Comandos Cruzados

Falsificación de Peticiones en Sitios Cruzados

Se analizó que las tres vulnerabilidades son las más riesgosas para un sistema informático por lo se debe tomar en cuenta mecanismos de seguridad que permita brindar la debida prevención a nivel de software.

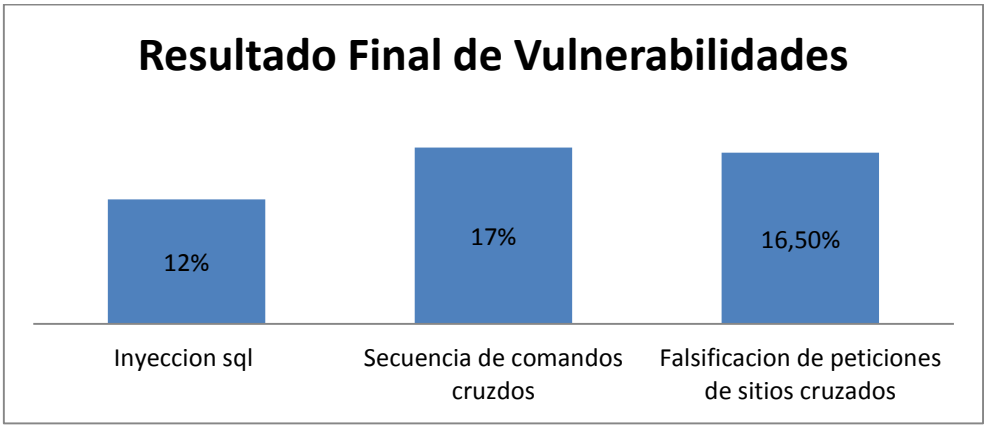


Figura 29. Resultado Final de Vulnerabilidades

Adaptado por: Gavidia Marco & Jessica Valle

Para las vulnerabilidades seleccionadas con anterioridad se procede a desarrollar mecanismos de seguridad que permita brindar la debida protección a nivel de software, que van hacer implementados en el sistema del Cementerio Municipal de Riobamba.

3.1.4 DESARROLLOS DE MECANISMOS DE PROTECCION.

Para prevenir las vulnerabilidades seleccionadas se debe aplicar los siguientes mecanismos de protección para cada una de ellas, el código que se debe aplicar al sistema se detalla a continuación:

3.1.4.1 INYECCION SQL

Aplicado este código al sistema, no podrá entrar a cualquier página por que inmediatamente le redireccionará a la página de login para ocultar el verdadero contenido y evitar ser inyectado de código malicioso. El lenguaje seleccionado es porque tiene código abierto, crea contenidos dinámicos y se puede interactuar con el usuario; además el código utilizado solo es un ejemplo ya que pueden existir diferentes formas de protección para esta vulnerabilidad.

```
<?php require_once('Connections/conect2.php'); ?>
<?php
if (!function_exists("GetSQLValueString")) {
function GetSQLValueString($theValue, $theType, $theDefinedValue = "",
$theNotDefinedValue = "")
{
  if (PHP_VERSION < 6) {
    $theValue = get_magic_quotes_gpc() ? stripslashes($theValue) : $theValue;
  }
  $theValue = function_exists("mysql_real_escape_string") ?
mysql_real_escape_string ($theValue) : mysql_escape_string($theValue);

  switch ($theType) {
    case "text":
```

```
    $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
    break;
  case "long":
  case "int":
    $theValue = ($theValue != "") ? intval($theValue) : "NULL";
    break;
  case "double":
    $theValue = ($theValue != "") ? doubleval($theValue) : "NULL";
    break;
  case "date":
    $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
    break;
  case "defined":
    $theValue = ($theValue != "") ? $theDefinedValue : $theNotDefinedValue;
    break;
 }
 return $theValue;
}
}
?>
<?php
// *** Validate request to login to this site.
if (!isset($_SESSION)) {
 session_start();
}
$loginFormAction = $_SERVER['PHP_SELF'];
if (isset($_GET['accesscheck'])) {
 $_SESSION['PrevUrl'] = $_GET['accesscheck'];
}
if (isset($_POST['login'])) {
```

```
 $loginUsername=$_POST['login'];
 $password=$_POST['password'];
 $MM_fldUserAuthorization = "";
 $MM_redirectLoginSuccess = "index1.php";
 $MM_redirectLoginFailed = "index2.php";
 $MM_redirecttoReferrer = false;
 mysql_select_db($database_conect2, $conect2);
   $LoginRS__query=sprintf("SELECT Login, Clave FROM usuario WHERE
Login=%s AND Clave=%s",
   GetSQLValueString($loginUsername, "text"), GetSQLValueString($password,
"text"));
    $LoginRS = mysql_query($LoginRS__query, $conect2) or die(mysql_error());
 $loginFoundUser = mysql_num_rows($LoginRS);
 if ($loginFoundUser) {
    $loginStrGroup = "";
         if (PHP_VERSION >= 5.1) {session_regenerate_id(true);} else
{session_regenerate_id();}
   $_SESSION['MM_Username'] = $loginUsername;
   $_SESSION['MM_UserGroup'] = $loginStrGroup;
   if (isset($_SESSION['PrevUrl']) && false) {
     $MM_redirectLoginSuccess = $_SESSION['PrevUrl'];
   }
   header("Location: " . $MM_redirectLoginSuccess );
 }
 else {
   header("Location: ". $MM_redirectLoginFailed );
 }
}
?>
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head>
<link rel="shortcut icon" href="isgcmr.ico">
<?php
session_start();
?>
<title>Pagina Inicio</title>
<link href="hojas/layout01.css" rel="stylesheet" type="text/css" />
<link href="hojas/divs.css" rel="stylesheet" type="text/css" />
<link href="" media="screen" rel="stylesheet" type="text/css" />
<link href="hojas/style.css" rel="stylesheet" type="text/css" />
<script src="SpryAssets/SpryMenuBar.js" type="text/javascript"></script>
<link href="SpryAssets/SpryMenuBarHorizontal.css" rel="stylesheet"
type="text/css" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<style type="text/css">
body {
        background-color: #FFF;
        background-image: url(botones/degradado-fondo.jpg);
}
</style>
</head>
<body>
<form method="POST" action="<?php echo $loginFormAction; ?>">
<div id="wrapper">
   <div id="container">
   <div id="header">
  <img src="images/CEMENTERIO/bannercementerio.gif" width="855"
height="152" />
</div>
   <p> </p>
```

```
    <table width="325" height="94" border="0" align="center">
      <tr>
      <td width="92">Usuario</td>
      <td width="164"><input type="text" name="login" id="login" /></td>
      <td width="302" rowspan="3"><label for="login1"></label>  <label
for="password"><img src="Images/CEMENTERIO/candado.jpg" width="97"
height="90" /></label></td>
    </tr>
    <tr>
      <td>Contraseña</td>
      <td><input type="text" name="password" id="password" /></td>
      </tr>
    <tr>
      <td colspan="2" align="center"><input type="submit" name="button"
id="button" value="Ingresar" /></td>
      </tr>
</table>
  <p> </p>
  </div>
</div>
</form>
</body>
</html>
```

El método de logueo para las otras páginas está restriongido por el siguiente código:

```
<?php
if (!isset($_SESSION)) {
  session_start();
}
$MM_authorizedUsers = "";
$MM_donotCheckaccess = "true";
```

```
// *** Restrict Access To Page: Grant or deny access to this page
function isAuthorized($strUsers, $strGroups, $UserName, $UserGroup) {
  // For security, start by assuming the visitor is NOT authorized.
  $isValid = False;

  // When a visitor has logged into this site, the Session variable MM_Username set equal to their username.
  // Therefore, we know that a user is NOT logged in if that Session variable is blank.
  if (!empty($UserName)) {
    // Besides being logged in, you may restrict access to only certain users based on an ID established when they login.
    // Parse the strings into arrays.
    $arrUsers = Explode(",", $strUsers);
    $arrGroups = Explode(",", $strGroups);
    if (in_array($UserName, $arrUsers)) {
      $isValid = true;
    }
    // Or, you may restrict access to only certain users based on their username.
    if (in_array($UserGroup, $arrGroups)) {
      $isValid = true;
    }
    if (($strUsers == "") && true) {
      $isValid = true;
    }
  }
  return $isValid;
}

$MM_restrictGoTo = "index2.php";
```

```
if (!((isset($_SESSION['MM_Username'])) &&
(isAuthorized("",$MM_authorizedUsers, $_SESSION['MM_Username'],
$_SESSION['MM_UserGroup'])))) {
  $MM_qsChar = "?";
  $MM_referrer = $_SERVER['PHP_SELF'];
  if (strpos($MM_restrictGoTo, "?")) $MM_qsChar = "&";
  if (isset($_SERVER['QUERY_STRING']) &&
strlen($_SERVER['QUERY_STRING']) > 0)
  $MM_referrer .= "?" . $_SERVER['QUERY_STRING'];
  $MM_restrictGoTo = $MM_restrictGoTo. $MM_qsChar . "accesscheck=" .
urlencode($MM_referrer);
  header("Location: ". $MM_restrictGoTo);
  exit;
}
```

3.1.4.2 SECUENCIA DE COMANDOS CRUZADOS (XSS)

Para evitar esta vulnerabilidad se ha utilizado código para eliminar la información registrada de una sección en la cual no permitirá ejecutar y se convertirá todo a texto **(encriptado)**, es un leguaje muy fácil de utilizar, su sintaxis es simple y es muy rápido de configurar, estas líneas de código son solo un ejemplo ya que pueden existir varias formas de protección.

```
var_dump
session_destroy
<?php include("1_validar.php"); ?>:
lock code :
$name =$_GET['name'];        mejorar con  $name =htmlentities($_GET['name']);
$code = $_GET['code'];          mejorar con  $code = htmlentities($_GET['code']);
' or 1 = '1.
$pass=sha1($password);
$dos = sha1(md5($password));
```

3.1.4.3 FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS (CSRF)

Cuando se tiene una sección abierta en el navegador el código inmediatamente protege el robo de dominios y el cambio de contraseñas; este lenguaje es Open Source, tiene soporte de programación orientada a objetos, lo más importante es que puede conectarse con cualquier base de datos; este código solo es un ejemplo ya que pueden a ver varias formas de protección.

```
{
   public static function getToken()
   {
      $token = sha1(uniqid());
      $_SESSION['token'] = $token;
      return $_SESSION['token'];
   }

   public static function checkToken($token)
   {
      if (isset($_SESSION['token'])) {
         if ($token == $_SESSION['token']) {
            unset($_SESSION['token']);
            return true;
         }
      }
       return false;
   }
}
<?php
 session_start();
```

```
 if (isset($_POST['uname'], $_POST['token'])) {
  if (!empty($_POST['uname']) && !empty($_POST['token'])) {
   if (!Security::checkToken($_POST['uname'])) {
    // Show the error or redirect on home page!
    header('Location: index.php');
    die();
   }
    // Succeed!
   print_r($_POST);
  }
 }
?>
<html>
 <head>
  <title>CSRF - TheCodePress</title>
 </head>
 <body>
  <form action="index.php" method="POST">
   <label>Email:</label><br />
   <input type="text" name="uname" placeholder="Username" />
   <input type="hidden" name="token" value="<?php echo Security::getToken();
?>" />
  </form>
</body>
</html>
```

3.2 DESARROLLO DEL SISTEMA PARA EL CEMENTERIO MUNICIPAL DE RIOBAMBA.

3.2.1 METODOLOGÍAS DE DESARROLLO DE SOFTWARE

"Las metodologías de desarrollo de software son un conjunto de procedimientos, técnicas y herramienta que ayuda a los desarrolladores a realizar un software mediante un framework que es usado para estructurar, planear y controlar el proceso de desarrollo en sistemas de información.

El framework para metodología de desarrollo de software consiste en:

Es una filosofía de desarrollo de programas de computación con el enfoque del proceso de desarrollo de software. (Desarrollodefw.blogspot.com, Metodologías de Desarrollo de Software, 2012, pág. 1)

3.2.1.1 CARACTERÍSTICAS DE LAS METODOLOGÍA

- ✓ Existencia de reglas predefinidas
- ✓ Cobertura total del ciclo de desarrollo
- ✓ Verificaciones intermedias
- ✓ Planificación
- ✓ Control
- ✓ Comunicación efectiva
- ✓ Utilización sobre un abanico amplio de proyectos
- ✓ Fácil formación
- ✓ Herramientas CASE
- ✓ Actividades que mejoren el proceso de desarrollo
- ✓ Soporte al mantenimiento
- ✓ Soporte de la reutilización de software (Desarrollodefw.blogspot.com, Metodologías de Desarrollo de Software, 2012, pág. 3)

3.2.1.2 DIFERENCIAS ENTRE METODOLOGÍAS AGILES Y METODOLOGÍAS TRADICIONALES

Tabla 21. Diferencias de metodologías agiles y tradicionales

Metodologías Agiles	Metodologías Tradicionales
Son Adoptivas más predictivas	**Potencian la planificación detallada a largo plazo**
Procesos que se adoptan y progresan con el cambio	**Cuando existan cambios todo lo planificado puede venirse abajo**
Basadas en heurísticas provenientes de prácticas de producción de código	**Basadas en normas provenientes de están dar es seguidos por el entorno de desarrollo**
Especialmente preparados para cambios durante el proyecto	**Cierta resistencia a los cambios**
Impuestas internamente (por el equipo)	**Impuestas externamente**
Proceso menos controlado , con pocos principios	**Proceso mucho más controlado ,con numerosas políticas/normas**

Fuente: *PPT*. (Junio de 2012). Recuperado el 21 de Septiembre de 2013, de SoftLayer Technologies Inc.: http://www.slideshare.net/afrancoing/facci-metodologias-agiles

Adaptado por: Gavidia Marco & Jessica Valle

3.2.1.2.1 METODOLOGÍA ÁGIL PROGRAMACIÓN EXTREMA O XP.

Es una metodología para el desarrollo de software que consiste básicamente en ajustarse estrictamente a una serie de reglas que se centran en las necesidades del cliente para lograr un producto de buena calidad en poco tiempo.

La Programación Extrema es una metodología ágil centrada en potenciar las relaciones interpersonales como clave para el éxito en el desarrollo de software.

XP tuvo su origen a finales de 1980. A partir de entonces, sus prácticas fueron perfeccionadas y sus ideas se centraron en el desarrollo de un software que fuera, a la vez, adaptativo y orientado a las personas. (ETECSA, Febrero , pág. 10)

Este tipo de programación es la adecuada para los proyectos con requisitos imprecisos, muy cambiantes y con un riesgo técnico excesivo.

3.2.1.2.2 FASES DEL CICLO DE VIDA DE XP

Las Principales fases que comprende un proyecto al utilizar la metodología XP

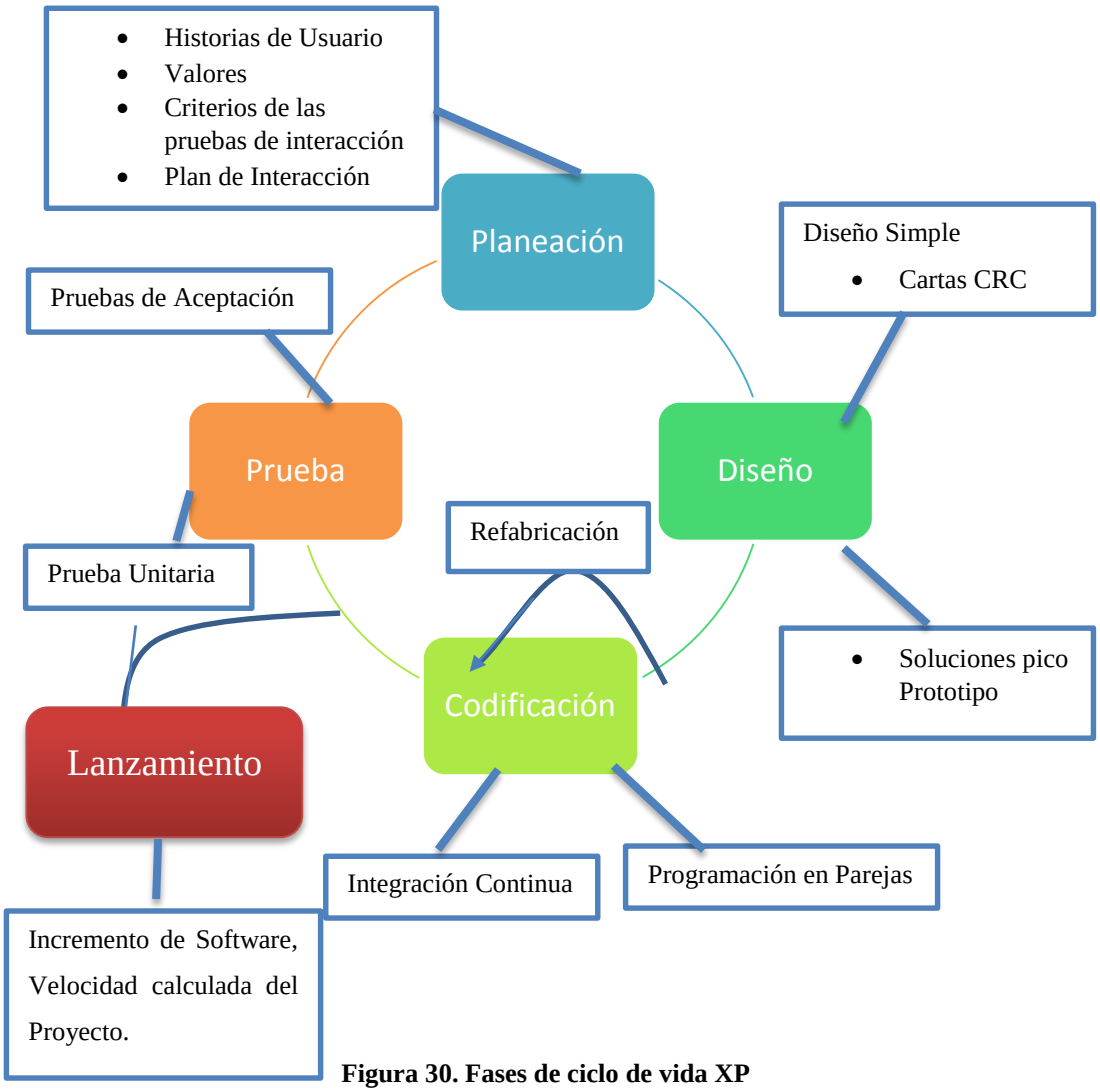


Figura 30. Fases de ciclo de vida XP

Adaptado por: Gavidia Marco & Jessica Valle

3.2.1.2.3 CRITERIOS DE SELECCIÓN DE LA METODOLOGÍA

Para comparar las metodologías de desarrollo no se propone ninguna técnica o regla comparativa debido a que cada metodología presenta un paradigma diverso, sin embargo existen criterios que los desarrolladores de software y aplicaciones web toman a consideración para que la metodología seleccionada ofrezca un óptimo funcionamiento.

- ✓ **Adaptación**

  Este criterio facilita conocer, prever la metodología con el tipo de solución que se busca a corto y largo plazo, y las alternativas posibles (Si es una metodología ágil tradicional).

- ✓ **Aceptación**

  La aceptación que da una metodología muestra una idea de los resultados que han obtenido en los proyectos que se han utilizado. Es decir una metodología que no proporcionara una solución aceptable, no habría ganado adeptos en el tiempo

- ✓ **Soporte**

  El soporte de una metodología, tiene toda la disponibilidad, así como la facilidad de adquisición de información referente a la metodología

- ✓ **Sencillez**

  Este parámetro se refiere a la facilidad de comprensión y la creación del modelamiento propuesto en una metodología, sin que esto conlleva la exclusión de aspectos necesarios: es decir que no haya lugar a confusión de sus declaraciones

- ✓ **Completitud**

  Este criterio está relacionado con la inclusión dentro de la metodología de todos los aspectos importantes en el proceso de desarrollo de la aplicación web, sin que esto conlleve a la redundancia.

3.2.1.2.4 COMPARACIÓN Y DISCUSIÓN

Una vez citado los criterios que se utilizaran para la ponderación en la comparación de la metodología (Metodología de Programación Extrema, Metodología Scrum) a utilizarse en el desarrollo del proyecto. Aquí se citan la forma de ponderación de acuerdo al siguiente detalle.

Opciones de Respuesta	Valor
Alta	5
Media Alta	4
Media	3
Media Baja	2
Baja	1

Figura 31. Opciones de respuesta comparación de Metodologías

Adaptado por: Gavidia Marco & Jessica Valle

La comparación entre las dos metodologías es consecuencia de la investigación realizada en distintas fuentes de información, de manera que puedan ser definidos, los criterios de respuesta, en base a la apreciación resultante de dicha investigación, como se muestra a continuación.

Adaptación

Al realizar la comparación es este criterio se ve que las metodología Programación Extrema (XP) es orientados al desarrollo ágil según la clasificación realizada, es así que esta metodología contemplan una adaptación alta. Mientras que la metodología Scrum es una metodología tradicional utilizada altamente en desarrollos de aplicaciones web y contempla una adaptación media alta.

Tabla 22. Valoración

ADAPATACIÓN	
XP	Alta
SCRUM	Media Alta

Adaptado por: Gavidia Marco & Jessica Valle

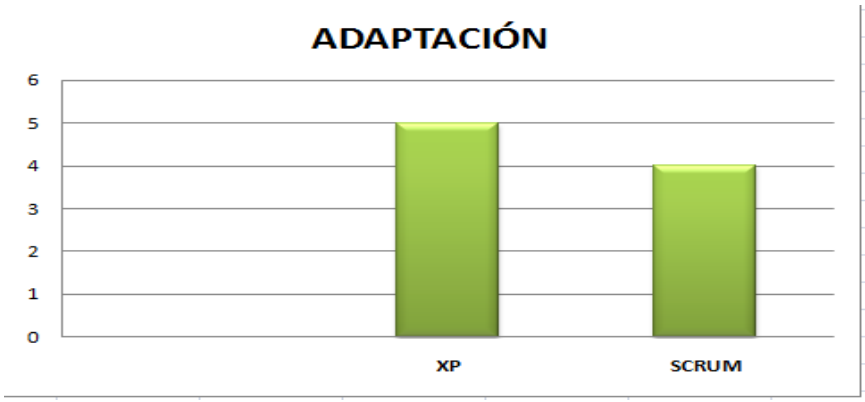


Figura 32. Adaptación de Metodologías Ágiles

Adaptado por: Gavidia Marco & Jessica Valle

Programación extrema (XP) es una metodología de desarrollo ágil y de acuerdo al proyecto planteado y la utilización de un framework para su desarrollo hace que esta metodología supere a la metodología SCRUM que se basa en la creación y asignación de tareas, pero no es una metodología ágil.

Aceptación

Al realizar la comparación entre las dos metodologías se puede apreciar que XP tiene una mayor aceptación, debido a que esta metodología ha tenido actualizaciones cambios permanentes en su estructura y es la que mayormente se ha utilizado contemplan una ponderación Alta. SCRUM que está orientada a la obtención de resultados para su desarrollo ágil le sigue con una ponderación media alta.

Tabla 23. Comparación de parámetros de Aceptación

ACEPTACIÓN	
XP	Alta
SCRUM	**Media Alta**

Adaptado por: Gavidia Marco & Jessica Valle

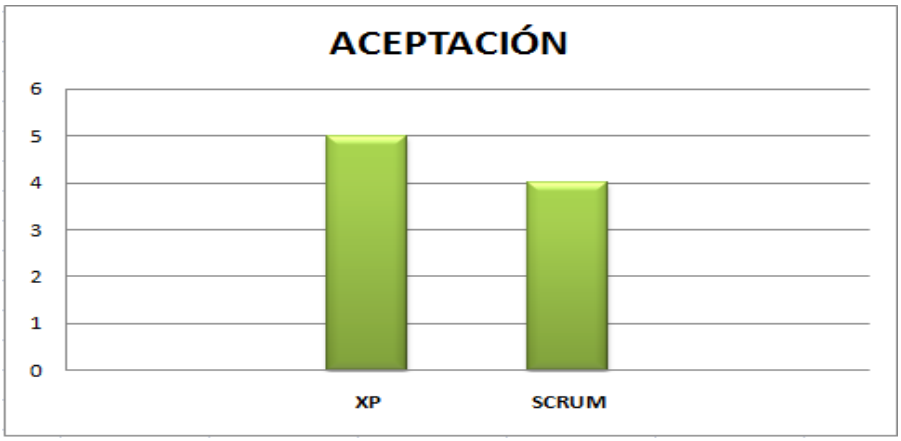


Figura 33. Comparación de Aceptación

Adaptado por: Gavidia Marco & Jessica Valle

La metodología XP tiene un alto nivel de aceptación especialmente por los dos tipos de pruebas que maneja durante todo su proceso, las pruebas del sistema y las pruebas de aceptación son herramientas que han ayudado para que sea ampliamente aceptado.

La metodología SCRUM es una metodología en auge, sus puntos de aceptación no son tan altos debido a la poca utilización, sin embargo hay parámetros a tomar en cuenta: en sus fases, la fase de especulación ya que se construirá el producto a partir de las ideas principales y se comprueban las partes realizadas y su impacto en el entorno.

Soporte

La facilidad para encontrar información sobre las metodologías en diferentes medios especialmente el internet, se aprecia que XP, tiene gran cantidad de documentales muy bien explicados por lo contempla una valoración media alta, y SCRUM con valoración baja.

Tabla 24. Comparación de Metodologías de Soporte

SOPORTE	
XP	Alta
SCRUM	Baja

Adaptado por: Gavidia Marco & Jessica Valle

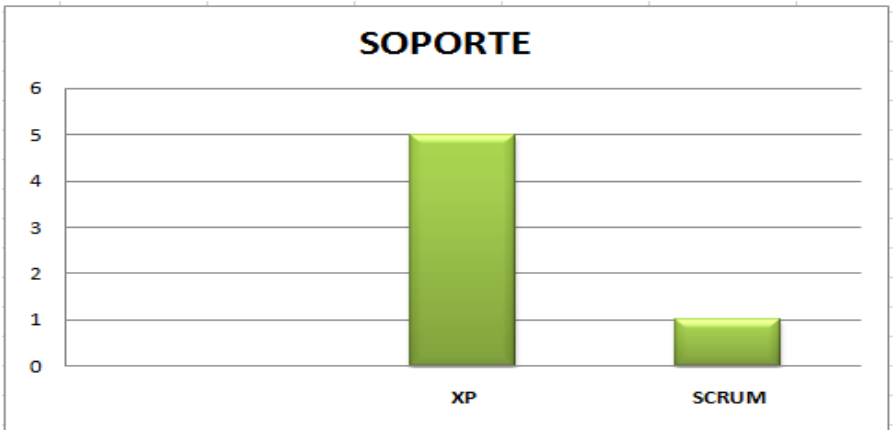


Figura 34. Comparación de Soporte

Adaptado por: Gavidia Marco & Jessica Valle

El soporte es un parámetro muy claro, se ha podido observar que el apoyo bibliográfico, y el acceso a estos es sencillo. Razón por la cual se ve viable efectuar metodología XP.

Sencillez

En cuanto a la sencillez analiza las fases que contemplan cada metodología; la fase de XP de post proyecto garantiza el mantenimiento de un portal web la valoración es media alta, mientras que la metodología SCRUM sus fases son muy generales y no destacan mucho por lo general es baja.

Las dos metodologías trabajan con el proceso interactivo – incremental

Tabla 25. Comparación de Metodologías de Sencillez

SENCILLEZ	
XP	Media Alta
SCRUM	Baja

Adaptado por: Gavidia Marco & Jessica Valle

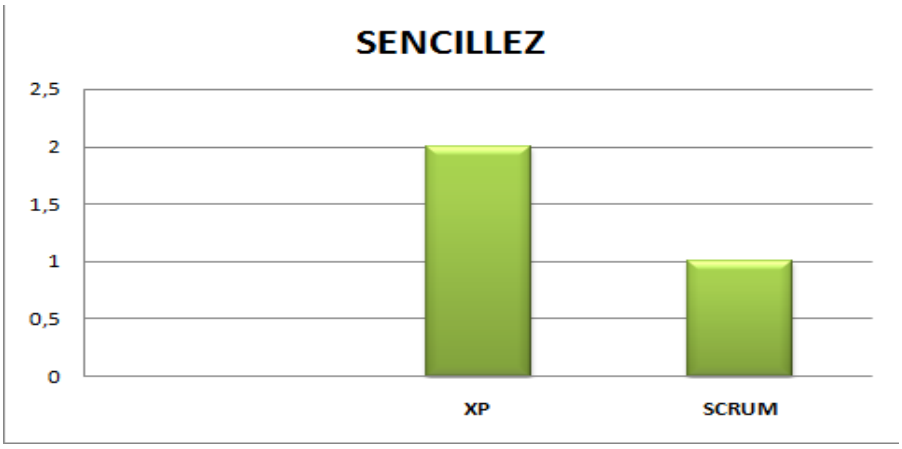


Figura 35. Comparación de la Sencillez

Adaptado por: Gavidia Marco & Jessica Valle

Las cuatro fase que maneja la metodología XP están muy bien identificadas las actividades que se van a realizar en cada una de ellas, la fase de planificación que abarca todo el estudio para evitar inconvenientes a futuro, la fase de diseño maneja todo el ciclo de vida de un software, la fase de codificación y la fase de pruebas.

En la metodología SCRUM resulta mayor trabajo al momento de realizar las fases para el desarrollo de Software que lleva a cabo.

Completitud

Al comparar las fases de la metodología XP se puede ver claramente que las fases abarcan todo el ciclo de vida de una aplicación web, a través de modelo funcionales de interacción en cada etapa de desarrollo y tiene una completitud media alta y en la metodología SCRUM las fases se basan en la teoría de control de procesos enfocado en el proceso iterativo e incremental para optimizar la predictibilidad y el control del riesgo se da una completitud media baja.

Tabla 26. Comparación de metodología de Completitud

COMPLETITUD	
XP	Media Baja
SCRUM	Media Alta

Adaptado por: Gavidia Marco & Jessica Valle

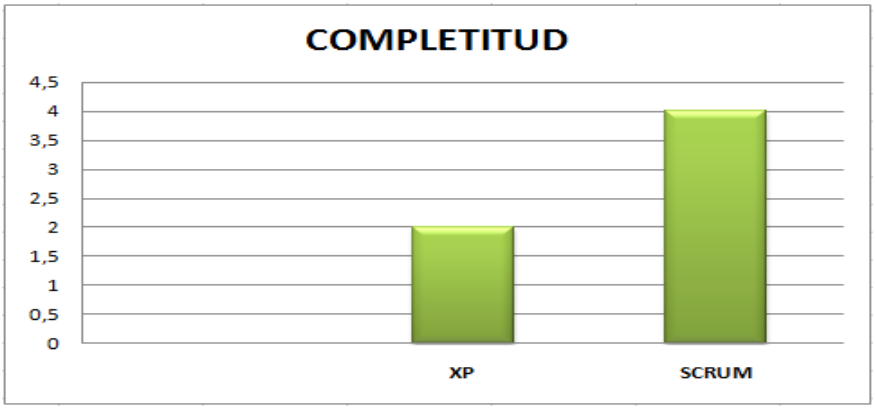


Figura 36. Comparación de Completitud

Adaptado por: Gavidia Marco & Jessica Valle

SCRUM en esta metodología profundiza un sistema iterativo que controlará los cambios de estado de la tarea, hasta que esta resulta completada, el factor más importante que apoya es la escalabilidad y en la metodología XP no profundiza los aspectos post proyecto que en aplicaciones web y especialmente portales web, la escalabilidad es el factor más influyente.

Consecuencia de la comparación

Tabla 27. Comparación General de las Metodologías XP, SCRUM

CRITERIO	XP		SCRUM	
	Respuesta	**Valor**	**Respuesta**	**Valor**
Adaptación	Alta	5	Media Alta	4
Aceptación	Media Alta	5	Alta	4
Soporte	Media	5	Media	1
Sencillez	Media Alta	2	Media	1
Completitud	Media Alta	2	Media Alta	4
		19		**14**

Figura 37. Comparación de Metodologías de Desarrollo

Adaptado por: Gavidia Marco & Jessica Valle

Figura 38. Resultado General de las Metodologías

Adaptado por: Gavidia Marco & Jessica Valle

En base a las ponderaciones realizadas en la sección y de acuerdo a los parámetros planteados en la sección se puede apreciar que la metodología de desarrollo ágil en aplicaciones web XP supera a la metodología SCRUM, por tal razón se utilizara la metodología ágil de desarrollo de aplicaciones web XP (Programación Extrema) en el desarrollo del sistema Informático para el Cementerio Municipal de Riobamba.

3.2.1.2.5 FASES DE LA METODOLOGIA XP

A. FASE: PLANIFICACIÓN DEL PROYECTO.

- ✓ **Historias de usuario**

Las historias de usuario tienen la misma finalidad que los casos de uso. Son usadas para estimar tiempos de desarrollo de la parte de la aplicación que describen. También se utilizan en la fase de pruebas, para verificar si el programa cumple con lo que especifica la historia de usuario. Cuando llega la hora de implementar una historia de usuario, el cliente y los desarrolladores se reúnen para concretar y detallar lo que tiene que hacer dicha historia.

En la fase de Planificación se establece la creación de historias de usuarios que equivale a los requisitos funcionales de IEEE830.

Estos son los requisitos funcionales extraídos de las historias de usuarios de la fase de planificación en XP:

- Iniciar Sesión: Autenticación de usuario con nombre y contraseña
- Cementerio: Ingresar, actualizar, eliminar y listar
- Sector: Ingresar, actualizar, eliminar y listar
- Sección: Ingresar, actualizar, eliminar y listar
- Trabajador: Ingresar, actualizar, eliminar y listar
- Categoría (de tumba): Ingresar, actualizar, eliminar y listar
- Tipo (de Cargo): Ingresar, actualizar, eliminar y listar
- Nichos: Ingresar, actualizar, eliminar y listar
- Sepultura: Ingresar, actualizar, eliminar y listar
- Mausoleo: Ingresar, actualizar, eliminar y listar
- Usuario: Ingresar, actualizar, eliminar.
- Familiar: Ingresar, actualizar, buscar, eliminar y listar
- Fallecido: Ingresar, actualizar, buscar, eliminar y listar
- Tumba: Ingresar, actualizar, buscar, eliminar y listar
- Asignar: Nicho, Sepultura y Mausoleo.
- Ayuda
- Reportes:
    - Total Nichos por sección
    - Total Sepulturas por sección
    - Total Mausoleos por sección

B. FASE: DISEÑO.

✓ DISEÑOS SIMPLES:

La metodología X.P sugiere conseguir diseños simples y sencillos. Hay que procurar hacerlo todo lo menos complicado posible para conseguir un diseño fácilmente entendible e impleméntale que a la larga costará menos tiempo y esfuerzo desarrollar.

Figura 39. Diseño Simple para el Sitio Web

Adaptado por: Gavidia Marco & Jessica Valle

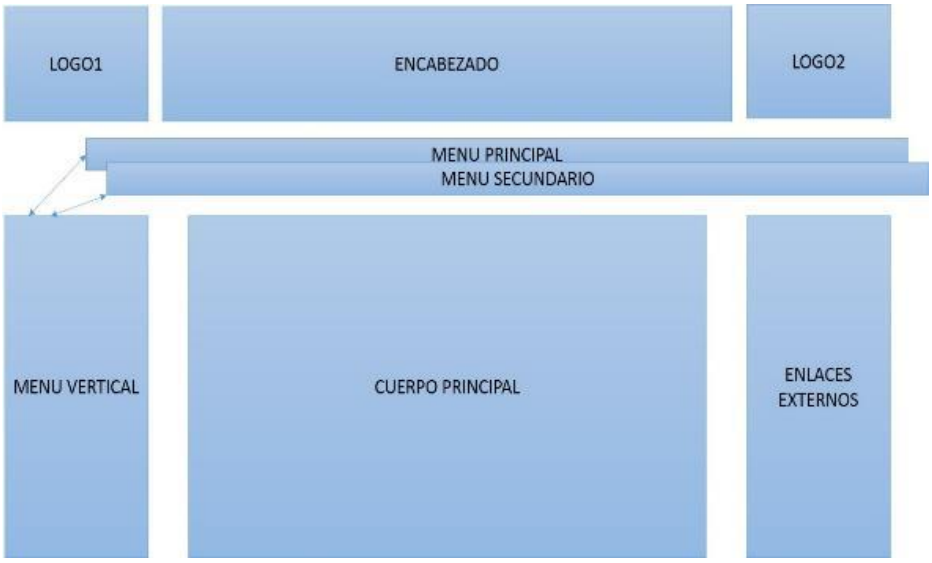


Figura 40. Diseño simple para Sistema CMR

Adaptado por: Gavidia Marco & Jessica Valle

C. FASE: CODIFICACIÓN.

La codificación debe hacerse a través de estándares de codificación ya creados. Programar bajo estándares mantiene el código consistente y facilita su comprensión y escalabilidad.

Crear test que prueben el funcionamiento de los distintos códigos implementados ayudará a desarrollar dicho código.

Crear estos test antes ayudara a saber qué es exactamente lo que tiene que hacer el código a implementar y se conocerá que una vez implementado pasará dichos test sin problemas ya que dicho código ha sido diseñado para ese fin.

Como ya se comentó anteriormente. X.P opta por la programación en pareja ya que permite un código más eficiente y con una gran calidad.

X.P también propone un modelo de desarrollo colectivo en el que todos los programadores están implicados en todas las tareas; cualquiera puede modificar o ampliar una clase o método de otro programador si es necesario y subirla al repositorio de código. El permitir al resto de los programadores modificar códigos que no son suyos no supone ningún riesgo ya que para que un código pueda ser publicado en el repositorio tiene que pasar los test de funcionamiento definidos para el mismo.

La optimización del código siempre se debe dejar para el final. Hay que hacer que funcione y que sea correcto, más tarde se puede optimizar.

En esta fase se coloca la programación en PHP y mysql, un ejemplo es el siguiente:

OPERACIÓN DE INGRESAR USUARIO

```
<?php
if( isset($_GET["Login"]) ){
   $login = $_GET["Login"];
}else{
   $login="";
}

if( isset($_GET["Clave"]) ){
   $clave = $_GET["Clave"];
}else{
   $clave="";
}

if( isset($_GET["Nombre"]) ){
```

```
   $nombre = $_GET["Nombre"];
}else{
    $nombre="";
}

if( isset($_GET["Apellido"]) ){
   $apellido = $_GET["Apellido"];
}else{
    $apellido="";
}

if( isset($_GET["Direccion"]) ){
   $direccion = $_GET["Direccion"];
}else{
    $direccion="";
}
if( isset($_GET["Telefono"]) ){
    $telefono = $_GET["Telefono"];
}else{
    $telefono="";
}
if( isset($_GET["estado"]) ){
    $estado = $_GET["estado"];
}else{
    $estado="ok";
}
include("conexion.php");
$sql = "select MAX(IdUsuario) as ultimo from usuario";
$resultado = mysql_query($sql,$con);
//echo $sql;
```

```
while( $row = mysql_fetch_array($resultado))
{
   $ultimo = $row["ultimo"] ;
}
$id= $ultimo+1;
?>
```

Por motivos de que las líneas de código son extensas no se ha colocado la programación de todo el sistema, sin embargo en la siguiente imagen se puede observar con un diagrama entidad relación y también el diagrama de clases para poder conocer como está estructurado el sistema en la parte de codificación.

D. FASE: PRUEBAS.

La metodología XP menciona que se deben realizar pruebas a lo largo del proyecto, con el fin de asegurar en todo momento la realización de lo planteado en el diseño. En este proceso participa el equipo de desarrollo y también el cliente para las pruebas de aceptación

El Diseño de Pruebas se realiza para todas las partes del sistema como una práctica para garantizar el buen funcionamiento independientemente de las herramientas utilizadas.

Las pruebas deben ser automatizadas para que puedan ejecutarse de manera fácil y rápida. De esta forma se puede modificar el código y asegurarnos que funciona correctamente con los cambios producidos.

PRUEBAS UNITARIAS

Para realizar las pruebas unitarias se ha tomado en consideración el sitio web y el sistema CMR.

Sitio web para el Cementerio Municipal de Riobamba

Para realizar las pruebas en Joomla se usa gestor de base de datos, Php My admin o Mysql Administrador se crea una copia de respaldo de la base de datos antes de instalar cualquier módulo o componente, luego crear una base de datos de pruebas,

ejemplo bdpruebas, y copiar allí todo tu respaldo, ahora ya se tiene 2 bases de datos iguales, la original y la otra de pruebas.

Luego se ubica el archivo configuration.php que se encuentra en la raíz de la instalación de Joomla y modificar la siguiente línea de código

Línea original:

var $db = 'bdoriginal';

Línea modificada:

var $db = 'bdpruebas';

De esta manera se puede tener Joomla controlado contra posibles errores que genere el módulo o componente a instalar, de esta manera si algo llega a fallar o lo encuentras diferente a como estaba antes de instalar, con sólo volver el nombre original de la base de datos lo tendrás igual e intacto.

Sistema CMR

Para hacer pruebas en el Sistema CMR se tiene la ayuda de herramientas de dreamweaver o sitios web online donde se puede hacer pruebas de código como por ejemplo http://writecodeonline.com/php/ el cual permite probar en código en tiempo real.

CASOS DE USO

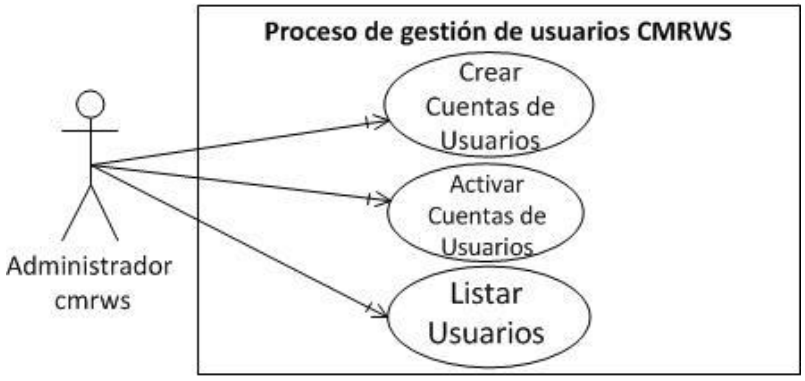


Figura 41. Caso de uso del proceso de gestión de usuarios CMRWS

Adaptado por: Gavidia Marco & Jessica Valle

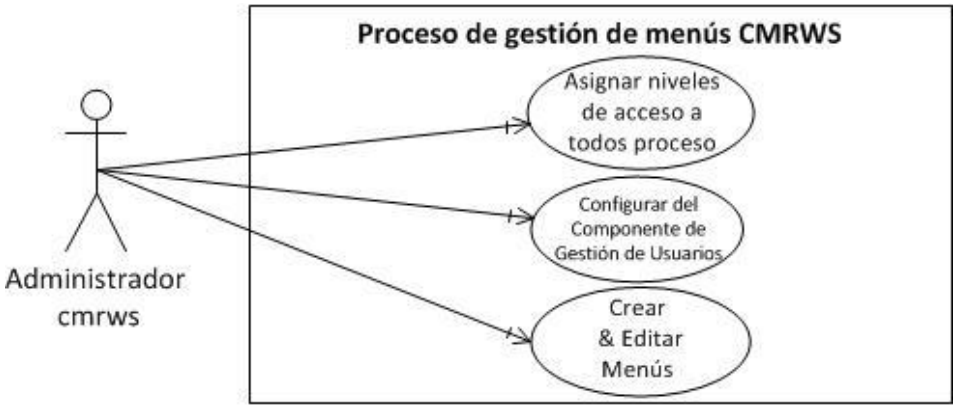


Figura 42. Caso de uso del proceso de gestión de menús CMRWS

Adaptado por: Gavidia Marco & Jessica Valle

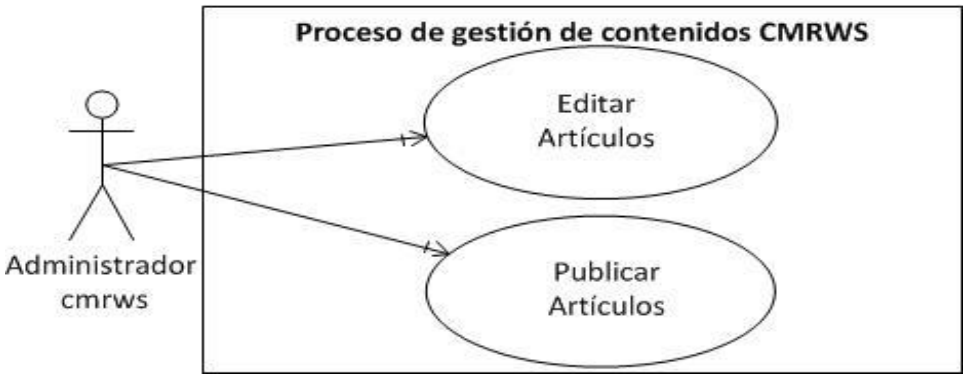


Figura 43. Caso de uso del proceso de gestión de contenidos CMRWS

Adaptado por: Gavidia Marco & Jessica Valle

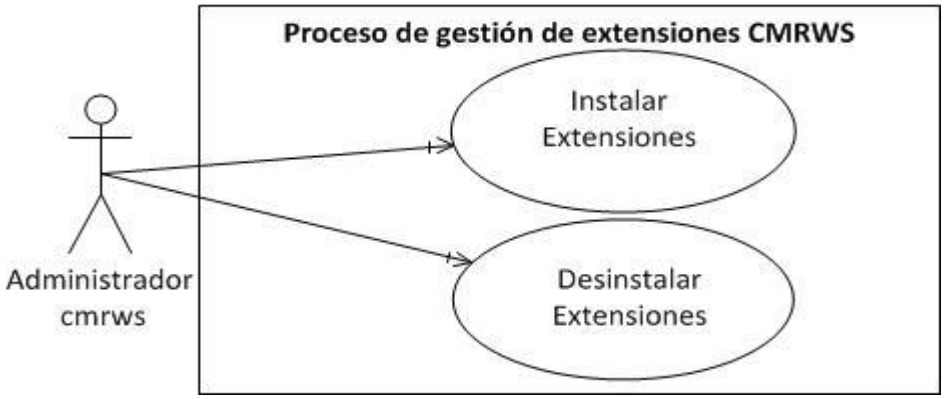


Figura 44. Caso de uso del proceso de gestión de extensiones CMRWS

Adaptado por: Gavidia Marco & Jessica Valle

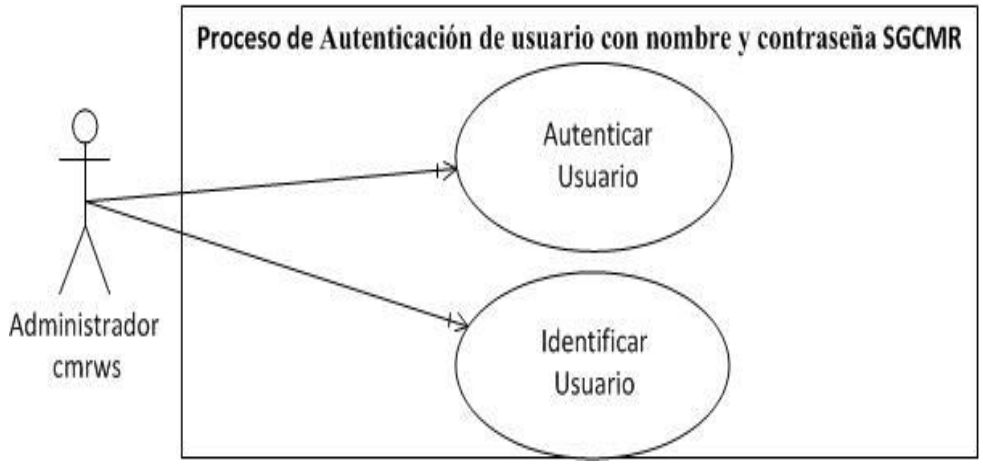


Figura 45. Caso de uso del proceso de Autenticación de usuario del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

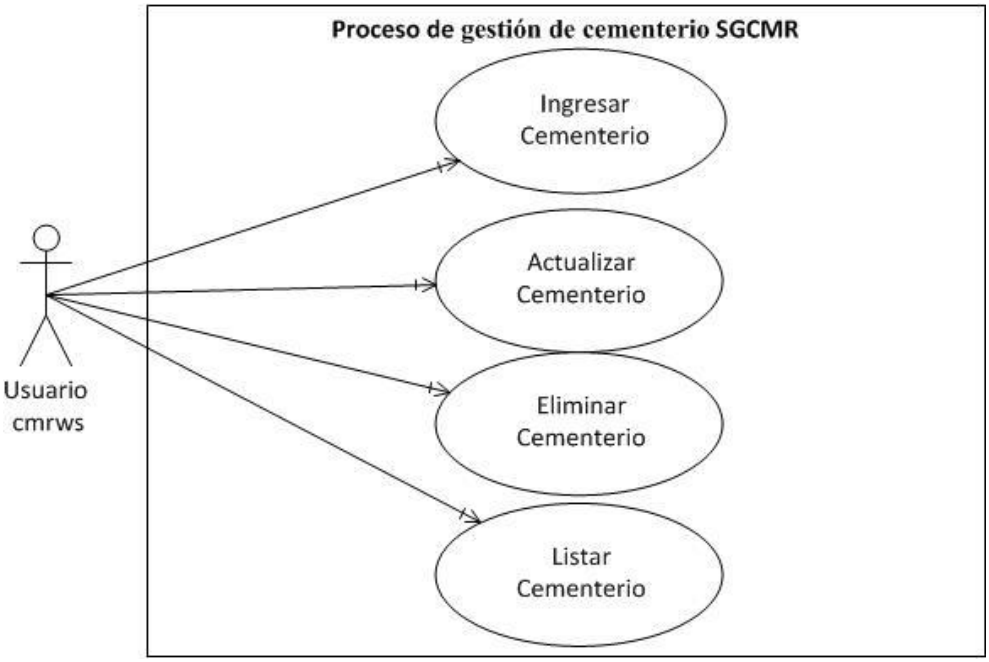


Figura 46. Caso de uso del proceso de gestión de Cementerio del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

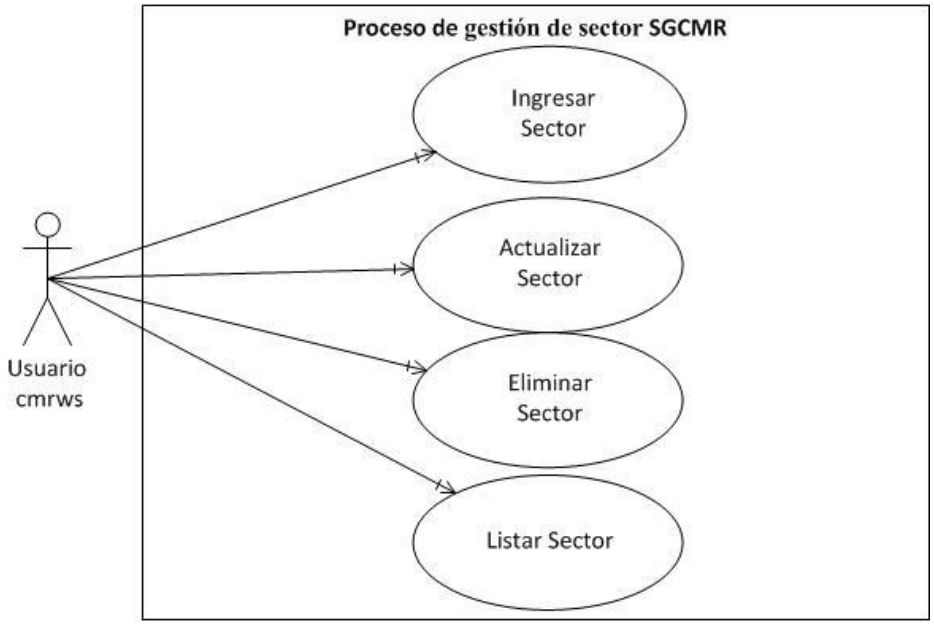


Figura 47. Caso de uso del proceso de gestión de Sector del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

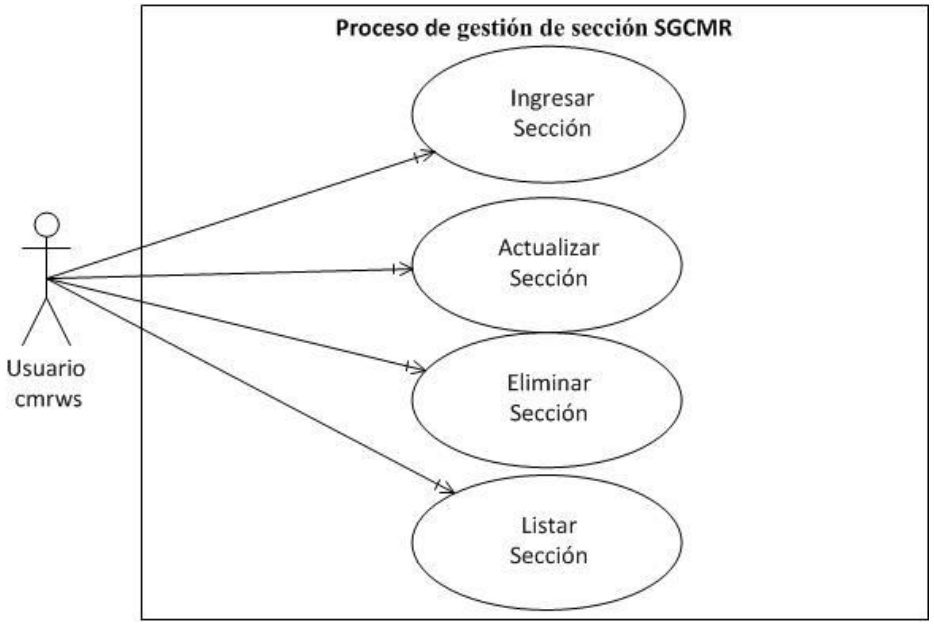


Figura 48. Caso de uso del proceso de gestión de Sección del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

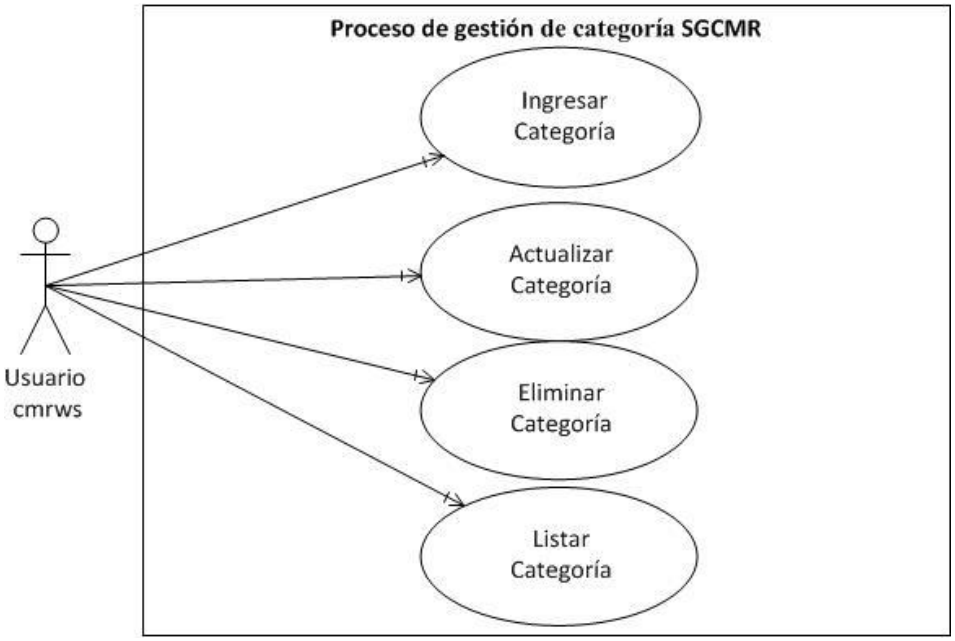


Figura 49. Caso de uso del proceso de gestión de Categoría del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

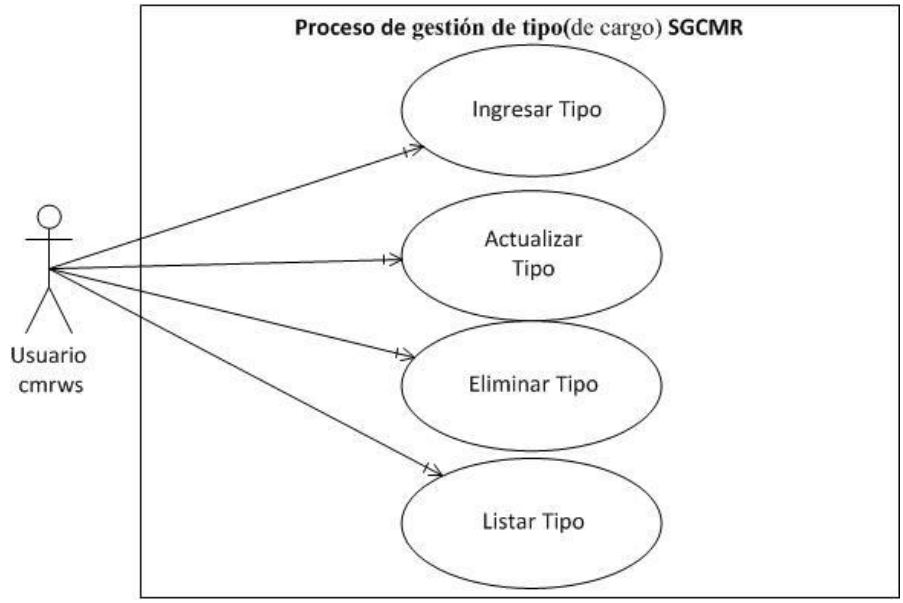


Figura 50. Caso de uso del proceso de gestión de Tipo del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

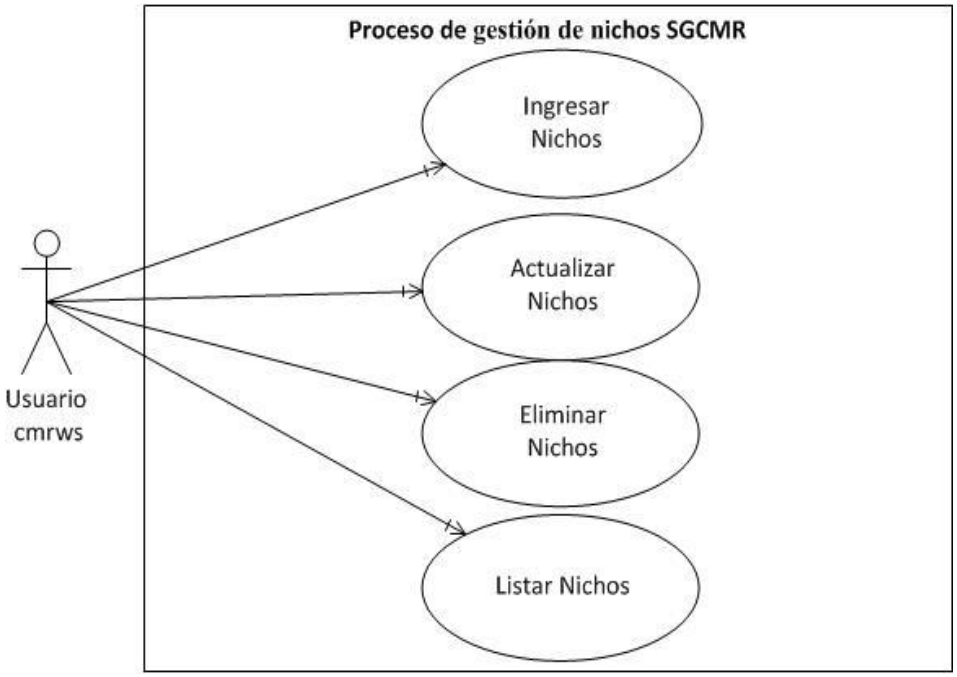


Figura 51. Caso de uso del proceso de gestión de nichos del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

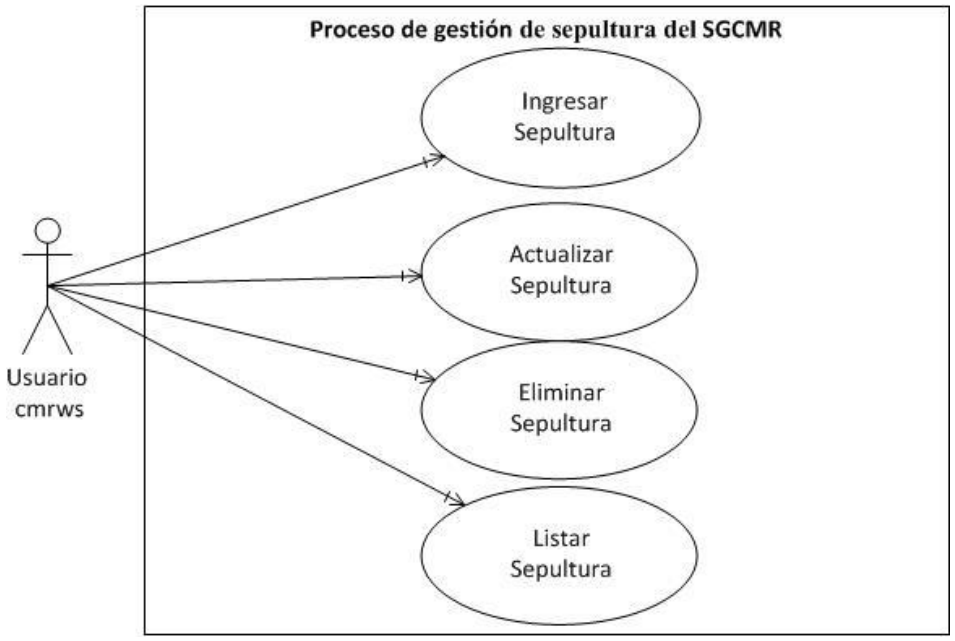


Figura 52. Caso de uso del proceso de gestión de sepultura del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

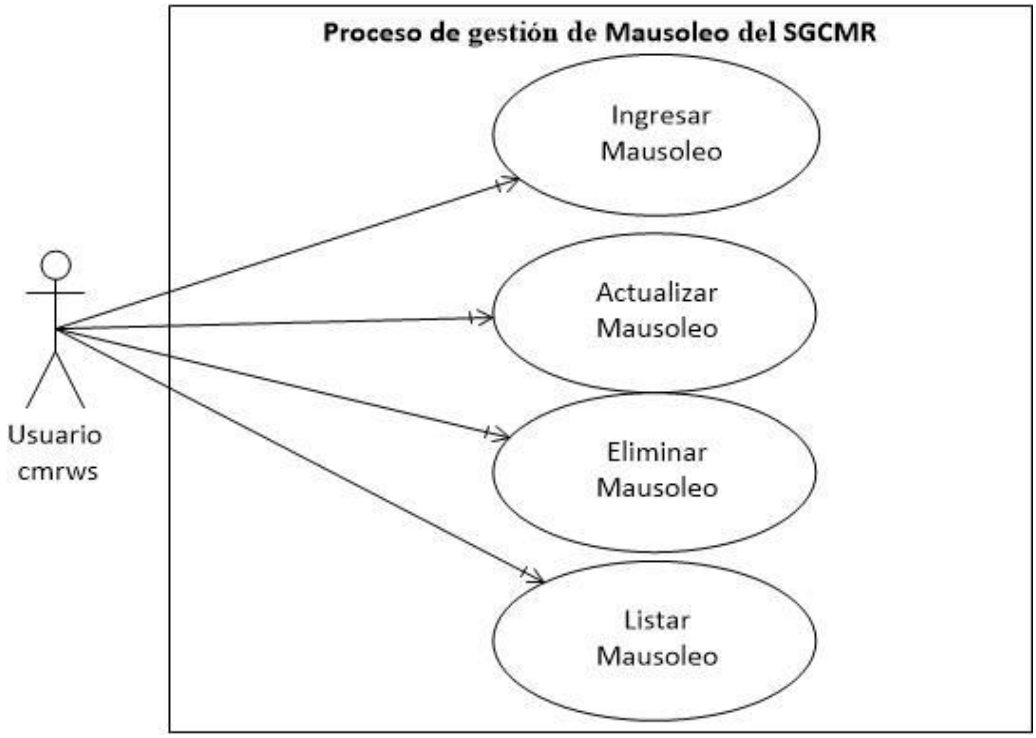


Figura 53. Caso de uso del proceso de gestión de mausoleo del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

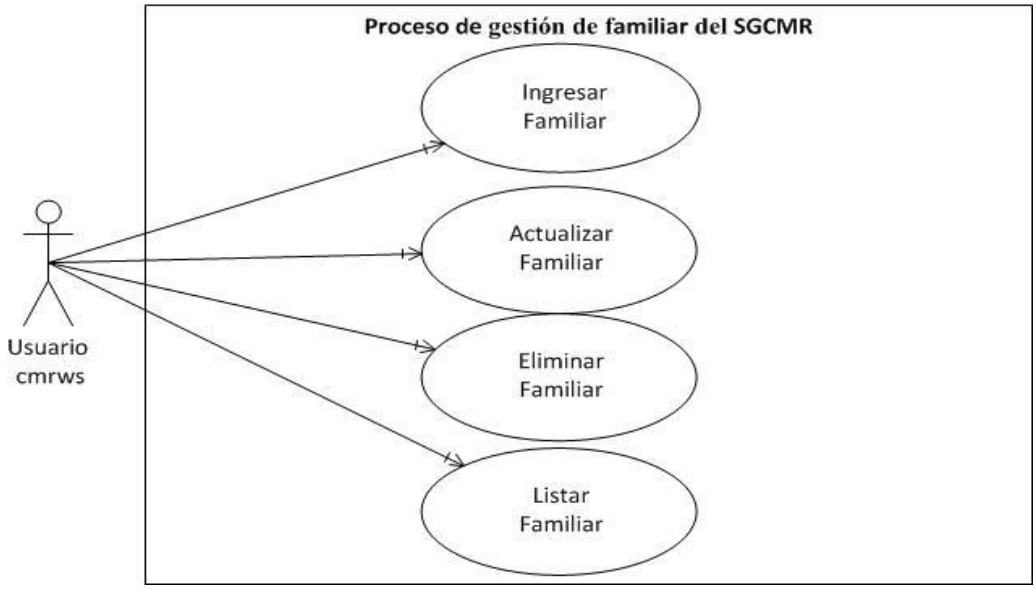


Figura 54. Caso de uso del proceso de gestión de familiar del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

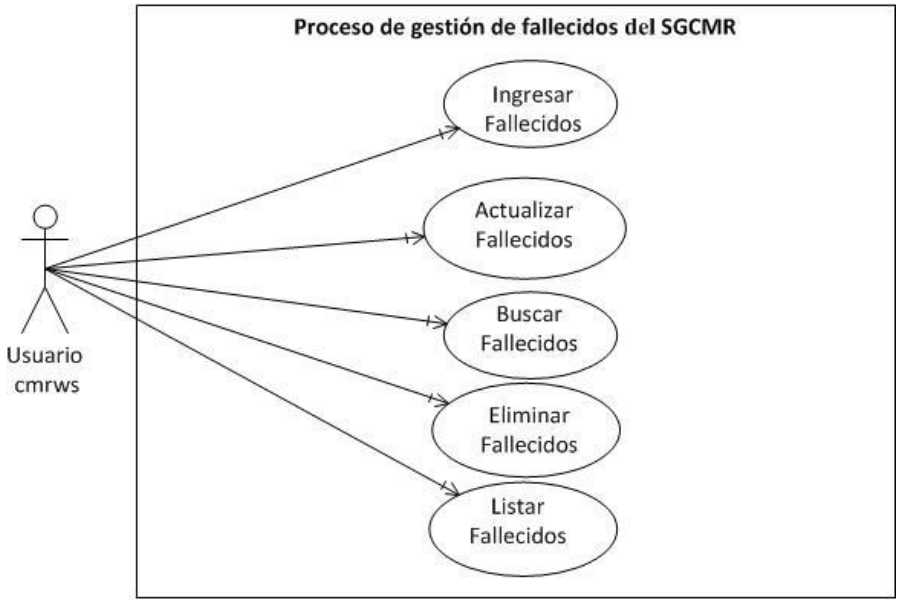


Figura 55. Caso de uso del proceso de gestión de Fallecido del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

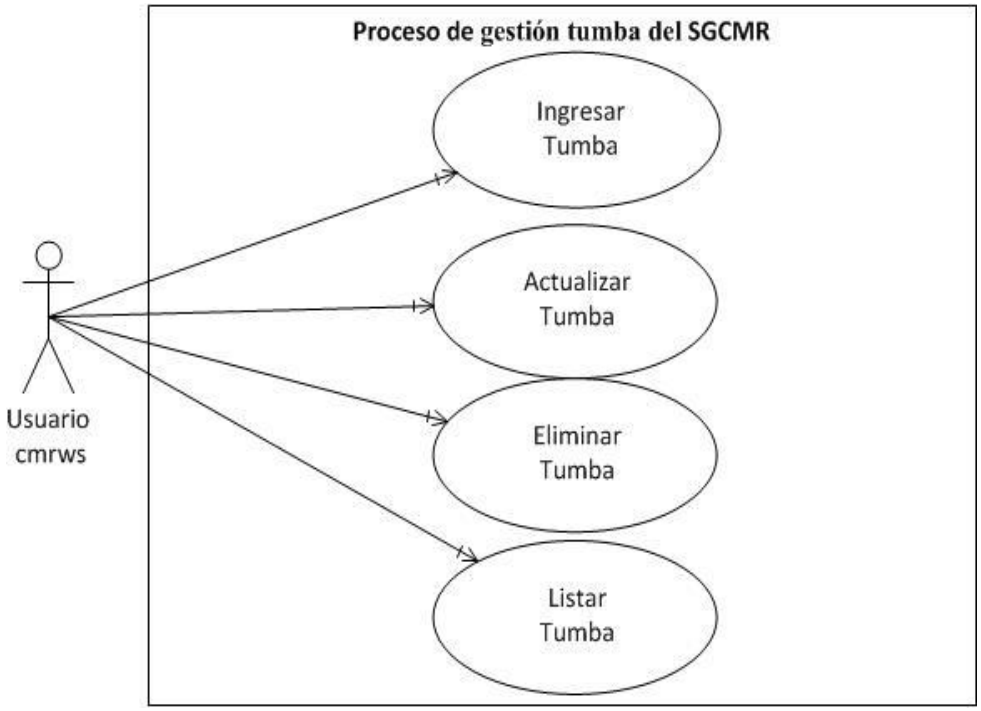


Figura 56. Caso de uso del proceso de gestión de tumbas del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

Figura 57. Caso de uso del proceso de Registro de Asignación del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

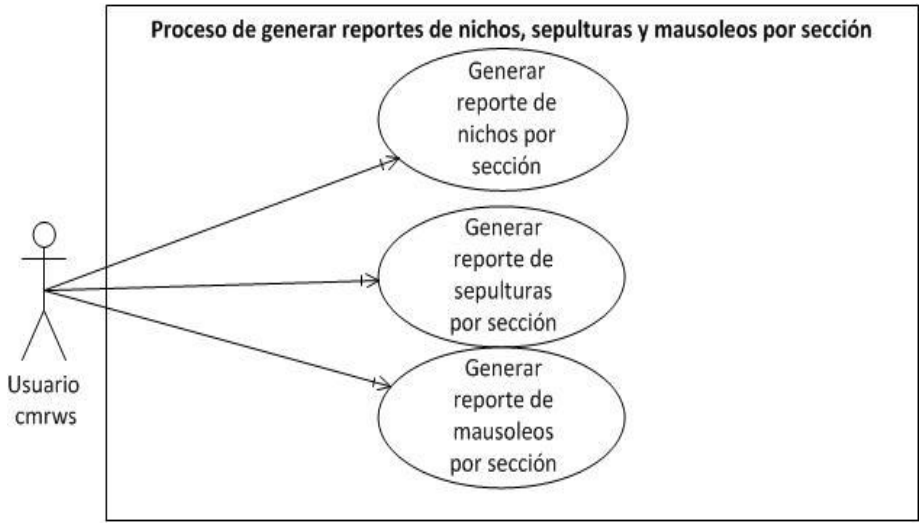


Figura 58. Caso de uso del proceso de generación de reportes del SGCMR

Adaptado por: Gavidia Marco & Jessica Valle

MODELO ENTIDAD RELACION

Con los datos obtenidos en la especificación de requisitos se plantea el siguiente modelo relacional, el esquema planteado en la Figura 61 muestra un total de 12 tablas las cuales se describen todos los campos definidos:

Tabla "Cementerio" almacena los datos de los cementerios que se encuentran a cargo, los datos de esta tabla son los siguientes:

- ✓ IdCementerio
- ✓ Nombre
- ✓ Dirección
- ✓ Teléfono

Tabla "Sector" almacena los datos de los 5 sectores que se encuentra divido el Cementerio Municipal de Riobamba.

- ✓ IdSector
- ✓ IdCementerio
- ✓ NombreSector

Tabla "Sección" almacena los datos de los bloques y filas de cada sector. Para ello se tiene:

- ✓ IdSección
- ✓ IdSector
- ✓ NombreSección

Tabla "Mausoleo" almacena el número de tumbas en la que se encuentran sepultadas las personas. Para lo cual se necesita:

- ✓ Id Mausoleo
- ✓ IdTumba
- ✓ IdSección
- ✓ Numero_Mausoleo
- ✓ Mantenimiento
- ✓ Observación

Tabla "Nicho" almacena el número de nicho en la que se encuentran exhumadas las personas. En esta tabla se ingresaran los siguientes datos:

- ✓ IdNicho
- ✓ IdSeccion
- ✓ IdTumba
- ✓ Numero_Nicho
- ✓ Mantenimiento
- ✓ Observación

Tabla "Sepultura" almacena el número del sarcófago en la que se encuentran sepultadas las personas, para eso se requiere:

- ✓ IdSepultura
- ✓ IdTumba

- ✓ IdSección
- ✓ Numero_Sepultura
- ✓ Renovación
- ✓ Observación

Tabla "Tumba" almacena el número de la bóveda en la que se encuentran sepultadas las personas, los datos son los siguientes:

- ✓ IdTumba
- ✓ IdCategoria

Tabla "Categoría" almacena los datos de cada tumba, si son de propiedad o municipal para lo cual se necesita:

- ✓ IdCategoria
- ✓ Nombre_Categoria

Tabla "Fallecido" almacena los datos personales de cada fallecido, para eso se requieren:

- ✓ IdFallecido
- ✓ FechaFallecido
- ✓ IdTumba
- ✓ NombreFallecido
- ✓ IdFamiliar
- ✓ ApellidoFamiliar

Tabla "Familiar" almacena los datos personales del familiar que va a estar a cargo de la persona fallecida, los datos son:

- ✓ IdFamiliar
- ✓ Cédula
- ✓ NombreFamiliar
- ✓ ApellidoFamiliar
- ✓ TeléfonoFamiliar
- ✓ DirecciónFamiliar
- ✓ Correo

Tabla "Trabajador" almacena los datos personales del Trabajador y el sector en el que va a trabajar, para ello se requiere:

- ✓ IdTrabajador
- ✓ IdTipo
- ✓ IdCementerio
- ✓ NombreTrabajador
- ✓ ApellidoTrabajador
- ✓ Salario

Tabla "Cargo" almacena los datos de la dignidad que tiene cada Trabajador, los datos son:

- ✓ IdCargo
- ✓ IdTrabajador
- ✓ NombreCargo

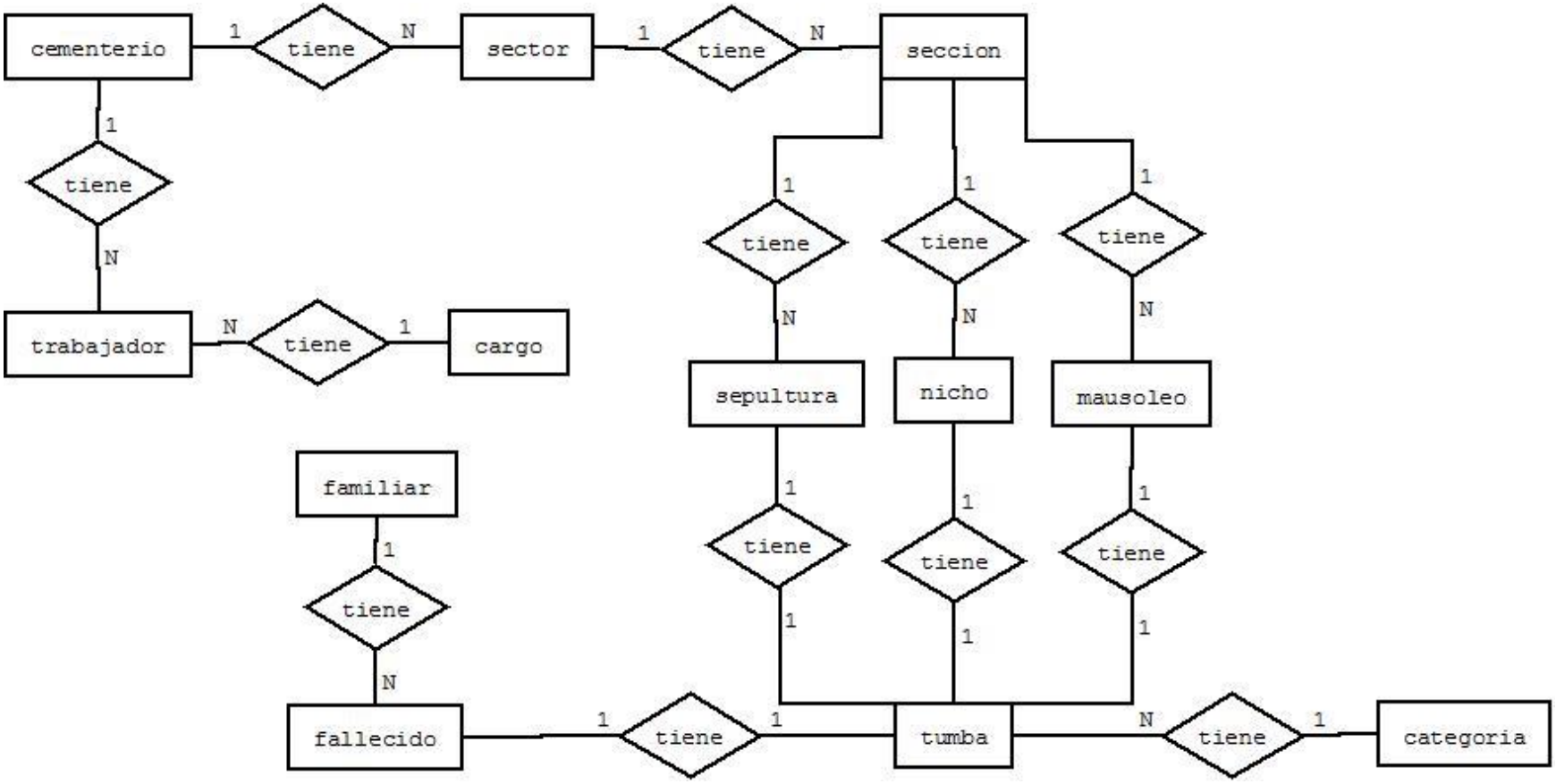


Figura 59. Diagramas Entidad relación

Adaptado por: Gavidia Marco & Jessica Valle

DIAGRAMA DE CLASES

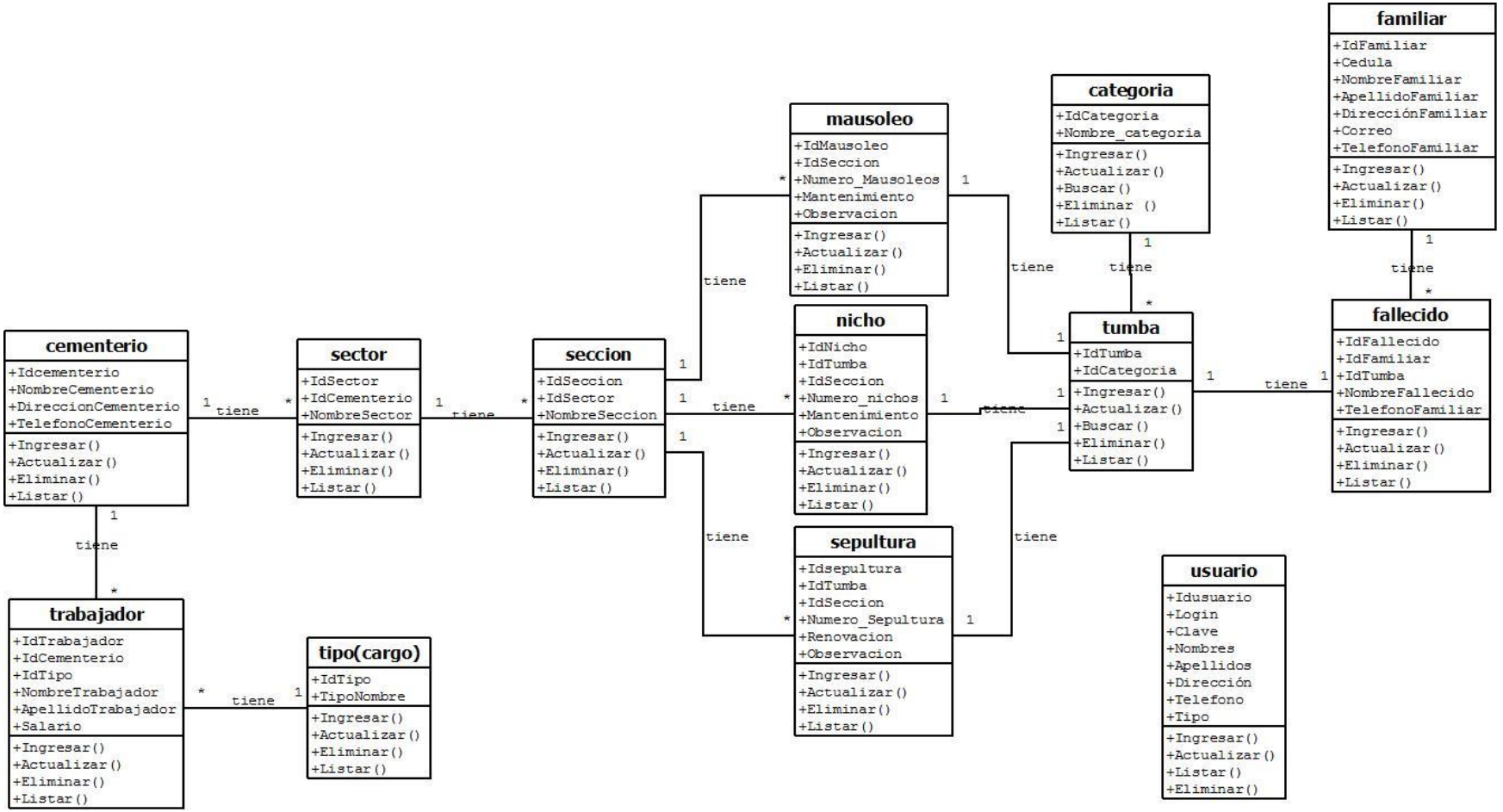


Figura 60. Diagramas de Clases
Adaptado por: Gavidia Marco & Jessica Valle

CAPÍTULO IV

METODOLOGÍA

4.1 TIPO DE ESTUDIO

4.1.1 DESCRIPCIÓN DE LA METODOLOGÍA

La metodología es el estudio de los procedimientos en la adquisición o exposición del conocimiento científico, conjuntos de procedimientos de investigación aplicables en alguna ciencia.

La metodología comprende un conjunto de reglas que surgen del estudio de una disciplina científica.

En la presente investigación se han aplicado los siguientes métodos:

Método Inductivo- Deductivo.- Se lleva a cabo una etapa de observación y registro de los hechos. A continuación se procederá al análisis de lo observado.

Método Experimental.- Análisis de las diversas herramientas software utilizadas para el modelado de datos, diseño de datos, diseño de interfaz, programación web a utilizarse en el proyecto.

Método Bibliográfico.- Se determina las fuentes más importantes que proporcionen información y documentación como: código fuente, libros, scripts, etc.

4.2 POBLACIÓN MUESTRA

4.2.1 POBLACIÓN

La población son 10 tipos de vulnerabilidades que son las más comunes e importantes que afectan en los sistemas informáticos según OWASP TOP TEN PROJECT. (OWASP, OWASP Top Ten 2013 Proyect, 2013)

4.2.2 MUESTRA

La muestra son los 3 tipos más frecuentes de vulnerabilidades para analizar.

4.2.3 HIPÓTESIS

El análisis de vulnerabilidades de software puede mejorar la seguridad en los Sistemas Informáticos

- ✓ **H1.-**Con el análisis de vulnerabilidades de software se mejorará la seguridad del sistema Informático del Cementerio Municipal de Riobamba?
- ✓ **Ho.-**Con el análisis de vulnerabilidades de software no se mejorará la seguridad del sistema Informático del Cementerio Municipal de Riobamba?

Se pensaría que en el Cementerio Municipal de Riobamba con un sistema debidamente protegido mejorará la seguridad del sistema, dando como resultado un sistema seguro y eficiente.

4.2.4 IDENTIFICACIÓN DE VARIABLES

Tabla 28. Tabla de variables dependiente e independiente

Objetivos	Variables
✓ Analizar las vulnerabilidades de Software para mejorar la seguridad en los Sistemas Informáticos.	✓ **Dependiente** Análisis de la vulnerabilidad de software ✓ **Independiente** Mejora de la seguridad en los Sistemas Informáticos.

Adaptado por: Gavidia Marco & Jessica Valle

4.3 OPERACIONALIZACIÓN DE VARIABLES

Tabla 29. Operacionalización de las variables

OBJETIVO	VARIABLE	CONCEPTO	INDICADOR	TÉCNICA E INSTRUMENTO
Analizar las vulnerabilidades de Software para mejorar la seguridad en los Sistemas Informáticos.	• **Dependiente** Análisis de la vulnerabilidad de software	Proceso de inspeccionar, estudiar cualquier defecto que tiene los activos de software y datos que permiten explotarlos con el fin de que el atacante pueda hacerse con el control del sistema.	Comparación cualitativa y cuantitativa de las vulnerabilidades. Seguridad y protección por vulnerabilidades. Encuestas Funcionalidad	Porcentaje de Satisfacción
	• **Independiente** Mejora de la seguridad en los Sistemas Informáticos.	Diseño de la seguridad de los datos en sistemas automatizados al momento de asegurar un nivel aceptable de riesgo.	Medida de desempeño Análisis cualitativo y cuantitativo de las seguridades del Sistema Pruebas ante vulnerabilidades Encuestas	Porcentaje de Mejora Porcentaje de Satisfacción

Adaptado por: Gavidia Marco & Jessica Valle

4.4 PROCEDIMIENTOS

Para la recopilación de la información se realizaran algunos procedimientos.

La técnica de investigación que se empleará:

Entrevista: a los usuarios del sistema, trabajadores del Cementerio que manejan el sistema.

Encuesta: trabajadores del Cementerio que manejan el sistema para conocer la ubicación y localización de las personas fallecidas.

Observación: Se realizará pruebas con programas y aplicaciones web para ver las vulnerabilidades de software y datos.

Análisis: Análisis documental, tablas de resultados, estándares, mediciones, ponderaciones cualitativas y cuantitativas.

Organización y tabulación de la información.

4.4.1 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Los instrumentos que se utilizaron para la recolección de datos fueron

- ✓ Entrevistas
- ✓ Encuestas
- ✓ Observación
- ✓ Análisis

Además de la utilización de los mecanismos de protección contra las vulnerabilidades obtenidas.

CAPÍTULO V

PROCESAMIENTO Y ANALISIS

Para determinar si el análisis de vulnerabilidades de software tiene un valor significativo se realizó la prueba del t- student para el análisis de datos, mediante esta prueba se puede calificar si la seguridad del sistema Informático del Cementerio Municipal de Riobamba ha tenido un cambio significativo en comparación con los datos que se tenía al principio el sistema.

T- Student es una distribución de probabilidad que surge del problema de estimar la media de una población normalmente distribuida cuando el tamaño de la muestra es pequeño, en este caso es menor a 30 datos.

5.1 COMPROBACION DE LA HIPOTESIS

Tabla 30. Tiempos Sin y Con protección

N°		Vulnerabilidades	Sin Protección	Con Protección
1	EXPLOTACIÓN	Inyección Sql (SQLi)	3	2
2		Secuencias de Comandos de Sitios Cruzados (XSS)	2	1
3		Falsificación de Peticiones en Sitios Cruzados (CSRF)	3	2
4	PREVALENCIA	Inyección Sql (SQLi)	2	2
5		Secuencias de Comandos de Sitios Cruzados (XSS)	4	4
6		Falsificación de Peticiones en Sitios Cruzados (CSRF)	2	2
7	DETECCIÓN	Inyección Sql (SQLi)	2	1
8		Secuencias de Comandos de Sitios Cruzados (XSS)	3	2
9		Falsificación de Peticiones en Sitios Cruzados (CSRF)	2	1
10	IMPACTO	Inyección Sql (SQLi)	3	2
11		Secuencias de Comandos de Sitios Cruzados (XSS)	2	1
12		Falsificación de Peticiones en Sitios Cruzados (CSRF)	2	1

Adaptado por: Gavidia Marco & Jessica Valle

5.1.1 PRUEBA DE HIPÓTESIS

$$H_o = \mu_{sp \leq \mu_{cp}}$$

La hipótesis Nula es igual al promedio de las vulnerabilidades sin protección menor o igual al promedio de las vulnerabilidades con protección.

$$H_1 = \mu_{sp > \mu_{cp}}$$

La hipótesis alternativa es igual al promedio de las vulnerabilidades sin protección y es mayor al promedio de las vulnerabilidades con protección la cual va a ser comprobada.

NIVEL DE SIGNIFICANCIA

Rango de aceptación de que pueda haber 0.05 o 5% error. $\propto = \mathbf{0,05}$

REGION CRÍTICA

gl = región critica

N = Número de parámetros de vulnerabilidades que se tabula en cada pregunta para obtener valores.

$$\boldsymbol{gl = N - 1}$$

$$\boldsymbol{gl = 12 - 1}$$

$$\boldsymbol{gl = 11}$$

CALCULOS

Los parámetros de T-Tabulación serán entre (0,05: 11); el resultado obtenido es 1,795.

TABLA

Tabla 31. Tabulación T-Student

α / n-1	0,25	0,2	0,15	0,1	**0,05**	0,025	0,01	0,005	0,0005
1	1,0000	1,3764	1,9626	3,0777	6,3138	12,7062	31,8205	63,6567	636,6192
2	0,8165	1,0607	1,3862	1,8856	2,9200	4,3027	6,9646	9,9248	31,5991
3	0,7649	0,9785	1,2498	1,6377	2,3534	3,1824	4,5407	5,8409	12,9240
4	0,7407	0,9410	1,1896	1,5332	2,1318	2,7764	3,7469	4,6041	8,6103
5	0,7267	0,9195	1,1558	1,4759	2,0150	2,5706	3,3649	4,0321	6,8688
6	0,7176	0,9057	1,1342	1,4398	1,9432	2,4469	3,1427	3,7074	5,9588
7	0,7111	0,8960	1,1192	1,4149	1,8946	2,3646	2,9980	3,4995	5,4079
8	0,7064	0,8889	1,1081	1,3968	1,8595	2,3060	2,8965	3,3554	5,0413
9	0,7027	0,8834	1,0997	1,3830	1,8331	2,2622	2,8214	3,2498	4,7809
10	0,6998	0,8791	1,0931	1,3722	**1,8125**	2,2281	2,7638	3,1693	4,5869
11	0,6974	0,8755	1,0877	1,3634	1,7959	2,2010	2,7181	3,1058	4,4370

Adaptado por: Gavidia Marco & Jessica Valle

5.1.2 ANALISIS ESTADISTICO DE T-STUDENT

Tabla 32. Prueba T con los tiempos parciales "sin" y "con" protección.

Prueba t para medias de dos muestras emparejadas		
	Variable 1	Variable 2
Media	μ_{sp} 2,5	μ_{cp} 1,75
Varianza	0,454545455	0,75
Observaciones	12	12
Coeficiente de correlación de Pearson	0,856348839	
Diferencia hipotética de las medias	0	
Grados de libertad	11	
Estadístico t	5,744562647	
P(T<=t) una cola	**6,47008E-05**	
Valor crítico de t (una cola)	1,795884814	
P(T<=t) dos colas	**0,000129402**	
Valor crítico de t (dos colas)	2,200985159	

Adaptado por: Gavidia Marco & Jessica Valle

5.1.3 DECISIÓN DEL ANALISIS DE T-STUDENT

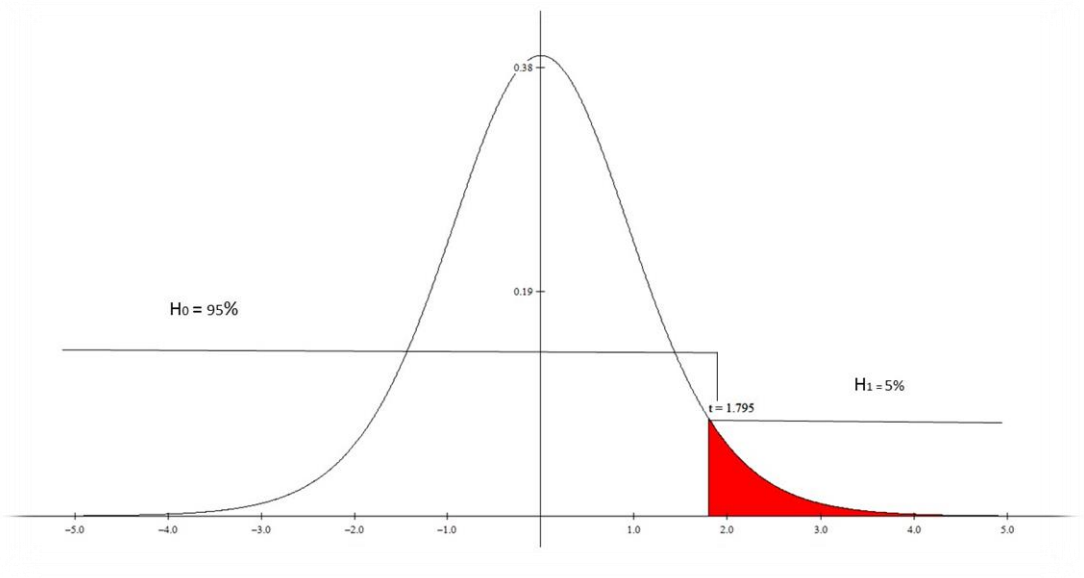


Figura 61. Gráfico de H0, H1 y t de la comprobación

μ_{sp} =2,5 μ_{cp} =1,75

Se rechaza la Ho por cuanto el valor de P (t<=t) 0.000129402 es menor que 0.05 es decir el promedio de vulnerabilidades con protección tiene una mejor seguridad en comparación con un sistema sin protección por cuanto se acepta la H1.

CAPÍTULO VI

RESULTADOS y DISCUSIÓN

6.1 RESULTADOS DE VULNERABILIDADES DEL SISTEMA CEMENTERIO MUNICIPAL DE RIOBAMBA.

En el siguiente proyecto se va a determinar cada una de las vulnerabilidades implementadas en el sistema, la herramienta que se utilizarán de código abierto es la siguiente:

DAMN VULNERABLE WEB APP (DVWA) 1.0.8

Es una herramienta hecha en PHP y MySQL para la explotación de vulnerabilidades de los sistemas, está hecha para montar un entorno de pruebas de penetración legal, para Testear cada vulnerabilidad. DVWA está divido en tres niveles: Low, medium y hight, cada uno respectivamente va aumentar su nivel de dificultad. Las técnicas que evalúa esta aplicación son las siguientes:

SQL Injection

XSS (Cross Site Scripting)

CSRF (Cross Site Request Forgery)

LFI (Local File Inclusion)

RFI (Remote File Inclusion)

Command Execution

Upload Script

Login Brute Force

FUCIONAMIENTO

Esta vulnerabilidad nos permite ejecutar comandos de consola desde la web, para poder ver, modificar, eliminar archivos y directorios del servidor, las posibilidades son infinitas, su única limitación es el usuario que usa la consola para ejecutar los comandos, así dependería de los permisos de ese usuario para realizar ciertas acciones. (RedInfoCo, 2014)

Utilizar la aplicación DVWA los parámetros a evaluarse será a través del escaneo activo y se evaluaran la alerta de alta prioridad (color rojo), alerta de prioridad mediana (color tomate), las alertas de baja prioridad (color amarillo) y la alerta informativa (color azul).

Figura 62. Alertas de DVWA

Fuente: Parte inferior de la interfaz de OWASP ZAP.

Adaptado por: Gavidia Marco & Jessica Valle

Esta herramienta se encuentran disponibles en el internet y se utilizada para realizar pruebas al sistema de: Inyección SQL, Secuencia de comandos cruzados (XSS) y la falsificación de sitios cruzados (CSRF). A continuación se describirá cada una de ellas.

6.2 COMPARATIVA DE SEGURIDAD ENTRE UN SISTEMA DE INFORMACION CON PROTECCION Y SIN PROTECCION.

6.2.1 PRUEBAS DEL SISTEMA INFORMATICO SIN PROTECCION

6.2.1.1 DVWA-SQL INJECTION Y DVWA-XSS

OWASP Zed Attack Proxy es una herramienta libre que permite realizar pruebas de petición de Sql Injection y XSS generado por el software como se detalla a continuación.

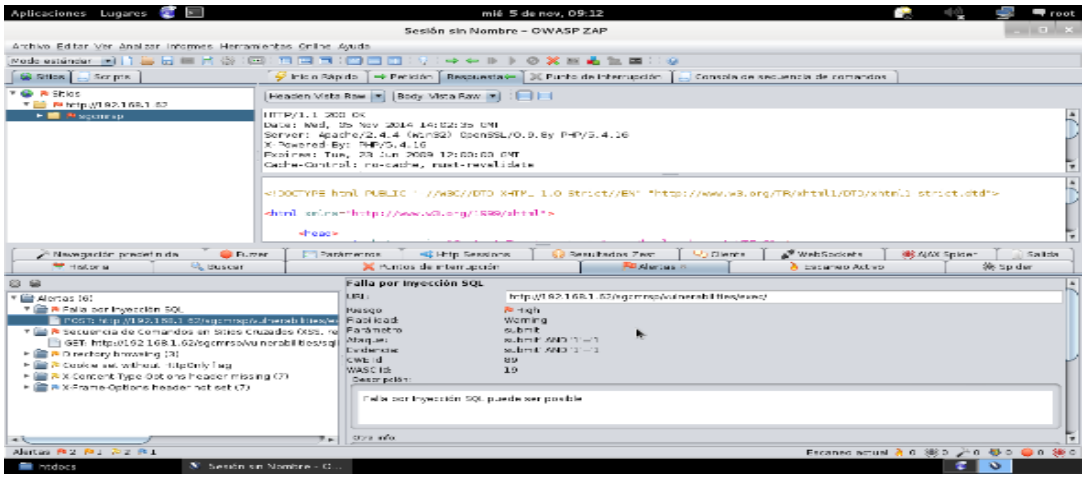


Figura 63. Escaneo de Inyección Sql y XSS en el Sistema del Cementerio

Fuente: Parte de la interfaz de OWASP ZAP.

Adaptado por: Gavidia Marco & Jessica Valle

Al terminar el escaneo de las vulnerabilidades se muestra las alertas de mayor prioridad con una bandera roja, al ser las más peligrosas para el sistema. De esa manera se puede verificar el código al cual fue afectado para aplicar el mecanismo de protección adecuado para esa vulnerabilidad.

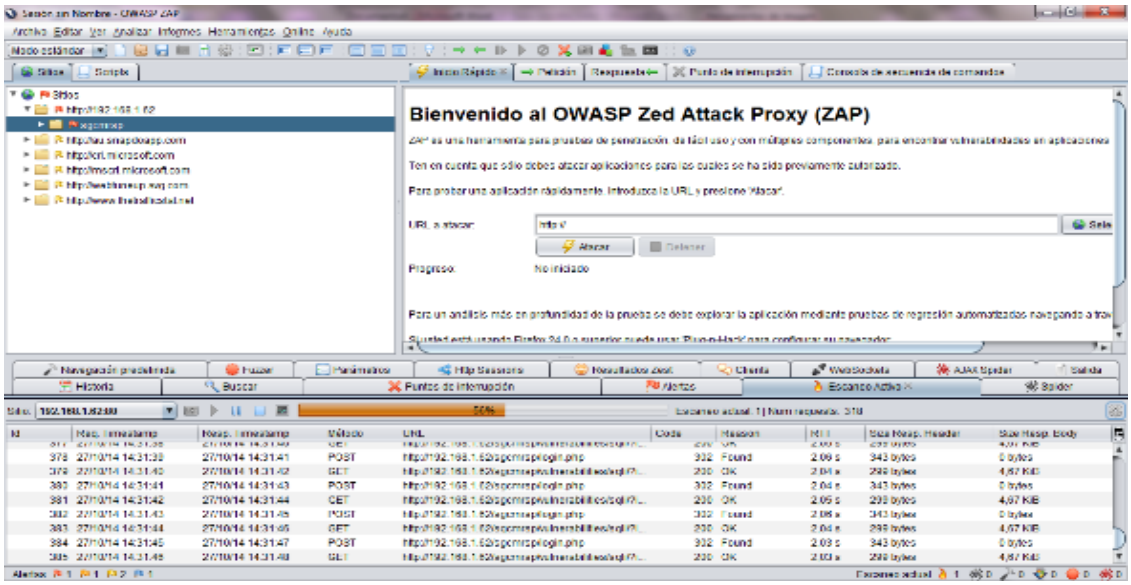


Figura 64. Resultado final del escaneo de Inyección Sql y XSS

Fuente: Interfaz de OWASP ZAP.

Adaptado por: Gavidia Marco & Jessica Valle

Durante el escaneo se identificó 6 alertas que tenía la aplicación, los cuales se detallan a continuación:

Tabla 33. Alertas del sistema

Alertas	Concepto
✓ **Inyeccion SQL**	Es una alerta de alta prioridad y su riesgo es muy grave.
✓ **XSS**	Es una alerta de alta prioridad y su riesgo es muy grave.
✓ **Directory Browsing**	Esta alerta es de prioridad mediana y su riego no es tan alto pero si de consideración.
✓ **Cookie set without HttpOnly flag** ✓ **X-Content-Type-Options header missing**	Mientas que estas alertas son de baja prioridad, su riesgo no tiene consecuencias.
✓ **X-Frame –Options header not set**	Además está alerta es informativa y no tiene ningún riesgo en el sistema.

Adaptado por: Gavidia Marco & Jessica Valle

6.2.1.2 DVWA-CSRF

Damn Vulnerable Web App es una herramienta que permite explotar las vulnerabilidades web en php y mysql y posee herramientas de detección y configuración personalizadas para el análisis.

Figura 65. Resultado de infiltración de CSRF

Fuente: Parte de la interfaz de DVWA.

Adaptado por: Gavidia Marco & Jessica Valle

6.2.2 PRUEBAS DEL SISTEMA INFORMATICO CON PROTECCION

6.2.2.1 DVWA-SQL INJECTION, XSS, CSRF

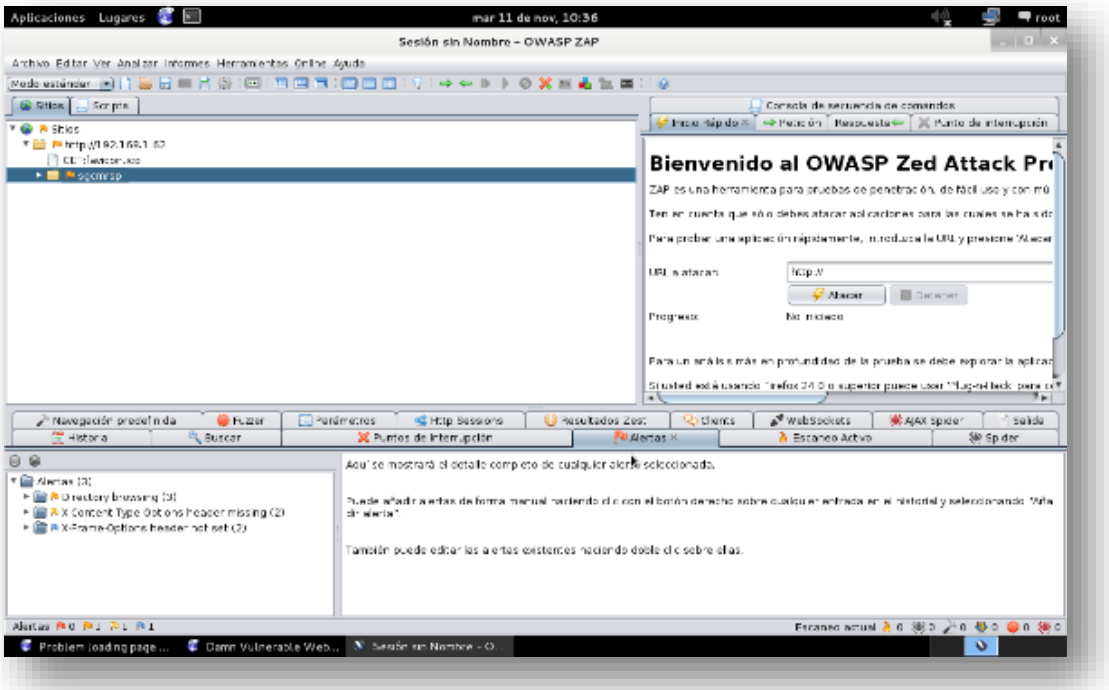


Figura 66. Resultado Final del sistema con Protección

Fuente: Parte de la interfaz de DVWA.

Adaptado por: Gavidia Marco & Jessica Valle

Con la herramienta OWASP Zed Attack Proxy de escaneo de las vulnerabilidades se observó que durante el análisis del sistema del Cementerio Municipal de Riobamba ya no se muestran las vulnerabilidades de Inyección Sql, Xss y CSRF, por tal motivo se considera que esta apropiadamente protegido.

- ✓ **Resultado**

En el escenario sin protección se obtiene el análisis de las vulnerabilidades que dieron como resultado obtener alertas de Inyección SQL, XSS y CSRF como se observa en el panel de alertas de la herramienta OWASP ZAP. Con la función spider para escanear más recursos que tengan el sistema en la url que se coloca en el navegador.

Luego de escanear todos los recursos la herramienta mostrara todo tipo de ataques. Esto implica desde una búsqueda de configuración en un simple parámetro de alguno de los archivos que compone la web, hasta ataques de SQL injection, XSS, y terminado con la búsqueda automática de otras vulnerabilidades.

- ✓ **Discusión**

Antes del análisis no se conocía que tipos de vulnerabilidades existían, los parámetros de evaluación y cuáles eran las más riesgosas para un sistema informático a nivel de software, pero a través de herramientas automatizadas como OWASP ZAP se ha podido realizar un recorrido de las url realizar un escaneo activo para analizar el contenido y encontrar alertas de vulnerabilidades existentes. Esto permitirá tomar acciones para poder reducir los factores de riesgos a través de mecanismo de protección.

- ✓ **Resultado**

Los resultados del análisis con protección ha permitido determinar los factores de riesgo como la explotación, prevalencia, detección e impacto que inciden en la seguridad del sistema informático gracias a los componentes de los cuales está hecho la herramienta OWASP ZAP que se explica a continuación:

Spider detectar automáticamente nuevas direcciones URL y los agrega a la lista de direcciones, el proceso continúa de forma recursiva, siempre que se encuentren nuevos recursos.

En la Imagen se puede observar que ya no existen alertas de Inyección SQL, Secuencia de Comandos en Sitios Cruzados y Falsificación de Peticiones en sitios Cruzados en el sistema que se ha conectado en red para crear la arquitectura cliente servidor. Con la implementación de mecanismos de protección, se fortaleció el sistema del Cementerio Municipal de Riobamba en su seguridad ante las tres vulnerabilidades analizadas.

- ✓ **Discusión**

Después de la implementación de mecanismos de protección el sistema ya no es vulnerable ante inyección sql, CSRF y XSS el cual afectaba al activo de software, específicamente en datos y de esa manera asegurar al sistema de la integridad, confidencialidad y disponibilidad. Esto evita que puedan acceder con facilidad a los datos al momento de usar funciones y código que tienen las tecnologías de desarrollo web que son PHP y mysql.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

- De acuerdo con los resultados de la investigación se puede afirmar que el análisis de vulnerabilidades ha permitido identificar las 3 debilidades más comunes y que más afectan a los sistemas informáticos a nivel de software que son inyección sql, secuencia de comandos de sitios cruzados y falsificación de peticiones de sitios cruzados a través de técnicas y herramientas que ha permitido poder evaluar los factores de riesgo de explotación, detección prevalencia e impacto que estas tienen cuando se produce un ataque a dichos sistemas.
- Se puede confirmar que para la implementación de mecanismos de protección se debe considerar los requerimientos institucionales, el entorno de funcionamiento y lenguajes de programación, esto determinó utilizar las tecnologías de desarrollo de php y mysql por ser open source y tener funciones que permiten evitar las vulnerabilidades más comunes a nivel de software.
- Se logró desarrollar el sistema informático obteniendo resultados positivos, en el Cementerio Municipal de Riobamba, con lo cual se cumple con el objetivo planteado mejorando la seguridad del sistema informático de un 2,5 a 1,75 que significa que mientas el valor es más bajo es más seguro según la metodología de factor de riesgo de OWASP.
- Para tener una seguridad informática completa se debe ampliar los conocimientos en el área de seguridad de sistemas informáticos, normas ISO, herramientas de desarrollo web, herramientas de búsqueda y explotación de vulnerabilidades.

7.2 RECOMENDACIONES

- Para desarrollar un buen análisis de vulnerabilidades de debe tomar en consideración información actual para poder aplicar con mayor eficacia las pruebas usando recursos hardware, software y humanos que sean accesibles para poder obtener resultados positivos y dar mejor solución para mejorar la seguridad de los sistemas informáticos.
- Es muy importante que las empresas tengan cultura de prevención para obtener beneficios a futuro y evitar contratiempos a la hora de sufrir ataques a sus sistemas informáticos para ello se debe trazar un plan de acción y políticas de seguridad de la información.
- Realizar una investigación con un mayor alcance tanto en el campo empresarial, investigativo, personal y económico con el fin de mejorar los activos como el software en los sistemas informáticos tanto en el sector público como el privado.
- Al momento de desarrollar un sistema se debe aplicar los debidos mecanismos de protección ante las vulnerabilidades analizadas para que el sistema este seguro y que la integridad, confidencialidad y disponibilidad de la información sea permanente.
- Se debe recopilar información y fuentes bibliográficas que sean actualizadas ya que en el tema de seguridad informática las recomendaciones o mecanismos ante vulnerabilidades pueden quedar obsoletas con el pasar del tiempo así como también investigaciones previas.
- Se debería contemplar la idea de la implementación de un departamento de seguridad informática en donde se capacite a personal del área de sistemas del GAD Riobamba y el Cementerio Municipal de Riobamba para disminuir los factores de riesgo de los sistemas informáticos ya que estos son recursos muy importantes para la sostenibilidad de dichas instituciones y empresas.

CAPÍTULO VIII

PROPUESTA

8.1 TITULO DE LA PROPUESTA.

Análisis de seguridad de aplicaciones web para evitar el acceso y robo de información.

8.2 INTRODUCCIÓN.

En la actualidad los hackers concentran sus esfuerzos en las aplicaciones basadas en la web como carritos de compra, formularios, páginas de inicio de sesión, el contenido dinámico, etc.

Del total de los sitios web el 70% tienen vulnerabilidades que pueden conducir al robo de datos corporativos sensibles, tales como, información de tarjeta de crédito y listas de clientes que están accesible las 24 horas y los 7 días de la semana, además desde cualquier parte del mundo, las aplicaciones web inseguras facilitan el acceso a bases de datos corporativas backend que permiten a los hackers llevar a cabo actividades ilegal que afecten a las organizaciones.

La investigación es propuesta como una medida de que los ataques a las aplicaciones Web, no tengan un rápido acceso, el cual afecte al servidor de seguridad, el sistema operativo, la seguridad a nivel de red y los datos corporativos.

La mayor parte de las Aplicaciones web no son probadas por ello tienen vulnerabilidades sin descubrir y por lo tanto son presa fácil para los piratas informáticos.

Esta investigación estará dividida de tal forma que se traten temas y soluciones para que los hackers o crackers no pongan en peligro las páginas o aplicaciones web.

Este rastreo permite encontrar posibles vulnerabilidades como inyección SQL, cross-site scripting entre otras vulnerabilidades que exponen todo proceso en los sistemas web.

Es muy útil también realizar informes concisos para identificar los tipos de vulnerabilidades que afectan a las aplicaciones web, lo que le permite proteger su negocio de inminentes ataques de hackers!

8.3 OBJETIVOS.

8.3.1 OBJETIVO PRINCIPAL

Análisis de seguridad de aplicaciones web para mejorar la confiabilidad información

8.3.2 OBJETIVOS ESPECIFICOS

Analizar las seguridades en aplicaciones web

Implementar software para monitorear vulnerabilidades, ataques.

Crear un manual para ciberseguridad y medidas ante acceso y robo de información no autorizado.

8.4 FUNDAMENTACION CIENTIFICO TECNICA.

8.4.1 CIBERSEGURIDAD

Ciberseguridad Ciudadana: El cual proporciona una protección integral del ciudadano en colaboración con empresas públicas o privadas a través de la web. Los elementos a proteger pueden ser la cedula de ciudadanía, acceso rápido de fronteras, firma electrónica, centros de alerta temprana (CERTs) e información al ciudadano (www.indracompany.com, 2014)

Ciberseguridad a Organizaciones: Estas pueden ser públicas o privadas y los elementos a proteger pueden ser a través de soluciones de ciberseguridad, consultoría y auditoría, formación en desarrollos e implantaciones de planes directores de seguridad, operación de Oficinas de Seguridad y Seguridad Gestionada (SOC).

Ciberseguridad en Infraestructuras Críticas: Para desarrollos e implantaciones de planes de ciberseguridad para Centrales Nucleares, refinerías, oleoductos, sistemas de control, presas y sistemas de distribución de agua, redes eléctricas todo esto mediante protección de los sistemas y redes que operan en las infraestructuras críticas antes mencionadas.

8.5 DESCRIPCIÓN DE LA PROPUESTA.

Se va a realizar un análisis de las seguridades en las aplicaciones web para ello habrá que segmentar cuales de ellas están más susceptibles a estos ataques ya que no todas son objeto en las cuales se centren los hackers.

También se debe realizar un levantamiento de información en donde se muestren estadísticas, historiales, etc., de cómo se ha llevado a cabo todos estos ataques, así como también la situación actual de los mismos para saber la adecuada forma de contrarrestar esa situación.

En lo posterior se puede implementar un software y en algunos casos también en hardware si se diera la factibilidad de tomar en cuenta el costo beneficio que ayude a tener un mayor control de los ataques y además de las vulnerabilidades de las aplicaciones web.

Finalmente realizar un manual de ciberseguridad que si bien la ISO27032 ya menciona información referente a este tema, pero con el inconveniente que tiene un elevado costo para adquirirlo lo cual no será la única opción sino que la experiencia e investigación quede plasmado en un documento físico después de realizar todo el trabajo.

8.6 MONITOREO Y EVALUACION DE LA PROPUESTA

El área de sistema de cualquier entidad institucional sea pública o privada no tiene los suficientes mecanismos, medidas o procedimientos que le ayuden a monitorear y evaluar los riegos que tienen sus sistemas informáticos en el área de software.

Para ello se ha de implementar software como por ejemplo Acunetix Web Vulnerabilities Scanner que comprueba automáticamente las aplicaciones web para la inyección de SQL, XSS y otras vulnerabilidades web.

Con la aplicación indicada anteriormente se puede brindar seguimiento y monitoreo a la propuesta y también a los sistemas para poder realizar un informe y manual correspondiente que respalde la investigación.

El monitoreo debe facilitar la evaluación del progreso hacia los objetivos y metas.

Para ello se realizara recolección continua de datos e información que permita medir si las actividades están implementadas según las expectativas, y si necesario abordar obstáculos y desafíos.

CAPÍTULO IX

BIBLIOGRAFÍA

Aguilera, P. (2010). *Seguridad informática.* Editex.

Asesoriait.com. (13 de Abril de 2013). *AiTSEO, Web App's, Desktop & Mobile Web Sites.* Recuperado el 6 de Septiembre de 2013, de Cross-Site Scripting – Conceptos de Seguridad Informática.: http://asesoriait.com/cross-site-scripting/

Blog, M. S. (19 de Febrero de 2013). *Mindedsecurity.com.* Recuperado el 23 de Octubre de 2013, de Minded Security Blog: http://blog.mindedsecurity.com/2013/02/real-life-vulnerabilities-statistics.html

Cyberintruder.com. (13 de Agosto de 2013). *CyberIntruder Learn Share Hack.* Recuperado el 13 de Septiembre de 2013, de SECURITY MISCONFIGURATION: http://www.cyberintruder.com/security-misconfiguration/#more-41

DEMS. (2014). *DEMS - Servicio de Monitoreo Externo DOSarrest.* Obtenido de http://www.dosarrest.com/dems-dosarrest-external-monitoring-services

Desarrollodefw.blogspot.com. (Diciembre de 2012). *Metodologías de Desarrollo de Software*. Recuperado el 21 de Septiembre de 2013, de http://desarrollodefw.blogspot.com/2012/10/introduccion_26.html

Desarrollodefw.blogspot.com. (Diciembre de 2012). *Metodologías de Desarrollo de Software*. Recuperado el 21 de Septiembre de 2013, de http://desarrollodefw.blogspot.com/2012/10/12-caracteristicas-principales.html

ETECSA. (2012 de Febrero). Recuperado el 21 de Septiembre de 2013, de http://www.ecured.cu/index.php/Metodolog%C3%ADas_de_desarrollo_de_software

GoDaddy.com, L. (31 de Julio de 2014). *Normas de gestión infosec ISO27k*. Obtenido de ISO27k&ISMSresources: http://www.iso27001security.com

ISO. (30 de Julio de 2014). *El portal de ISO 27001 en Español*. Obtenido de ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información: http://www.iso27000.es/iso27000.html

Marc, R. (2013). *MySQL, Expert PHP and Application Design and Development.* Estados Unidos.

MARKETO. (Abril de 2013). *Trustwave.* Recuperado el 23 de Octubre de 2013, de Trustwave.com: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

OWASP. (2013). *Owasp Day Costa Rica.* Recuperado el 20 de Octubre de 2013, de OWASP: https://www.owasp.org/images/7/7e/1.OWASP_Day_Costa_Rica_Michael.pdf

OWASP. (2013). *Owasp Top 10-2013 rcl* (Create Commons ed.). (O. Foundation, Ed.) Estados Unidos.

OWASP. (Octubre de 2013). *OWASP Top Ten 2013 Proyect*. Recuperado el 10 de ABRIL de 2013, de OWASP.ORG: https://www.owasp.org/index.php/OWASP_Top_Ten_Project

OWASP, Z. (18 de 11 de 2014). *OWASP.* Obtenido de https://www.owasp.org/index.php?title=OWASP_Zed_Attack_Proxy_Project&setlang=es

Publica, M. d. (2012). Guía de COmunicación Digital. *Seguridad*, 14.

RedInfoCo. (27 de Octubre de 2014). *Aprender, compartir y visualización*. Obtenido de http://www.redinfocol.org: http://www.redinfocol.org/dvwa-conociendo-y-explotando-diferentes-vulnerabilidades-level-low/

Resources.arcgis.com. (JUnio de 2010). *ArcGIS Resource Center.* Recuperado el 18 de Agosto de 2013, de http://resources.arcgis.com/es/content/enterprisegis/10.0/web_security

RRM, O. (12 de Febrero de 2008). *https://www.owasp.org.* Obtenido de https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Security, A. (2013). *Aspectsecurity.com.* Recuperado el 23 de Octubre de 2013, de Application Security Experts: https://www.aspectsecurity.com/uploads/downloads/2013/06/Aspect-2013-Global-AppSec-Risk-Report.pdf

Security, W. (2013). *WhiteHat Security - Your web application security company.* Recuperado el 23 de Octubre de 2013, de WhiteHat Security.com: http://owasptop10.googlecode.com/files/WPstats_winter11_11th.pdf

Softtek. (2012). *State of Art Software Security Statistical Report.* Recuperado el 23 de Octubre de 2013, de Softtek - IT Services and Business Process Solutions: https://www.softtek.com/webdocs/special_pdfs/WP-State-of-the-art-2013.pdf

Veracode. (7 de Diciembre de 2011). *Application Security Testing.* Recuperado el 23 de Octubre de 2013, de veracode.com: http://info.veracode.com/rs/veracode/images/VERACODE-SOSS-V4.PDF

www.indracompany.com. (06 de Noviembre de 2014). *Indracompany*. Obtenido de http://www.indracompany.com/sector/seguridad/oferta/ciberseguridad

www8.hp.com. (2013). *Cyber risk report 2013.* Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx%2F4AA5-0858ENW.pdf

CAPÍTULO X

ANEXOS

10.1 ANEXOS DE LAS FASES DE LA METODOLOGIA XP

10.1.1 HISTORIAS DE USUARIO DE LA PÁGINA WEB DE LA FASE DE PLANIFICACIÓN EN XP

MÓDULO N°1: INFORMACIÓN DE USUARIO

Tabla 34. Historia de Usuario de Información de Usuario [5]

HISTORIA DE USUARIO	
Número:1	Nombre de Administración de Usuario: Manejo de Usuario
Modificación (o extensión) de Administración de Usuario (Nro. y Nombre): NA	
Usuario: Super Administrador	Iteración Asignada: 1
Prioridad en Negocio: Media	Puntos Estimados: 2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: ✓ Se realiza la creación de usuarios y dar les diferentes permisos	
Observaciones: El Super Usuario es el encargado concederles diferentes permisos a los usuarios.	

Fuente:http://kovachi.sel.inf.uc3m.es/800spanish/Metodos_y_Modelos/xp_extreme_programming/escribir_historia.

Adaptado por: Gavidia Marco & Jessica Valle

[5] & [56] **Elaborado por:** Marco Gavidia y Jessica Valle **Fuente:** Byers, J. (Agosto de 2011). *Programacion-Extrema - home*. Recuperado el 2 de Abril de 2014, de http://programacion-extrema.wikispaces.com/7.+Artefactos

MÓDULO N°2: INFORMACIÓN DE MENÚS

Tabla 35. Historia de Usuario de Información de Menús

HISTORIA DE USUARIO	
Número:2	Nombre de Administración de Usuario: Información de Menús
Modificación (o extensión) de Administración de Usuario (Nro. y Nombre): NA	
Usuario: Super Administrador	Iteración Asignada: 1
Prioridad en Negocio: Media	Puntos Estimados: 2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: ✓ Se realiza la creación de usuarios y dar les diferentes permisos	
Observaciones: El Super Usuario es el encargado concederles diferentes permisos a los usuarios.	

Fuente:http://kovachi.sel.inf.uc3m.es/800spanish/Metodos_y_Modelos/xp_extreme_programming/escribir_historia.

Adaptado por: Gavidia Marco & Jessica Valle

MÓDULO N°3: INFORMACIÓN DE CONTENIDOS

Tabla 36. Historia de Usuario de Información de Contenidos

HISTORIA DE USUARIO	
Número:3	Nombre de Administración de Contenidos: Manejo de Contenidos
Modificación (o extensión) de Administración de Contenidos (Nro. y Nombre): NA	
Usuario: Super Administrador	Iteración Asignada: 3
Prioridad en Negocio: Media	Puntos Estimados: 2
Riesgo en Desarrollo: Baja	Puntos Reales: 1
Descripción: ✓ Se escribirá alguna reseña histórica referente al título del menú, además se podrá subir imágenes o galería de fotos.	
Observaciones: El Super Usuario podrá cambiar el texto, publicar o despublicar.	

Fuente:http://kovachi.sel.inf.uc3m.es/800spanish/Metodos_y_Modelos/xp_extreme_programming/escribir_historia.

Adaptado por: Gavidia Marco & Jessica Valle

MÓDULO N°4: INFORMACIÓN DE EXTENSIONES

Tabla 37. Historia de Usuario de Información de Extensiones

HISTORIA DE USUARIO	
Número:4	Nombre de Administración de Extensiones: Manejo de Extensiones
Modificación (o extensión) de Administración de Extensiones (Nro. y Nombre): NA	
Usuario: Super Administrador	Iteración Asignada: 4
Prioridad en Negocio: Media	Puntos Estimados: 2
Riesgo en Desarrollo: Alta	Puntos Reales: 3
Descripción: ✓ Se subirán archivos y se instalarán	
Observaciones: ✓ El Super Usuario podrá cargar los mejores plugins, módulos y plantillas que necesite la página.	

Fuente:http://kovachi.sel.inf.uc3m.es/800spanish/Metodos_y_Modelos/xp_extreme_programming/escribir_historia.

Adaptado por: Gavidia Marco & Jessica Valle

10.1.2 HISTORIAS DE USUARIO DEL SISTEMA CMR DE LA FASE DE PLANIFICACIÓN EN XP

Tabla 38. Historia de Usuario de Autenticación de usuario

HISTORIA DE USUARIO	
Número:1	**Nombre Historia de Usuario:** Autenticación de usuario con nombre y contraseña
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:1
Prioridad en Negocio: Alta	Puntos Estimados:3
Riesgo en Desarrollo: Alta	Puntos Reales: 3
Descripción: Una vez autenticado el sistema debe distinguir un usuario normal que tiene accesos limitados y funciones limitadas en el sistema con un usuario administrador que tiene acceso total a funciones y sistemas.	
Observaciones: Debe tener una interfaz de login con su respectivo password	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 39. Historias de Usuario de registro de cementerio

HISTORIA DE USUARIO	
Número:2	Nombre Historia de Usuario: Registro de Cementerio
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:2
Prioridad en Negocio: Alta	Puntos Estimados:3
Riesgo en Desarrollo: Alta	Puntos Reales: 3
Descripción: Una vez autenticado el sistema el Usuario debe acceder a un determinado menú que permita en ingreso de un cementerio con sus respectivos campos.	
Observaciones: Debe tener las operaciones de insertar, búsqueda, modificación y eliminación para el Administrador y para el usuario normal solo inserción y búsqueda.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 40. Historia de Usuario de Registro de Sector

HISTORIA DE USUARIO	
Número:3	Nombre Historia de Usuario: Registro de Sector
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:3
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de los diferentes sectores que tiene un cementerio	
Observaciones: Debe tener un selector de opciones de cementerio y otro campo para ingresar el sector	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 41. Historia de Usuario de Registro de Sección

HISTORIA DE USUARIO	
Número:4	Nombre Historia de Usuario: Registro de Sección
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:4
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de las diferentes secciones que tiene un cementerio	
Observaciones: Debe tener los siguientes campos como un selector de cementerio y la sección que desea.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 42. Historia de Usuario de Registro de Trabajador

HISTORIA DE USUARIO	
Número:5	Nombre Historia de Usuario: Registro de trabajador
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:5
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de las diferentes trabajadores que tiene un cementerio	
Observaciones: Debe tener los siguientes campos como un selector de cementerio y la sección que desea.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 43. Historia de Usuario de Registro de Categoría (de tumba)

HISTORIA DE USUARIO	
Número:6	Nombre Historia de Usuario: Registro de categoría
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:6
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de las diferentes categorías que tiene un cementerio	
Observaciones: Debe tener los siguientes campos como un selector de cementerio y la sección que desea.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Marco Gavidia & Jessica Valle

Tabla 44. Historia de usuario de Registro de Tipo (de cargo)

HISTORIA DE USUARIO	
Número:7	Nombre Historia de Usuario: Registro de Tipo(de cargo)
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:7
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de las diferentes categorías que tiene un cementerio	
Observaciones: Debe tener los siguientes campos como un selector de cementerio y la sección que desea.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 45. Historias de Usuario de Registro de Sepulturas

HISTORIA DE USUARIO	
Número:8	Nombre Historia de Usuario: Registro de Sepulturas
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:8
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de las diferentes sepulturas que se encuentran en las diferentes sectores del cementerio	
Observaciones: Las sepulturas deben tener una lista de opciones donde permita escoger la sección e ingresar el número sepulturas que tiene la sección seleccionada.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 46 . Historia de Usuario de Registro de Nichos

HISTORIA DE USUARIO	
Número:9	Nombre Historia de Usuario: Registro de Nichos
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:9
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de las nichos que se encuentran en las diferentes secciones del cementerio	
Observaciones: Los nichos deben tener un selector de secciones y un campo para ingresar el número de nichos que existen en dicha sección.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 47. Historias de Usuario de Mausoleos

HISTORIA DE USUARIO	
Número:10	**Nombre Historia de Usuario:** Registro de Mausoleos
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:10
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro las mausoleos que se encuentran en las diferentes áreas del cementerio	
Observaciones: Las sepulturas en el suelo deberán tener campos que ayudan a identificar si es de propiedad o pertenece al municipio.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Marco Gavidia & Jessica Valle

Tabla 48. Historia de Usuario de Registro de Familiares

HISTORIA DE USUARIO	
Número:12	**Nombre Historia de Usuario:** Registro de Familiares
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:12
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de familiares con los datos requeridos como nombre apellido, dirección y teléfono.	
Observaciones: La búsqueda de los registros de los familiares debe hacerse por apellido.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 49. Historias de Usuario de Registro de Personas fallecidas

HISTORIA DE USUARIO	
Número:11	**Nombre Historia de Usuario:** Registro de Personas fallecidas
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:11
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: Se realiza el registro de personas fallecida en la que se debe ingresar la cedula, Código de tumba, nombres y apellidos y la fecha de fallecimiento.	
Observaciones: La búsqueda de los registros de las personas fallecidas debe hacerse por apellido o nombre.	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 50. Historias de Usuario de Registro de Tumbas

HISTORIA DE USUARIO	
Número:12	Nombre Historia de Usuario: Tumbas
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:12
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: ✓ Ingresar ✓ Actualizar ✓ Buscar ✓ Eliminar ✓ Listar	
Observaciones: Las tumbas son únicas por cada persona fallecida debido que en muchas sepulturas hay más de una persona fallecida	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 51. Historia de usuario de Asignar

HISTORIA DE USUARIO	
Número:13	Nombre Historia de Usuario: Asignar
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:13
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: • Asignar: ✓ Nicho ✓ Sepultura ✓ Mausoleo. .	
Observaciones: Estos reportes representan la funcionalidad o valor agregado que ofrece el Sistema CMR	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Marco Gavidia & Jessica Valle

Tabla 52. Historias de Usuario para reportes

HISTORIA DE USUARIO	
Número:14	Nombre Historia de Usuario: Reportes
Modificación (o extensión) de Historia de Usuario (Nro. y Nombre):NA	
Usuario: Oficinista o Encargado del Sistema	Iteración Asignada:14
Prioridad en Negocio: Media	Puntos Estimados:2
Riesgo en Desarrollo: Media	Puntos Reales: 2
Descripción: • Reportes: o Total Nichos por sección o Total Sepulturas por sección o Total Mausoleos por sección .	
Observaciones: Estos reportes representan la funcionalidad o valor agregado que ofrece el Sistema CMR	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Marco Gavidia & Jessica Valle

10.1.3 TARJETAS CRC DE LAS HISTORIAS DE USUARIO DE LA PÁGINA WEB

Tarjeta CRC de Usuario

Escenarios:

- ✓ Crear nuevas cuentas de usuarios
- ✓ Editar perfil de usuario

Concederá diferentes permisos a un grupo o determinado usuario.

Tabla 53. Tarjeta CRC Usuario

Usuarios	
Responsabilidades	Colaboradores
Activar a los usuarios	
Concederle permisos	
Dar grupos	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://programacion-extrema.wikispaces.com/7.+Artefactos.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Menús

Escenarios:

- ✓ Crear nuevos menús
- ✓ Editar ,eliminar , despublicar y publicar los menús
- ✓ Modificar el Menú
- ✓ Pondrá título al menú y enlazará con un artículo

Tabla 54. Tarjeta CRC Menús

Menús	
Responsabilidades	Colaboradores
Seleccionar un Acceso	
Publicar	
Dar un orden para el menú	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Contenidos

Escenarios:

- ✓ Crear artículos en la categoría correspondiente en la que podrá contener archivos con texto y fotos.
- ✓ Editar los artículos
- ✓ Publicar y Presentar la información en el portal web

Escribir y subir imágenes en el artículo seleccionado.

Tabla 55. Tarjeta CRC Contenidos

Contenidos	
Responsabilidades	Colaboradores
Seleccionar el estado	
Seleccionar el autor del contenido	
Seleccionar el acceso	
Seleccionar el articulo más destacado	

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Extensiones

Escenarios:

- ✓ Seleccionar el archivo.
- ✓ Instalar Módulos, Plugin, Plantillas y de Idioma.

- ✓ Crear, Duplicar, los Módulos, Plugin, y Plantillas.
- ✓ Publicar y Despublicar Módulos, Plugin, y Plantillas.
- ✓ Ubicar la posición en la página de Módulos, Plugin, y Plantillas

Tabla 56. Tarjetas CRC Extensiones

Extensiones	
Responsabilidades Darle una posición Seleccionar el estado Seleccionar el Módulo Seleccionar el Acceso	Colaboradores

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

10.1.4 TARJETAS CRC DE LAS HISTORIAS DE USUARIO DEL SISTEMA CMR

Tarjeta CRC de Autenticación de usuario con nombre y contraseña

Escenarios:

- ✓ Pantalla de login.
- ✓ Autenticación de usuario

Tabla 57. Tarjeta CRC de Autenticación de Usuario con Nombre y contraseña

AUTENTICACIÓN DE USUARIO CON NOMBRE Y CONTRASEÑA	
Responsabilidades	Colaboradores
Login Autenticación	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Cementerio

Escenarios:

- ✓ Gestión de Información del Cementerio

Tabla 58. Tarjeta CRC de Cementerio

CEMENTERIO	
Responsabilidades	Colaboradores
• Cementerio: ✓ ingresar, ✓ actualizar, ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Sector

Escenarios:

- ✓ Gestión de Información de las Sector

Tabla 59. Tarjeta CRC de Sector

SECTOR	
Responsabilidades	Colaboradores
• Sector: ✓ Ingresar ✓ Actualizar ✓ Eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Sección

Escenarios:

- ✓ Gestión de Información de las Secciones

Tabla 60. Tarjeta CRC de Sección

SECCIÓN	
Responsabilidades	Colaboradores
• Sección: ✓ Ingresar ✓ Actualizar ✓ Eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Trabajador

Escenarios:

- ✓ Gestión de Información de Trabajadores

Tabla 61. Tarjeta CRC de Trabajador

TRABAJADOR	
Responsabilidades	Colaboradores
• Trabajador: ✓ Ingresar ✓ Actualizar ✓ Eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Categoría

Escenarios:

- ✓ Gestión de Información de las Categorías

Tabla 62. Tarjeta CRC de Categorías

CATEGORIA	
Responsabilidades	Colaboradores
• Categoría: ✓ ingresar ✓ actualizar ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Tipo

Escenarios:

- ✓ Gestión de Información de Tipos

Tabla 63. Tarjeta CRC de Tipo (de Cargo)

TIPO	
Responsabilidades	Colaboradores
• Tipo: ✓ ingresar ✓ actualizar ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Sepulturas

Escenarios:

- ✓ Gestión de Información de Sepulturas

Tabla 64. Tarjeta CRC de sepulturas

SEPULTURAS	
Responsabilidades	Colaboradores
• Sepultura: ✓ ingresar ✓ actualizar, ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Nichos

Escenarios:

- ✓ Gestión de Información de Nichos

Tabla 65. Tarjeta CRC de nichos

NICHOS	
Responsabilidades	Colaboradores
• Nichos: ✓ Ingresar ✓ Actualizar ✓ Eliminar ✓ Listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Mausoleos

Escenarios:

- ✓ Gestión de Información de Sepultura en el suelo

Tabla 66. Tarjeta CRC de Mausoleos

MAUSOLEO	
Responsabilidades	Colaboradores
• Mausoleo: ✓ ingresar ✓ actualizar ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Familiares

Escenarios:

- ✓ Gestión de Información de Familiares

Tabla 67. Tarjeta CRC de Familiares

FAMILIARES	
Responsabilidades	Colaboradores
• Familiares: ✓ ingresar ✓ actualizar ✓ buscar ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Tumbas

Escenarios:

- ✓ Gestión de Información de Tumbas

Tabla 68. Tarjeta CRC de Tumbas

TUMBAS	
Responsabilidades	Colaboradores
• Tumbas: ✓ ingresar ✓ actualizar ✓ buscar ✓ eliminar ✓ listar	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Personas Fallecidas
Escenarios:

- ✓ Gestión de Información de personas fallecidas

Tabla 69. Tarjeta CRC de Asignar

PEROSNAS FALLECIDAS	
Responsabilidades	Colaboradores
• Asignar: ✓ Nichos ✓ Sepulturas ✓ mausoleos	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Reportes

Escenarios:

- ✓ Generación de Reportes.
  - o Total de Nichos por sección
  - o Total de Mausoleos por sección
  - o Total de Sepulturas por sección

Tabla 70. Tarjeta CRC de reportes

REPORTES	
Responsabilidades	Colaboradores
Total de Nichos por sección Total de Mausoleos por sección Total de Sepulturas por sección	Administrador Usuario

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Escenarios:

- ✓ Crear usuarios para que puedan acceder al sistema
  - o Concederá diferentes permisos a un grupo o determinado usuario.

Tabla 71. Tarjeta CRC Usuario del Sistema Web CMR

Usuarios	
Responsabilidades • Usuario: • ingresar • actualizar • eliminar	Colaboradores

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Menús

Escenarios:

- ✓ Crear nuevos menús
- ✓ Editar ,eliminar , despublicar y publicar los menús
- ✓ Modificar el Menú
- ✓ Pondrá título al menú y enlazará con un artículo

Tabla 72. Tarjeta CRC Menús del Sistema Web CMR

Menús	
Responsabilidades Seleccionar un Acceso Publicar Dar un orden para el menú	Colaboradores

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Contenidos

- ✓ Escenarios:
- ✓ Crear artículos en la categoría correspondiente en la que podrá contener archivos con texto y fotos.
- ✓ Editar los artículos
- ✓ Publicar y Presentar la información en el portal web
- ✓ Escribir y subir imágenes en el artículo seleccionado.

Tabla 73. Tarjeta CRC Contenidos del Sistema Web CMR

Contenidos	
Responsabilidades Seleccionar el estado Seleccionar el autor del contenido Seleccionar el acceso Seleccionar el articulo más destacado	Colaboradores

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

Tarjeta CRC de Extensiones

Escenarios:

- ✓ Seleccionar el archivo.
- ✓ Instalar Módulos, Plugin, Plantillas y de Idioma.
- ✓ Crear, Duplicar, los Módulos, Plugin, y Plantillas.
- ✓ Publicar y Despublicar Módulos, Plugin, y Plantillas.
- ✓ Ubicar la posición en la página de Módulos, Plugin, y Plantillas

Tabla 74. Tarjetas CRC Extensiones del Sistema Web CMR

Extensiones	
Responsabilidades Darle una posición Seleccionar el estado Seleccionar el Módulo Seleccionar el Acceso	Colaboradores

Fuente: Byers, J. (Agosto de 2011). Programación-Extrema – home de http://rupcajamenor.wordpress.com/diseno/.

Adaptado por: Gavidia Marco & Jessica Valle

10.1.5 PRUEBAS DE ACEPTACIÓN PAGINA WEB

Tabla 75. Prueba de Aceptación de Usuario

Caso de Prueba de Aceptación: Gestor de Usuarios	
Código: 1	Historia de Usuario (Nro.): 01
Nombre: Gestor correcto de usuario	
Descripción: Se realiza la creación de usuarios y dar les diferentes permisos	
Condiciones de Ejecución: El Super Usuario es el encargado concederles diferentes permisos a los usuarios.	
Entrada / Pasos de ejecución: El usuario accede como Administrador / Usuarios Escoger gestor de Usuarios Dar clic en el botón nuevo para crear un nuevo usuario. Debe llenar el nombre, nombre del acceso, poner una contraseña, confirmar la contraseña, e-mail, fecha de registro, fecha última visita, fecha último reset. Puede bloquear al usuario de algunos artículos. Luego debe guardar & cerrar. Finalmente debe activar para que pueda tener permisos.	
Resultado Esperado: Los usuarios puedan formar parte de toda información que está en la página y que algunos tengan permisos especiales. Puedan actualizar la información y formar parte de las actividades planificadas por el Cementerio Municipal de Riobamba.	
Evaluación de la Prueba: El usuario fue creado exitosamente.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 76. Pruebas de Aceptación Gestor de Menús

Caso de Prueba de Aceptación: Gestor de Menús	
Código: 2	Historia de Usuario (Nro): 02
Nombre: Gestor correcto de Menús	
Descripción: Se creará menús para hacer vínculo con los artículos, pueden ser menú superior y menú principal	
Condiciones de Ejecución: El Super Usuario es el único encargado de realizar modificaciones a los menús que existan en la página	
Entrada / Pasos de ejecución: El usuario accede como Administrador / Menús Escoger Gestor de Menús Dar clic en el botón nuevo para realizar un nuevo menú Debe poner el título, tipo de menú y la descripción Luego debe seleccionar guarda & cerrar. Después de haber creado el menú debe dar clic en nuevo para crear elementos para el menú. Llenar el título del menú, alias, tipo elemento del menú Seleccionar el artículo que debe ir enlazado y automáticamente se llenara el enlace Además escoger la localización del menú, elemento padre, el estado, la página principal, el acceso y el idioma Finalmente guardar & cerrar.	
Resultado Esperado: Funcione adecuadamente cada vez que el usuario quiera cambiar de artículo.	
Evaluación de la Prueba: El menú fue creado exitosamente.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 77. Prueba de Aceptación de Contenidos

Caso de Prueba de Aceptación: Gestor de Contenidos	
Código: 3	Historia de Usuario (Nro): 03
Nombre: Gestor correcto de Contenidos	
Descripción: Se escribirá alguna reseña histórica referente al título del menú, además se podrá subir imágenes o galería de fotos.	
Condiciones de Ejecución: El Super Usuario podrá cambiar el texto, publicar o despublicar.	
Entrada / Pasos de ejecución: El usuario accede como Administrador / Contenidos Escoger gestor de Artículos. Dar clic en el botón nuevo para realizar un nuevo artículo Escribir un título, alias y el contenido o información que debe ir en el artículo Puede subir imágenes o galería de fotos Además de cambiar de tipo de letra, puede centrar, puede dar hipervínculos, crear tablas y formulas Selecciona guardar & cerrar Finalmente puede escoger el artículo más destacado para que se vea como página principal.	
Resultado Esperado: Que se visualice toda la información correctamente Las imágenes estén claras y muy visibles.	
Evaluación de la Prueba: El artículo fue creado exitosamente.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 78. Prueba de Aceptación de Extensiones

Caso de Prueba de Aceptación: Gestor de Extensiones	
Código: 4	Historia de Usuario (Nro): 04
Nombre: Gestor correcto de Extensiones	
Descripción: Se subirán archivos y se instalarán	
Condiciones de Ejecución: El Super Usuario podrá cargar los mejores plugins, módulos y plantillas que necesite la página.	
Entrada / Pasos de ejecución: El usuario accede como Administrador / Extensiones Escoger gestor de Extensiones Dar clic en el botón seleccionar archivo Escoger el archivo para subir pueden ser módulos, plugins, plantillas o incluso un módulo del idioma que desee. Seleccionar Upload & Instalar Se visualizara un mensaje que nos dirá que la instalación se ha realizado correctamente Optar por ubicar el archivo que fue instalado en el lugar que sea mejor para la página. Finalmente ponernos publicar	
Resultado Esperado: Que los módulos instalados estén sin falencias Estén en la posición correcta Su funcionamiento este en excelente.	
Evaluación de la Prueba: El archivo fue instalado exitosamente.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.
Adaptado por: Gavidia &Valle

10.1.6 PRUEBAS DE ACEPTACIÓN SISTEMA CMR

Tabla 79. Prueba de Aceptación de Autenticación de Usuario

Caso de Prueba de Aceptación: Autenticación de Usuario	
Código: 1	Historia de Usuario (Nro): 01
Nombre: Autenticación de usuario correcto	
Descripción: Se realiza la autenticación con usuario y contraseña	
Condiciones de Ejecución: El usuario principal y el usuario normal están debidamente registrados, ningún otro usuario puede tener acceso al Sistema CMR.	
Entrada / Pasos de ejecución: El usuario Administrador / Usuarios ingresa el nombre de usuario y contraseña Luego de colocar el usuario y contraseña presiona o hace un clic en el botón ingresar.	
Resultado Esperado: El Usuario Principal puede acceder a las gestiones de todo el Sistema CMR. El usuario normal solo tiene acceso a búsqueda e ingreso de datos del Sistema CMR.	
Evaluación de la Prueba: El usuario fue creado exitosamente.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 80. Prueba de Aceptación de gestión de Cementerio

Caso de Prueba de Aceptación: Gestión de Cementerio	
Código: 2	Historia de Usuario (Nro): 02
Nombre: Inserción, eliminación, modificación y búsqueda de cementerios	
Descripción: Gestión uno de los Módulos de Registro del Cementerio en cuál es la tabla cementerio.	
Condiciones de Ejecución: El usuario debe ingresar primero en el sistema y luego ingresar un cementerio para proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción cementerio en el cual encontrara las opciones ingresar, actualizar, eliminar y listar Cementerio a través de algunos botones en los cuales se deben hacer clic para realizar con éxito las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú cementerio y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar cementerios.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar cementerios se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 81. Caso de Prueba de Aceptación: Gestión de Sector

Caso de Prueba de Aceptación: Gestión de Sector	
Código: 3	Historia de Usuario (Nro.): 03
Nombre: Ingresar, actualizar, eliminar y listar sectores del cementerio.	
Descripción: Gestión de Sector	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos un cementerio para poder ingresar un sector en dicho cementerio para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción sector en el cual encontrara las opciones ingresar, actualizar, eliminar y listar Cementerio a través de algunos botones en los cuales se deben hacer clic para realizar con éxito las operaciones mencionadas	
Resultado Esperado: El Usuario Principal debe acceder al menú sección y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar cementerios.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar sectores se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 82. Prueba de Aceptación de gestión de Sección

Caso de Prueba de Aceptación: Gestión de Sección	
Código: 4	Historia de Usuario (Nro.): 04
Nombre: Ingresar, actualizar, eliminar y listar secciones de los diferentes sección del cementerio	
Descripción: Gestión de Sección	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos un sector para poder ingresar una sección en dicho sector para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción sección en el cual encontrara las opciones ingresar, actualizar, eliminar y listar secciones a través de algunos botones en los cuales se deben hacer clic para realizar con éxito las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú sección y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar sección.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar secciones se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 83. Prueba de Aceptación de gestión de categoría (de tumba)

Caso de Prueba de Aceptación: Gestión de Categoría	
Código: 5	Historia de Usuario (Nro.): 05
Nombre: Ingresar, actualizar, eliminar y listar los Categorías de las tumbas	
Descripción: Gestión de Sección	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos una categoría para poder ingresar una tumba en dicho cementerio para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción tumba en el cual encontrara las opciones ingresar, actualizar, eliminar y listar a las tumbas a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú sección y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar trabajadores.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar trabajadores se han realizado exitosamente y sin error alguno.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 84. Prueba de Aceptación de Tipo (de cargo)

Caso de Prueba de Aceptación: Gestión de Tipo	
Código: 6	Historia de Usuario (Nro.): 06
Nombre: Ingresar, actualizar, eliminar y listar los tipos de cargo de las tumbas	
Descripción: Gestión de Sección	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos un trabajador para poder ingresar una tipo de cargo en dicho cementerio para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción tumba en el cual encontrara las opciones ingresar, actualizar, eliminar y listar a las tumbas a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú sección y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar trabajadores.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar trabajadores se han realizado exitosamente y sin error alguno.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 85. Prueba de Aceptación de gestión de Nichos

Caso de Prueba de Aceptación: Gestión de Nichos	
Código: 7	Historia de Usuario (Nro.): 07
Nombre: Ingresar, actualizar, eliminar y listar secciones de los diferentes sectores del cementerio	
Descripción: Gestión de Sección	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos una sección para poder ingresar un nicho en la sección respectiva para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción nichos en el cual encontrara las opciones ingresar, actualizar, eliminar y listar nichos a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú nicho y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar nicho.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar cementerios se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 86. Prueba de Aceptación de gestión de Sepulturas

Caso de Prueba de Aceptación: Gestión de Sepulturas	
Código: 8	Historia de Usuario (Nro.): 08
Nombre: Ingresar, actualizar, eliminar y listar las sepulturas que existen en las diferentes secciones, sectores y cementerio.	
Descripción: Gestión de Sección	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos una sección para poder ingresar una sepultura en la sección respectiva para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción sepulturas en el cual encontrara las opciones ingresar, actualizar, eliminar y listar sepulturas a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú nicho y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar sepultura.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar sepulturas e han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 87. Prueba de Aceptación de Mausoleos

Caso de Prueba de Aceptación: Gestión de Mausoleo	
Código: 9	Historia de Usuario (Nro.): 09
Nombre: Ingresar, actualizar, eliminar y listar los mausoleos que existen en las diferentes secciones, sectores y cementerios.	
Descripción: Gestión de Mausoleo	
Condiciones de Ejecución: El usuario debe ingresar tener ingresado por lo menos una sección para poder ingresar una sepultura en la sección respectiva para posteriormente proceder a otras operaciones como eliminar modificar y listar	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción sepulturas en el cual encontrara las opciones ingresar, actualizar, eliminar y listar sepulturas a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú nicho y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar sepultura.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar sepulturas e han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 88. Prueba de aceptación de registro de familiares

Caso de Prueba de Aceptación: Registro de Familiares	
Código: 9	Historia de Usuario (Nro.): 09
Nombre: Ingresar, actualizar, eliminar y listar los mausoleos de los diferentes familiares de los fallecidos	
Descripción: Gestión de Sección	
Condiciones de Ejecución: El usuario principal y el usuario tienen acceso a las operaciones agregar y buscar un familiar mientras que solo el Usuario Administrador puede eliminar y modificar un registro de la tabla sección.	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción familiar en el cual encontrara las opciones ingresar, actualizar, eliminar y listar secciones a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú familiar y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar familiar.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar familiar se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 89. Prueba de aceptación de registro de Fallecidos

Caso de Prueba de Aceptación: Registro de Fallecidos	
Código: 10	Historia de Usuario (Nro.): 10
Nombre: Ingresar, actualizar, eliminar y listar los mausoleos de los diferentes fallecidos	
Descripción: Gestión de Fallecido	
Condiciones de Ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción fallecido en el cual encontrara las opciones ingresar, actualizar, eliminar y listar fallecido a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción fallecido en el cual encontrara las opciones ingresar, actualizar, eliminar y listar fallecido a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú fallecido y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar familiar.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar fallecido se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 90. Prueba de aceptación de registro de Tumbas

Caso de Prueba de Aceptación: Registro de Tumbas	
Código: 11	Historia de Usuario (Nro.): 11
Nombre: Ingresar, actualizar, eliminar y listar los tumbas de cada tumbas	
Descripción: Gestión de Tumba	
Condiciones de Ejecución: El usuario principal y el usuario tienen acceso a las operaciones agregar y buscar una tumbas mientras que solo el Usuario Administrador puede eliminar y modificar un registro de la tabla tumba.	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción tumbas en el cual encontrara las opciones ingresar, actualizar, eliminar y listar tumbas a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú tumbas y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar tumbas.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar tumbas se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 91. Prueba de aceptación de Asignar

Caso de Prueba de Aceptación: Registro de Asignar	
Código: 11	Historia de Usuario (Nro.): 11
Nombre: Asignar nichos, sepulturas y mausoleos	
Descripción: Gestión de Asignación	
Condiciones de Ejecución: El usuario principal y el usuario tienen acceso a las operaciones asignar un nichos, sepulturas o mausoleos.	
Entrada / Pasos de ejecución: El usuario Administrador@/y/o Normal ingresa en el menú superior en la opción asignar en el cual encontrara las opciones asignar nichos, sepulturas y mausoleos a través de algunos botones en los cuales se deben hacer clic para realizar con éxitos las operaciones mencionadas.	
Resultado Esperado: El Usuario Principal debe acceder al menú asignar y ha podido realizar las operaciones de ingresar, actualizar, eliminar y listar tumbas.	
Evaluación de la Prueba: Las operaciones de ingresar, actualizar, eliminar y listar tumbas se han realizado exitosamente y sin error alguno	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

Tabla 92. Prueba de aceptación de Reportes

Caso de Prueba de Aceptación: Reportes	
Código: 11	Historia de Usuario (Nro.): 11
Nombre: Generación de Reportes.	
Descripción: Generación de Reportes.	
Condiciones de Ejecución: El usuario principal y el usuario tienen acceso a las operaciones de generación de reportes mientras que solo el Usuario Administrador puede eliminar y modificar una generación de reportes.	
Entrada / Pasos de ejecución: El usuario Administrador@/y Normal ingresa en el menú superior en la opción de generación de reportes. Para generar reportes existe botones los cuales se debe hacer clic para realizar con éxitos dicha operación.	
Resultado Esperado: El Usuario Principal y Normal puede acceder al menú de reportes y ha podido realizar las operaciones de generar los mismos.	
Evaluación de la Prueba: Los reportes han sido generados exitosamente por parte del Administrador/a y usuario normal.	

Fuente: http://www.grin.com/es/e-book/210194/sistema-automatizado-para-la-gestion-y-el-control-de-los-combustibles-en.

Adaptado por: Gavidia Marco & Jessica Valle

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS Y COMPUTACIÓN

ENCUESTA PARA LOS TÉCNICOS DEL DEPARTAMENTO DE SISTEMAS DEL ILUSTRE MUNICIPIO DE RIOBAMBA

Objetivo:

OBTENER INFORMACIÓN SOBRE LAS VULNERABILIDADES DE SOFTWARE QUE ESTARÍAN AFECTANDO NEGATIVAMENTE A LOS SISTEMAS INFORMÁTICOS EN EL ILUSTRE MUNICIPIO DE RIOBAMBA.

NOTA: PORFAVOR CONTESTAR LAS PREGUNTAS CON LA MAYOR SERIEDAD POSIBLE.

Género: Masculino _____Femenino _____

Responda las siguientes preguntas con una "X" según usted crea conveniente o conozca del tema.

1. **¿Conoce usted algunas de las siguientes vulnerabilidades que existen en los sistemas informáticos desarrollados en Php y MySql?**

SI ( ) NO ( ) Inyección Sql
SI ( ) NO ( ) Falsificación de Peticiones en Sitios Cruzados
SI ( ) NO ( ) Secuencias de Comandos de Sitios Cruzados

2. **¿Qué niveles de riesgo asignaría al factor de probabilidad de explotación (violación de la seguridad en los sistemas informáticos) a las siguientes vulnerabilidades?**

Tabla 93. Factor de probabilidad de Explotación

Valores factor de probabilidad de explotación			Vulnerabilidades
	Difícil	1	Inyección Sql
	Media	2	
	Fácil	3	
	Difícil	1	Falsificación de Peticiones en Sitios
	Media	2	
	Fácil	3	
	Difícil	1	Secuencias de Comandos de Sitios Cruzados
	Media	2	
	Fácil	3	

Adaptado por: Gavidia Marco & Jessica Valle

3. **¿Con que Prevalencia (Frecuencia) las vulnerabilidades siguientes se manifiestan en los sistemas Informáticos?**

Tabla 94. Factor de Probabilidad de Prevalencia

Valores factor de probabilidad de prevalencia			Vulnerabilidades
	Poco Común	1	Inyección Sql
	Común	2	
	Difundida	3	
	Muy Difundida	4	
	Poco Común	1	Falsificación de Peticiones en Sitios
	Común	2	
	Difundida	3	
	Muy Difundida	4	
	Poco Común	1	Secuencias de Comandos de Sitios Cruzados
	Común	2	
	Difundida	3	
	Muy Difundida	4	

Adaptado por: Gavidia Marco & Jessica Valle

4. **¿Cómo calificaría el nivel de Detección (Localización) en los sistemas informáticos para las vulnerabilidades siguientes?**

Tabla 95. Factor de Probabilidad de Detección

Valores factor de probabilidad de detección			Vulnerabilidades
	Difícil	1	Inyección Sql
	Media	2	
	Fácil	3	
	Difícil	1	Falsificación de Peticiones en Sitios
	Media	2	
	Fácil	3	
	Difícil	1	Secuencias de Comandos de Sitios Cruzados
	Media	2	
	Fácil	3	

Adaptado por: Gavidia Marco & Jessica Valle

5. **¿El Impacto (grado de criticidad) que tiene cada una de estas Vulnerabilidades en los sistemas informáticos es:**

Tabla 96. Factor de Probabilidad de Impacto

Valores factor de probabilidad de impacto			Vulnerabilidades
	Menor	1	Inyección Sql
	Considerado	2	
	Grave	3	
	Menor	1	Falsificación de Peticiones en Sitios
	Considerado	2	
	Grave	3	
	Menor	1	Secuencias de Comandos de Sitios Cruzados
	Considerado	2	
	Grave	3	

Adaptado por: Gavidia Marco & Jessica Valle

Gracias por su ayuda…

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS Y COMPUTACIÓN

ENCUESTA PARA LOS TÉCNICOS DEL DEPARTAMENTO DE SISTEMAS DEL ILUSTRE MUNICIPIO DE RIOBAMBA

Objetivo:

OBTENER INFORMACIÓN DE LOS SISTEMAS INFORMÁTICOS A NIVEL DE SOFTWARE PARA SABER SI MEJORÓ LA SEGURIDAD EN EL SISTEMA DEL CEMENTERIO MUNICPAL DE RIOBAMBA.

NOTA: PORFAVOR CONTESTAR LAS PREGUNTAS CON LA MAYOR SERIEDAD POSIBLE.

Género: Masculino _____Femenino _____

Responda las siguientes preguntas con una "X" según usted crea conveniente o conozca del tema.

1. **¿Usted nota la mejora del factor de riesgo de explotación (violación de la seguridad en los sistemas informáticos) en el sistema SGMR?**

Tabla 97. Factor de Explotación con Protección

Valores factor de probabilidad de explotación			Vulnerabilidades
	Difícil	1	Inyección Sql
	Media	2	
	Fácil	3	
	Difícil	1	Falsificación de Peticiones en Sitios
	Media	2	
	Fácil	3	
	Difícil	1	Secuencias de Comandos de Sitios Cruzados
	Media	2	
	Fácil	3	

Adaptado por: Gavidia Marco & Jessica Valle

2. **¿Ha disminuido la Prevalencia (Frecuencia) de las vulnerabilidades en el sistema SGMR?**

Tabla 98. Factor de Prevalencia con Protección

Valores factor de probabilidad de prevalencia			Vulnerabilidades
	Poco Común	1	Inyección Sql
	Común	2	
	Difundida	3	
	Muy Difundida	4	
	Poco Común	1	Falsificación de Peticiones en Sitios
	Común	2	
	Difundida	3	
	Muy Difundida	4	
	Poco Común	1	Secuencias de Comandos de Sitios Cruzados
	Común	2	
	Difundida	3	
	Muy Difundida	4	

Adaptado por: Gavidia Marco & Jessica Valle

3. **¿Ha mejorado la Detección (Localización) de las vulnerabilidades en el sistema SGMR?**

Tabla 99. Factor de Detección con Protección

Valores factor de probabilidad de detección			Vulnerabilidades
	Difícil	1	Inyección Sql
	Media	2	
	Fácil	3	
	Difícil	1	Falsificación de Peticiones en Sitios
	Media	2	
	Fácil	3	
	Difícil	1	Secuencias de Comandos de Sitios Cruzados
	Media	2	
	Fácil	3	

Adaptado por: Gavidia Marco & Jessica Valle

4. **¿Ha Mejorado el Impacto (grado de criticidad) que tiene cada una de estas Vulnerabilidades en el sistema SGMR?**

Tabla 100. Factor de Impacto con Protección

Valores factor de probabilidad de impacto			Vulnerabilidades
	Menor	1	Inyección Sql
	Considerado	2	
	Grave	3	
	Menor	1	Falsificación de Peticiones en Sitios
	Considerado	2	
	Grave	3	
	Menor	1	Secuencias de Comandos de Sitios Cruzados
	Considerado	2	
	Grave	3	

Adaptado por: Gavidia Marco & Jessica Valle

5. **¿Una vez que usted ha usado el sistema SGMR ha observado que la seguridad ha mejorado ante las vulnerabilidades analizadas?**

SI ( ) NO ( )

6. ¿Qué le pareció el diseño de la interfaz que tiene el sistema SGMR?

Regular ( )

Buena ( )

Muy Buena ( )

Gracias por su ayuda…

10.2 GLOSARIO DE TERMINOS

10.2.1 Amenaza Informática

Es todo elemento o acción capaz de atentar contra la seguridad de la información, surge a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

10.2.2 Ataque Informático

Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

10.2.3 Bóveda

Construcción arquitectónica en forma de arco que cubre el espacio entre dos muros o varios pilares.

10.2.4 CSRF

Falsificación de petición en sitios cruzados, es un tipo de exploit malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web.

10.2.5 Código Malicioso

Es un conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso.

10.2.6 Encriptación

Es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación

10.2.7 Evento

Un evento es una acción que es detectada por un programa

10.2.8 Fraude

Es un engaño que está destinado a perjudicar la propiedad o patrimonio de una persona determinada, sea ésta natural o jurídica.

10.2.9 Hackers

Un hacker es alguien que descubre las debilidades de una computadora o de una red informática, pueden estar motivados por una multitud de razones, incluyendo fines de lucro.

10.2.10 Inyección Sql

Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

10.2.11 MY SQL

Es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.

10.2.12 Nicho

También se trata de la concavidad formada para colocar los féretros en un cementerio.

10.2.13 Owasp

Es el proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) ayuda a las organizaciones a entender y mejorar la seguridad de sus aplicaciones y servicios web.

10.2.14 Owasp Zap

Es una herramienta libre escrita en Java proveniente del Proyecto OWASP para realizar, en primera instancia, tests de penetración en aplicaciones web.

10.2.15 PHP

Es un lenguaje de código abierto muy popular, adecuado para desarrollo web y que puede ser incrustado en HTML.

10.2.16 Prevención

Es el resultado de concretar la acción de prevenir, la cual implica el tomar las medidas precautorias necesarias y más adecuadas con la misión de contrarrestar un perjuicio o algún daño que pueda producirse.

10.2.17 Protección

Es un cuidado preventivo ante un eventual **riesgo** o problema.

10.2.18 Scripts

Es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano.

10.2.19 SGCMR

Sistema de Gestión para el Cementerio Municipal de Riobamba.

10.2.20 Seguridad Informática

Es el área de la informática que se enfoca en la protección de la infraestructura computacional. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

10.2.21 Sepultura

Es el lugar donde se depositan los restos mortales o cadáveres de los difuntos (inhumación). Depende de la cultura del lugar, los cuerpos pueden introducirse en ataúdes, féretros o sarcófagos, o simplemente envolverse en telas.

10.2.22 Software

Es un conjunto de instrucciones detalladas que controlan la operación de un sistema computacional.

10.2.23 Spyware

Recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

10.2.24 TIC

Tecnologías de la Información y las Comunicación TICS al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones

10.2.25 Vulnerabilidad Informática

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño.

10.2.26 Xampp

Es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl.

10.2.27 XSS

Secuencia de comandos en sitios cruzados, es un problema de seguridad en las páginas web, generalmente por vulnerabilidades en el sistema de validación de datos entrantes. Un ataque XSS consiste en enviar un script malicioso a la página, ocultándolo entre solicitudes legítimas.

10.3 MANUAL USUARIO

Manual de Usuario

Para:

Sitio Web & Sistema CMR

Cementerio Municipal

GAD RIOBAMBA

Versión 1.0

Preparado por:

Marco Vinicio Gavidia Villacrés **marco_gavidia@hotmail.com**

Jessica Janneth Valle Padilla **jessy_valle19@yahoo.es**

Asistencia Técnica: Lola Rodríguez, Laura Lema

Fecha: Mayo 2014

INTRODUCCIÓN

En este documento se describirá los objetivos e información clara, concisa de cómo utilizar el sistema para el control y ubicación de las personas fallecidas en el cementerio municipal de Riobamba para la web y su funcionamiento.

El sistema web podrá encontrar toda la información necesaria acerca del Cementerio Municipal de Riobamba y del personal encargado, como también otros servicios:

Calendario de eventos.

El sistema del Cementerio Municipal de Riobamba.

Registro de Usuario

Contador de Visitas

El sistema para el control y ubicación de las personas fallecidas en el cementerio municipal de Riobamba fue creado con el objetivo de informar, controlar y controlar la información de las personas fallecidas, además dar a conocer todos los documentos que se necesita para poder enterrar, exhumar algún familiar fallecido.

Es de mucha importancia consultar este manual antes y/o durante la visualización de las páginas, ya que lo guiará paso a paso en el manejo de las funciones en él.

Con el fin de facilitar la comprensión del manual, se incluye gráficos explicativos.

OBJETIVO DE ESTE MANUAL

El objetivo primordial de este Manual es ayudar y guiar al usuario a utilizar el Sistema para el control de las personas fallecidas, registro de representante legal, registro del número de bóveda, nicho o sepultura de las personas fallecidas en el cementerio municipal de Riobamba en la que se obtiene la información deseada para poder despejar todas las dudas existentes.

DIRIGIDO

Este manual está orientado a los usuarios finales involucrados en la etapa de Operación del sitio web a utilizar el Sistema para el control de las personas fallecidas, registro de representante legal, registro del número de bóveda, nicho o sepultura de las personas fallecidas en el cementerio municipal de Riobamba y para todas las personas de la ciudad de Riobamba que van a interactuar con el sitio web.

CONOCIMIENTOS PREVIOS

Los conocimientos mínimos que deben tener las personas que operarán las páginas y deberán utilizar este manual son:

Conocimientos básicos acerca de Programas Utilitarios

Conocimientos básicos de Navegación en Web.

Conocimiento básico de Internet

Conocimiento básico de Windows

ESPECIFICACIONES TÉCNICAS

HARDWARE

Cliente Requerido

El Software soporta Internet Explore8, Joomla! 3.2.2 Stable, xampp 1.8.2.0 VC9y las siguientes versiones.

Servidor Windows

El sistema requiere básicamente todo lo que una instalación de Dominio Server requiere.

Se recomienda que se utilicen los requerimientos expuestos anteriormente para la mejor funcionalidad del Web Site.

SOFTWARE

La Base de Datos requerida para el sistema es Domino – Notes

El Software del Servidor es Domino Server, el sistema se puede administrar a través de la Web.

INGRESO AL SITIO WEB Y SISTEMA CMR

USO DEL WEBSITE CEMENTERIO MUNICIPAL DE RIOBAMBA

Para acceder a la página principal del Cementerio Municipal de Riobamba se debe ingresar a la siguiente dirección web.

http://www.cementerioderiobamba.com

Figura 67. Pantalla de Bienvenida del Cementerio Municipal de Riobamba

Adaptado: Marco Gavidia & Jessica Valle

ELEMENTOS DE LA PÁGINA PRINCIPAL DEL SITIO WEB

Como se puede observar en la ilustración 2, el Sitio Web Informativo consta de 4 partes básica:

Cabecera en la parte superior

Menú Superior

Contenidos en la parte central, donde se encuentra un breve reseña de bienvenida del Cementerio Municipal de Riobamba.

Calendario en la parte derecha.

Figura 68. Partes de la Página del Cementerio Municipal de Riobamba

Fuente: Interfaz de la Pagina CMR.Adaptado por: Gavidia Marco & Jessica Valle

Figura 69. Partes de la Interfaz del sitio web del CMR

Adaptado: Marco Gavidia & Jessica Valle

La cabecera es la parte más importante de la página web ya que en ella se encuentra la imagen corporativa que identifica al Cementerio Municipal de Riobamba como también encontrar otros servicios que son:

- ✓ Inicio
- ✓ Misión & Visión
- ✓ ¿Quiénes Somos?
- ✓ El Cementerio
- ✓ Antecedentes
- ✓ Historia
- ✓ Personajes Destacados
- ✓ Historia del Cementerio
- ✓ Personal Administrativo
- ✓ Funerarias
- ✓ Sistema CMR
- ✓ Contáctenos

Figura 70. Menú Superior

Adaptado: Marco Gavidia & Jessica Valle

MENÚ REGISTRO/ ACCESO DE USUARIOS

La única sección de la página que requiere que el usuario introduzca información es la sección de registro de usuarios, el comprende 2 sitios diferentes

ACCESO DE USUARIOS REGISTRADOS

Que consta de 2 campos: Nombre de Usuario y Contraseña

Figura 71. Acceso de Usuarios del CMR Website

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE NUEVOS USUARIOS

Que consta de 4 campos: Nombre, Usuario, Contraseña y Dirección de Correo Electrónico

Figura 72. Registro de Usuarios Nuevos del CMR Website

Adaptado: Marco Gavidia & Jessica Valle

El usuario registrado solo podrá hacer uso de su cuenta cuando el administrador de la página web haya validado su registro.

CALENDARIO

Visualiza el calendario del mes actual y día

Figura 73. Calendario del CMR Website

Adaptado: Marco Gavidia & Jessica Valle

CONTADOR DE VISITAS

En la parte izquierda se encuentra el contador de visitas el cual nos muestra cuantas personas visitaron la página lo podrán ver por día, semanas y por meses.

Figura 74. Contador de visitas del CMR Website

Adaptado: Marco Gavidia & Jessica Valle

USO DEL SISTEMA CMR

ANTES DE EMPEZAR

Para la mejor utilización de este programa usted debe:

Configurar la pantalla de su navegador en una resolución de 1024 por 768 pixeles.

Utilizar como navegador Internet Explorer 8.0 o Mozilla Firefox 5.0 o superiores.

Para acceder al Sistema CMR de Riobamba se debe ingresar a la siguiente dirección web.

Luego debe hacer clic en SISTEMA CMR.

Figura 75. Como ingresar al Sistema CMR desde la Pagina Web

Adaptado: Marco Gavidia & Jessica Valle

ELEMENTOS DEL SISTEMA CMR

Como se puede observar en la ilustración 2, el Sitio Web Informativo consta de 5 partes básica:

- ✓ Interfaz de Autenticación.
- ✓ Cabecera en la parte superior (banner)
- ✓ Menú Superior
- ✓ Menú Lateral
- ✓ Contenidos en la parte central.

Luego usted va a visualizar la siguiente ventana donde podrá autenticarse al ingresar el usuario y contraseña.

MODULO DE LOGIN

La siguiente interfaz permite ingresar al Sistema CMR. La interfaz consta de un usuario y contraseña como se muestra a continuación.

Figura 76. Interfaz de autenticación del Sistema CMR

Adaptado: Marco Gavidia & Jessica Valle

MODULO DE CEMENTERIO

REGISTRO DE CEMENTERIO

Para registrar un Cementerio se debe dar clic en el menú de Cementerio y luego ingresar, inmediatamentedebe llenar los siguientes campos: Nombre, Dirección, Teléfono.

Luego de haber ingresado un cementerio podrá escoger las siguientes opciones: actualizar, listar y eliminar.

.

Figura 77. Módulo Cementerio

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE SECTOR

Para registrar un Sector se debe dar clic en el menú de Sector y luego ingresar, inmediatamentedebe llenar los siguientes campos: Seleccionar un Cementerio, llenar el nombre del sector.

Luego de haber ingresado un sector podrá escoger las siguientes opciones: actualizar, listar y eliminar.

Figura 78. Módulo de Sector

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE SECCIÓN

Para registrar una Sección se debe dar clic en el menú de Sección y luego ingresar, inmediatamentedebe llenar los siguientes campos: Seleccionar un Sector, llenar el nombre de sección.

Luego de haber ingresado una sección podrá escoger las siguientes opciones: actualizar, listar y eliminar.

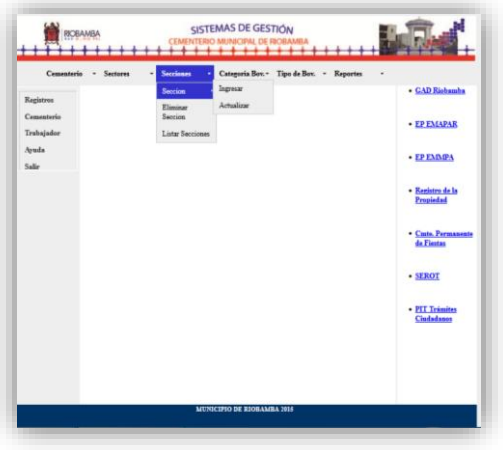


Figura 79. Módulo de Sección

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ DE CATEGORIA DE BÓVEDAS

Para registrar una Categoría de Bóvedas se debe dar clic en el menú Categoría y luego ingresar, inmediatamentedebe ingresar una categoria ya sea municipal, privada o sin nombre.

Luego de haber ingresado una categoría podrá escoger las siguientes opciones: actualizar, listar y eliminar.

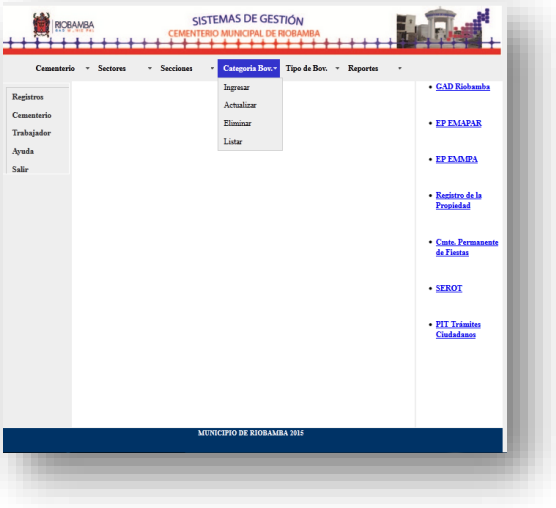


Figura 80. Módulo de Categoría de Bóvedas

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ DE TIPOS DE BÓVEDAS

Para registrar un tipo de bóveda se debe dar clic en el menú de tipo de bóveda y luego debe escoger nicho, sepultura o mausoleo donde debera ingresar el nombre de la sección y el numero de cada uno de ellos.

Luego de haber ingresado un tipo de bóveda podrá escoger las siguientes opciones: actualizar, listar y eliminar.

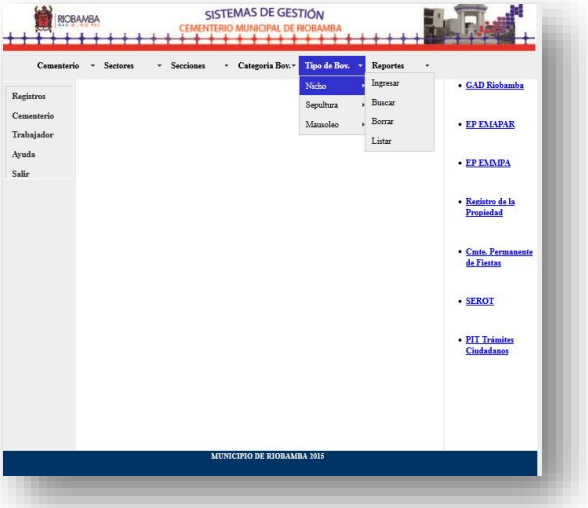


Figura 81. Módulo de Tipos de Bóvedas

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE REPORTES

Para obtener un reporte se debe dar clic en el menú total para escoger las siguientes opciones: nicho, sepultura y mausoleo, para ello se debe seleccionar los siguientes campos: Cementerio, Sector, Sección.

Se mostrará una tabla con los datos requidos.

Figura 82. Módulo de Reportes

Adaptado: Marco Gavidia & Jessica Valle

MODULO DE REGISTRO

REGISTRO DE FAMILIARES

Para registrar Familiares se debe dar clic en el menú familiar y luego ingresar, inmediatamente debe llenar los siguientes campos: Cédula, Nombre, Apellido, Dirección, Teléfono y el Correo.

Luego de haber ingresado un Familiar podrá escoger las siguientes opciones: actualizar, listar y eliminar.

Figura 83. Módulo de Familiar

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE FALLECIDOS

Para registrar Fallecidos se debe dar clic en el menú Fallecido y luego ingresar, inmediatamente debe llenar los siguientes campos: Nombre, Apellido y la Fecha de Fallecimiento.

Luego de haber ingresado un fallecido podrá escoger las siguientes opciones: actualizar, listar y eliminar.

Figura 84. Módulo de Fallecidos

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE TUMBAS

Para registrar Tumbas se debe dar clic en el menú tumbas y luego ingresar, inmediatamente debe seleccionar la categoría: Municipal, Propietario o Sin Nombre.

Luego de haber ingresado una tumba podrá escoger las siguientes opciones: actualizar, listar, buscar y eliminar.

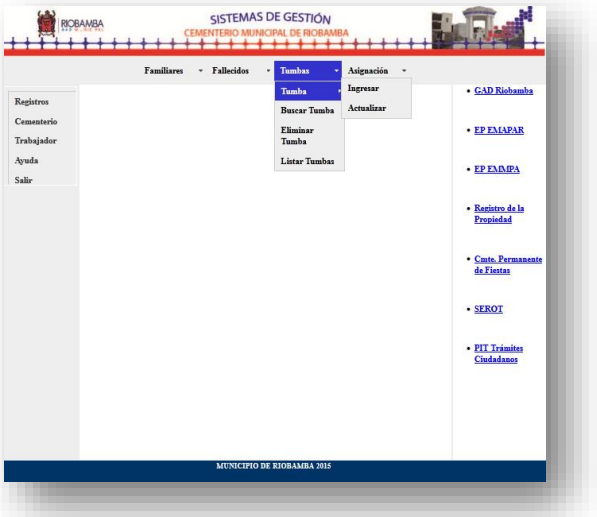


Figura 85. Módulo de Tumbas

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE ASIGNACIÓN

Para registrar Asignación se debe dar clic en el menú asignación y debe escoger las siguientes opciones: nicho, sepultura y mausoleo. Además debe seleccionar Cementerio, Sector y Sección para obtener un reporte.

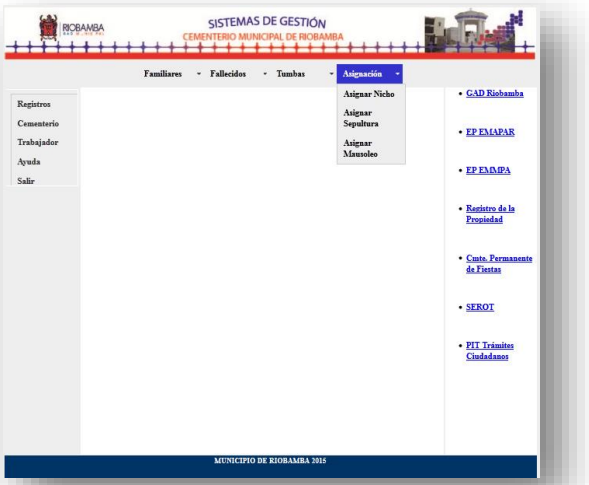


Figura 86. Módulo de Asignación

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE TRABAJADOR

Para registrar Trabajador se debe dar clic en el menú Trabajador y luego ingresar, inmediatamente debe selccionar el Cementerio, Cargo y llenar los siguientes campos: Nombre, Apellido, Salario, Categoría.

Luego de haber ingresado un trabajador podrá escoger las siguientes opciones: actualizar, listar y eliminar.

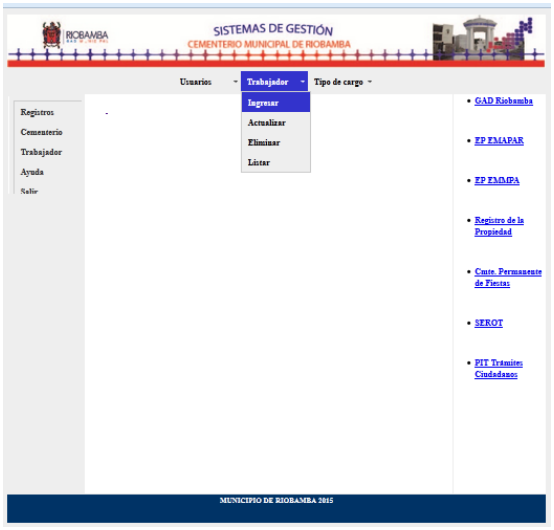


Figura 87. Módulo de Trabajador

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ TIPO DE TRABAJADOR

Para registrar Tipo de Trabajador se debe dar clic en el menú Ingresar, inmediatamente debe selccionar el Cargo del trabajador. Además podrá escoger las siguientes opciones: actualizar, listar y eliminar.

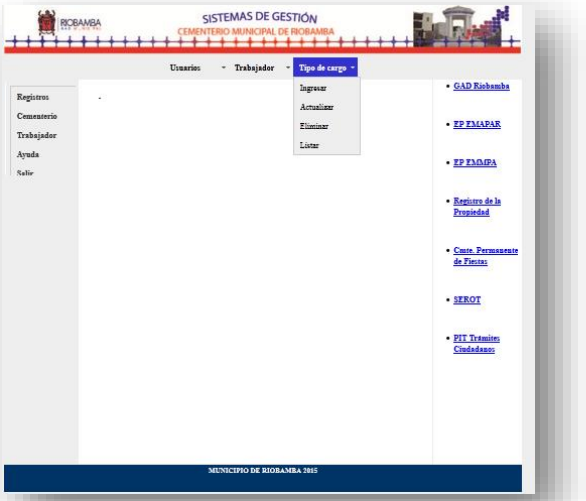


Figura 88. Módulo de Registro de Trabajador

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ USUARIOS

Para registrar a los Usuarios se debe dar clic en el menú Ingresar, inmediatamente debe seleccionar el tipo de usuario y llenar los siguientes campos: Nombre, Apellido, Login, Dirección, Teléfono. Además podrá escoger las siguientes opciones: actualizar, listar y eliminar.

Figura 89. Módulo de Registro de Usuarios

Adaptado: Marco Gavidia & Jessica Valle

GLOSARIO DE TERMINOS

A

APACHE: (Acrónimo de "a patchy server"). Servidor web de distribución libre y de código abierto, **APPSERVER: es** una herramienta OpenSource para Windows que facilita la instalación de Apache, MySQL y PHP en la cual estas aplicaciones se configuran en forma automática.

B

BACK-END: El front-end es la parte del software que interactúa con el o los usuarios y el back-end es la parte que procesa la entrada desde el front-end.

BANNER*:* Un ***banner*** (*en español*: banderola) es un formato publicitario en Internet.

C

CACHÉ: es una referencia por rango de inicio y otro de fin1 (/ˈkæʃ/ o /kaʃ/) usada por la unidad central de procesamiento de una computadora.

CHECK BOX: Elemento de interfaz gráfico (widget) que permite al usuario marcar múltiples selecciones de un número de opciones. Generalmente son mostrados en pantalla como cuadraditos que pueden estar vacíos (para falso) o tildados o rellenos (para verdadero). Por lo general al lado de los cuadrados hay un texto que explica el significado de que el casillero esté o no chequeado.

COMBOBOX: (lista desplegable con entrada). Elemento GUI que permite al usuario escribir sobre este o seleccionar una opción de una lista existente de opciones. Un ejemplo de combo box son las barras de direcciones usadas en los navegadores web.

F

FILEZILLA: es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de GNU. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS).

FILTRO: Un programa para acceder a una corriente de datos:

FORMULARIO: Se llama formulario a una página con espacios vacíos que han de ser rellenados con alguna finalidad, por ejemplo una solicitud de empleo en la que has de rellenar espacios libres con la información personal requerida.

FRONT-END: Es la parte del software que interactúa con el o los usuarios

FTP: (siglas en inglés de ***F****ile* ***T****ransfer* ***P****rotocol*, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

H

HOSTING: El alojamiento web (en inglés *web hosting*) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

L

LOGIN: (en español **ingresar** o **entrar**) es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizará credenciales provistas por el usuario.

M

MÓDULO: Un **módulo de** Joomla es un mecanismo para usar bibliotecas de código externas a un sitio creado en Joomla.

P

PHP: es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas

PORTAL WEB: Un portal de Internet es un sitio web cuya característica fundamental es la de servir de *Puerta de entrada* (única) para ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema.

PLUG-IN: Un complemento es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API. También se lo conoce como **plug-in** (del inglés "enchufable"), **add-on** (agregado), complemento, conector o extensión.

S

SMTP: Simple Mail Transfer Protocol (**SMTP** Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.).

10.4 **MANUAL TÉCNICO**

Manual de Técnico

Para:

Sitio Web & Sistema CMR

Cementerio Municipal

GAD RIOBAMBA

Versión 1.0

Preparado por:

Marco Vinicio Gavidia Villacrés **marco_gavidia@hotmail.com**

Jessica Janneth Valle Padilla **jessy_valle19@yahoo.es**

Asistencia Técnica: Lola Rodríguez, Laura Lema

Fecha: Julio 2015

INTRODUCCIÓN

El sistema Sitio Web & Sistema CMR Cementerio Municipal está compuesto de forma que permita que la información contenida pueda ser agregada, editada y/o eliminada por personal encargado de los departamentos.

Para alcanzar estos propósitos se ha hecho uso de PHP que es un lenguaje que se adecua a las nuevas necesidades de las aplicaciones web actuales, sin la necesidad de actualizaciones bruscas que generen más problemas que soluciones.

A través de esta tecnología la administración y seguridad de la información se dará de forma centralizada y segura de datos, al mismo tiempo facilita la actualización eficiente de dicha información.

Acerca de la página no ha sido posible especificar lo que un sitio web debe o no contener a la salida de un proceso de desarrollo totalmente, porque su estructura y funcionalidad evolucionará con el tiempo. Además, la información contenida y presentada dentro de un sitio web también cambiará. La habilidad de mantener la información y la estructura del sitio son considerados al desarrollar el sito. Estos factores hacen del desarrollo de aplicaciones web sean diferentes al desarrollo del software tradicional.

La mayoría de los sistemas web posee información y satisfacen las necesidades del usuario continuamente, de ahí que los desarrolladores permiten adoptar sus principios.

En cuanto a este manual se ha considerado incluir todos los aspectos técnicos necesarios mana el manejo, instalación y control tanto del sistema como el sitio web para el Cementerio Municipal de Riobamba.

OBJETIVO DE ESTE MANUAL

El objetivo primordial de este Manual es ayudar y guiar al técnico a informarse y utilizar herramientas para que Sistema de Gestión del Cementerio Municipal de Riobamba entre en producción(ejecución) para de esa manera poder hacer uso de la información deseada para poder despejar todas las dudas existentes y para poder comprender:

- Guía para gestión de herramientas para poner en funcionamiento el sistema para el gestión del cementerio municipal de Riobamba
- Conocer cómo utilizar el sistema, mediante una descripción detallada e ilustrada de las opciones.
- Conocer el alcance de toda la información por medio de una explicación detallada e ilustrada de cada una de las páginas que lo conforman el manual técnico.

DIRIGIDO

Este manual está orientado a los técnicos u otros tipos de personal encargado de departamento de sistemas del GAD Riobamba.

Solamente dichas personas están autorizadas a realizar modificaciones en el sistema.

Una vez finalizado el proyecto el Departamento del GAD Riobamba está encargado de definir políticas, normas, etc. para la administración del sistema CMR y el sitio web.

También a través de este manual el personal podrá estar en la capacidad de supervisar el cumplimiento de políticas, normas, etc. que permitan el correcto funcionamiento de los Sistemas.

Definir conjuntamente con los departamentos pertinentes, los contenidos o cambios para el o los sistema para que también de igual forma puedan ser capacitados en herramientas necesarias para el mantenimiento y ejecución

CONOCIMIENTOS PREVIOS

Los conocimientos mínimos que deben tener las personas que operarán las páginas y deberán utilizar este manual son:

- Conocimientos básicos acerca de Programas Utilitarios
- Conocimientos básicos de Navegación en Web.
- Conocimiento básico de Internet
- Conocimiento básico de Windows

Pasos para encender la computadora

Encienda el C.P.U. presionar el botón Power (Ver Figura N 1)

Encienda el monitor presionar el botón Power (Ver Figura N 1)

Figura 90. Botón de Encendido de la Persona

Fuente: http://www.cca.org.mx/profesores/abc/imagenes/m1/u2/t1/encendido.jpg

Espere mientras carga el Sistema Operativo. La apariencia de la pantalla mientras se carga el sistema es de un color negro y se aprecia la frase de iniciar Windows.

Automáticamente aparecerá la pantalla de Windows. La pantalla de Windows puede ser de varios tipos o diseño.

ESPECIFICACIONES TÉCNICAS

Para la implementación del Web Sitie Sistema para el control y ubicación de las personas fallecidas en el cementerio municipal de Riobamba para la web requerimos lo siguiente:

HARDWARE

Cliente Requerido

El Software soporta Internet Explore8, Joomla! 3.2.2 Stable, xampp 1.8.2.0 VC9y las siguientes versiones.

Servidor Windows

El sistema requiere básicamente todo lo que una instalación de Dominio Server requiere.

Se recomienda que se utilicen los requerimientos expuestos anteriormente para la mejor funcionalidad del Web Site.

SOFTWARE

- La Base de Datos requerida para el sistema es Domino – Notes

El Software del Servidor es Domino Server, el sistema se puede administrar a través de la Web.

REGLAS DE NEGOCIO

DEFINICIÓN DE REGLAS DEL NEGOCIO SITIO WEB

- ✓ La plataforma para desarrollar el Sitio Web Informativo es Joomla 3.2.2, la misma que ha sido utilizada en otros sistemas web de la Institución, por motivos de seguridad.
- ✓ Todos los Sistemas Web Informativos deben manejar la imagen corporativa del Municipio de Riobamba.

DEFINICIÓN DE REGLAS DEL NEGOCIO SGCMR

- Iniciar Sesión: Autenticación de usuario con nombre y contraseña
- Cementerio: Buscar

- Área: Buscar
- Bóvedas: Agregar ,Eliminar y modificar los diferentes tipos de Bóvedas(Institucionales ,Municipal y Propietarios)
- Nichos: Agregar ,Eliminar y modificar los diferentes tipos de Nichos(Institucionales ,Municipal y Propietarios)
- Sepultura en el Suelo: Agregar ,Eliminar y modificar los diferentes tipos de Sepulturas en el Suelo (Institucionales ,Municipal y Propietarios)
- Personas fallecidas: Búsqueda personas fallecidas que están en bóvedas, nichos y sepulturas en el suelo.
- Contribuyentes: Búsqueda de contribuyentes del servicio de mantenimiento de bóvedas, nichos y sepultura en el suelo.
- Reportes:
    - Búsquedas de personas por apellidos
    - Cobro de Mantenimientos por bóveda usada o nicho usado
    - Cantidad de Bóvedas especiales
    - Cantidad de Bóvedas extras y generales
    - Cantidad de Bóvedas Institucionales.
    - Cantidad de nichos
    - Resumen total de bóvedas y nichos ocupados y desocupados.
    - Enlace a búsquedas desde página web de información de personas fallecidas.

DESCRIPCIÓN DEL SITIO WEB Y SGCMR

DESCRIPCIÓN DEL SITIO WEB INFORMATIVO DEL CMR

El Sitio Web constará de toda la información del Cementerio, contendrá una portada atractiva para los visitantes de este sistema, mostrará una bienvenida de la Dra. Lola Rodríguez directora del Cementerio, tendrá un menú superior para mayor facilidad de navegación.

En el menú superior encontrará las siguientes opciones:

- ✓ Inicio
- ✓ Misión & Visión
- ✓ ¿Quiénes Somos?
- ✓ El Cementerio
- ✓ Antecedentes
- ✓ Historia
- ✓ Personajes Destacados
- ✓ Historia del Cementerio
- ✓ Personal Administrativo
- ✓ Funerarias
- ✓ Sistema CMR
- ✓ Contáctenos

Acceso:

- ✓ Usuario
- ✓ Contraseña

DESCRIPCIÓN DEL SISTEMA DE GESTION DEL CMR

El Sistema de Gestión constará de toda la información que se maneja en cuanto los servicios funerarios del Cementerio, contendrá una interfaz atractiva para los usuarios de este sistema, la cual será aprobada por el Departamento de Sistemas y

El departamento Administrativo del Cementerio a cargo de la Dra. Lola Rodríguez directora del Cementerio, tendrá un menú superior para mayor facilidad de navegación.

En el menú superior encontrará las siguientes opciones:

Menú de Registro:

- ✓ Familiares
- ✓ Fallecidos
- ✓ Tumbas
- ✓ Asignación
- ✓ Ayuda

Menú cementerio

- ✓ Cementerio
- ✓ Sectores
- ✓ Secciones
- ✓ Trabajadores
- ✓ Tipos
- ✓ Calificación
- ✓ Usuario
- ✓ Reportes

DESCRIPCIÓN DE COTENIDO DEL SITIO WEB Y SGCMR

Para la realización de este sitio web se basó fundamentalmente en las necesidades que tenía el Cementerio Municipal de Riobamba aquí pueden publicar toda la información relacionada con su funcionamiento y descripción en general.

Una de los requerimientos del Sitio Web y del SGCMR es que sea fácil de navegar para el usuario a través de su interfaz., es por este motivo que este sitio web tiene las siguientes características.

- ✓ Plataforma Joomla 3.2.2 (Sitio Web)
  - o Imágenes
  - o Módulos
  - o Plugins

- ✓ XAMPP

A continuación se tiene toda la información fundamental de cada uno de estos aspectos.

JOOMLA 3.2.2

Joomla! 3.2.2 permite crear, administrar y organizar el contenido más fácilmente que en versiones anteriores.

Joomla es un sistema de administración de contenido (CMS) más popular y ampliamente utilizado. Su última versión 3.2.2 hace más fácil e intuitivo crear cualquier tipo de sitio web con aplicaciones en línea que te proporcionan abundancia de características.

La facilidad de uso, extensibilidad y un modelo para fácil aprendizaje han hecho que Joomla sea el software CMS más popular hoy en día. Lo mejor de todo, Joomla es código abierto y gratis para todos.

Joomla 3.2.2 realiza un seguimiento a cada parte del contenido en tu sitio web, el contenido puede ser texto simple, fotos, música, video, documentos, o casi cualquier otra cosa que te puedas imaginar.

XAMPP

XAMPP es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl. El nombre proviene del acrónimo de X (para cualquiera de los diferentes sistemas operativos), Apache, MySQL, PHP, Perl.

El programa está liberado bajo la licencia GNU y actúa como un servidor web libre, fácil de usar y capaz de interpretar páginas dinámicas. Actualmente XAMPP está disponible para Microsoft Windows, GNU/Linux, Solaris y MacOS X.

INSTALACION DEL SITIO WEB Y SGCMR

El sitio web Y el sistema de gestión CMR se ha desarrollado en un entorno local y los pasos para la instalación son
Instalar en el ordenador la versión de php 5.4.16 y mysql 4.0.4 con la versión de apache 2.4.4 que es la mínima para que funcione el CMS de Joomla versión 3.2.2.; que para facilitar el trabajo se podría instalar XAMP versión para sistema operativo Windows en su versión 1.8.2.0 VC9.

Abrimos el navegador y en la barra de direcciones se coloca http://localhost/phpmyadmin/ en el cual tendrá que crear una base de datos que se llame cementerios, la cual está destinada para el sitio web del cementerio Municipal de Riobamba. Y una base de datos que se llame cementerio la cual está destinada para el sistema.
Luego se procede a importar los datos a través de un archivo de consulta sql que está dentro del CD.
Ahora nos dirigimos a la dirección C:\xampp\htdocs o el directorio donde esté instalado la aplicación de xamp.
Para el sitio web y el sistema esté en internet debe asegurarse que el servicio que le ofrecen de hosting soporte los requerimientos indicados, si cumple con estos pasos se procederá a editar el archivo configuration.php y se procede a editar la líneas que contengan var $host = 'localhost'; sustituimos localhost por el nombre de nuestro portal así mismo se recomienda configurar las variables que se encuentran como el servicio de smtp el servicio de ftp el cache etc.
Para subir el portal se recomienda instalar el filezilla cliente.

ELEMENTOS DEL SITIO WEB Y SGCMR

ELEMENTOS DEL SITIO WEB

Figura 91. Elementos del Sitio Web
Adaptado por: Marco Gavidia. & Jessica Valle

ELEMENTOS DEL SISTEMA CMR

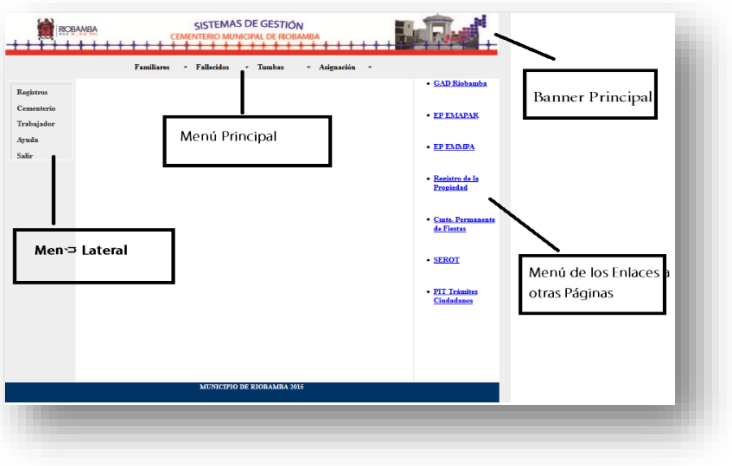


Figura 92. Partes del Sistema de Gestión del CMR

Adaptado por: Marco Gavidia & Jessica Valle

BANNER PRINCIPAL

Banner Principal: El banner del Sistema CMR se realizado una animación en flash con fotos tomadas del lugar.

AREA DEL MENU

El menú principal muestra los módulos de registro (todo información relacionada con las personas fallecidas), cementerio (todo lo relacionado con el cementerio), y el módulo de login en este caso para salir del sistema.

INGRESO AL SITIO WEB INFORMATIVO & SGCMR

INGRESO AL SISTEMA CMR

Para ingresar al Sistema de Gestión del Cementerio Municipal de Riobamba se debe ingresar a la siguiente dirección.

http://localhost/aplicacioncp/index.php

Figura 93. Ingreso al Sistema de Gestión del Cementerio Municipal de Riobamba

Adaptado por: Marco Gavidia & Jessica Valle

Después se puede observar la interfaz de Autenticación del SGCMR

Figura 94. Interfaz de Login del SGCMR

Adaptado: Marco Gavidia & Jessica Valle

INGRESO AL SITIO WEB CMR

Para ingresar a la página del Cementerio Municipal de Riobamba se debe ingresar a la siguiente dirección.

http://www.cementerioderiobamba.com

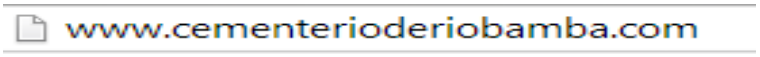


Figura 95. Ingreso a la página del IP

Adaptado: Marco Gavidia & Jessica Valle

Después se puede observar la página principal del Cementerio

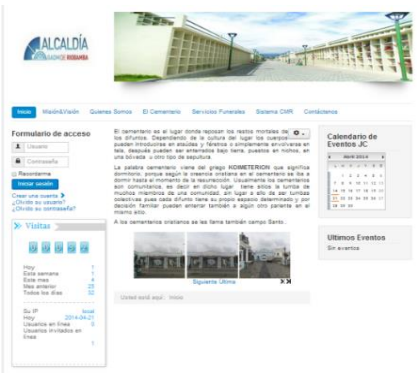


Figura 96. Página principal

Adaptado por: Marco Gavidia & Jessica Valle

INGRESO COMO ADMINISTRADOR.

Ingreso a la dirección web:

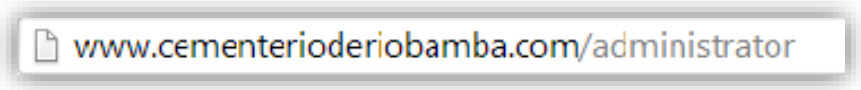


Figura 97. Ingreso como Administrador

Adaptado por: Marco Gavidia & Jessica Valle

Se debe ingresar los datos siguientes:

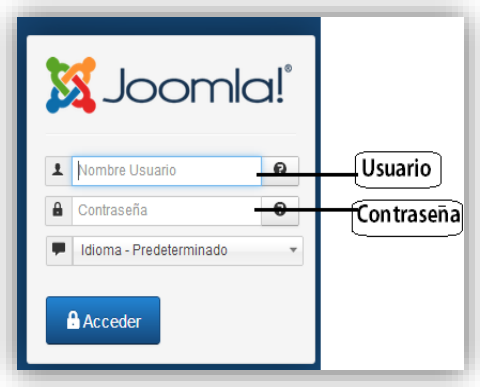


Figura 98. Ingreso de Datos

Adaptado por: Marco Gavidia & Jessica Valle

Página del administrador

http://www.cementerioderiobamba.com/administrator/index.php

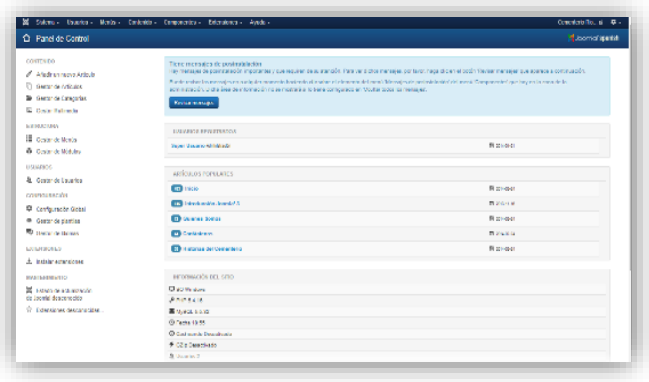


Figura 99. Página del Administrador

Adaptado por: Marco Gavidia & Jessica Valle

SECCION DE ENLACES A SITIOS EXTERNOS

En esta parte de la interfaz se podrá acceder a sitios web relacionados con el GAD Riobamba

FUNCIONES PRINCIPALES DEL SITIO WEB Y SGCMR

FUNCIONES PRINCIPALES DEL SISTEMA DE GESTION CMR

El sistema está desarrollado para trabajar intranet de manera independiente del portal web con solo digital en el navegador la siguiente dirección http://localhost/aplicacioncp/

MODULO DE AUTENTICACIÓN

La siguiente interfaz permite ingresar al Sistema CMR. La interfaz consta de un usuario y contraseña como se muestra a continuación**.**

Figura 100. Interfaz de autenticación del Sistema CMR

Adaptado: Marco Gavidia & Jessica Valle

MODULO DE CEMENTERIO

REGISTRO DE CEMENTERIO

El registro de Cementerio se realiza de la siguiente manera:

Debe hacer clic en el menu superior en Cementerio, luego se desplegara un submenú donde podrá ingresar y actualizar.

Además realizará las siguientes operaciones: buscar, eliminar y listar

Los campos a llenar serán: Nombre, Dirección, Teléfono

Figura 101. Registro del Cementerio

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE SECTOR

El registro de Sector se realiza de la siguiente manera:

Debe hacer clic en el menu superior de Sector, luego se desplegara un submenú donde podrá ingresar y actualizar.

Además realizará las siguientes operaciones: eliminar y listar

El campo que deberá llenar es el Nombre y seleccionar el nombre del Cementerio.

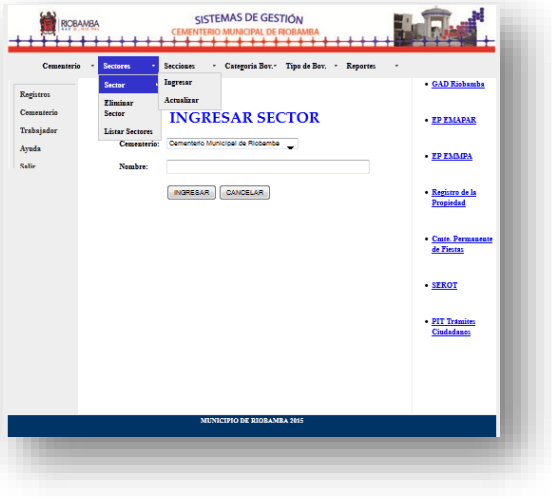


Figura 102. Registro de Sector

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE SECCIÓN

El registro de Sección se realiza de la siguiente manera:

Debe hacer clic en el menu superior de Sección, luego se desplegara un submenú donde podrá ingresar y actualizar.

Además realizará las siguientes operaciones: eliminar y listar

El campo que deberá llenar es el Nombre y seleccionar un Sector.

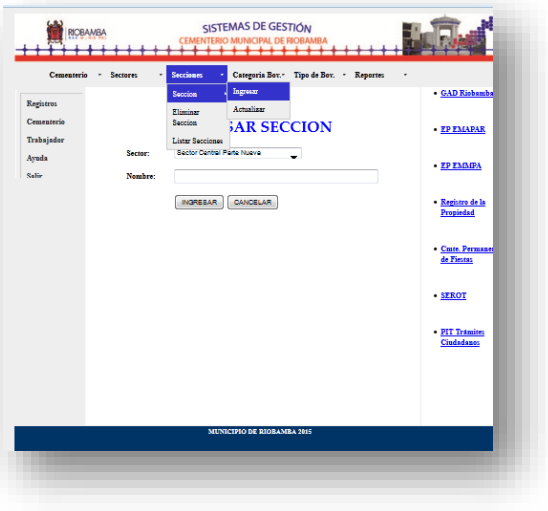


Figura 103. Registro de Sección

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ DE CATEGORÍA DE BOVEDAS

El registro de tipo de Bóvedas se realiza de la siguiente manera:

Debe hacer clic en el menú superior de tipo de Bóvedas, luego se desplegara un submenú donde podrá escoger ingresar, eliminar, listar y actualizar.

El campo que deberá llenar será: Nombre de Categoría.

Figura 104. Registro de Categoría de Bóvedas

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ DE TIPO DE BOVEDAS

El registro de tipo de Bóvedas se realiza de la siguiente manera:

Debe hacer clic en el menú superior de tipo de Bóvedas, luego se desplegara un submenú donde podrá escoger entre nichos, sepultura y mausoleo. Además eligirá se desea ingresar, eliminar, listar y actualizar.

El campo que deberá seleccionar será: Sección y el número de nicho, sepultura o mausoleo.

Figura 105. Registro de Tipo de Bóvedas

Adaptado: Marco Gavidia & Jessica Valle

REPORTES

El registro de reportes se realiza de la siguiente manera:

Debe hacer clic en el menú superior de reportes, luego se desplegara un submenú donde podrá escoger entre nichos, sepultura y mausoleo. Además eligirá se desea ingresar, eliminar, listar y actualizar.

Los campos que deberán seleccionar serán: Cementerio, Sector y Sección para poder tener una tabla detallada de lo que necesite.

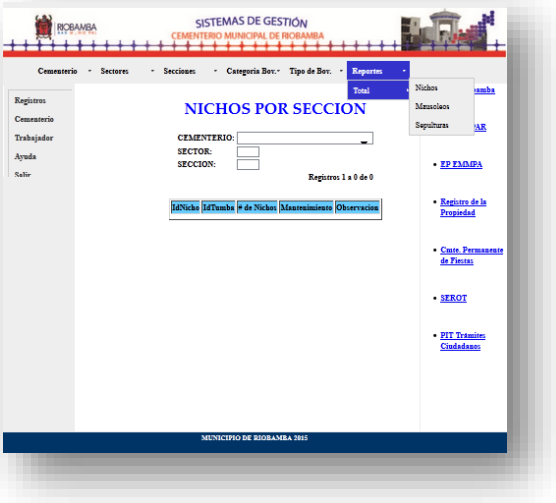


Figura 106. Registro de Reportes

Adaptado: Marco Gavidia & Jessica Valle

MODULO DE TRABAJADOR

REGISTRO DE TRABAJADORES

El registro de Trabajadores se realiza de la siguiente manera:

Debe hacer clic en el menú superior de trabajador, luego se desplegara un submenú donde podrá ingresar, eliminar, listar y actualizar.

Los campos a llenar serán: Nombre, Apellido, Salario, Categoría. Además seleccionar el Nombre del Cementerio y el Cargo que tiene el trabajador.

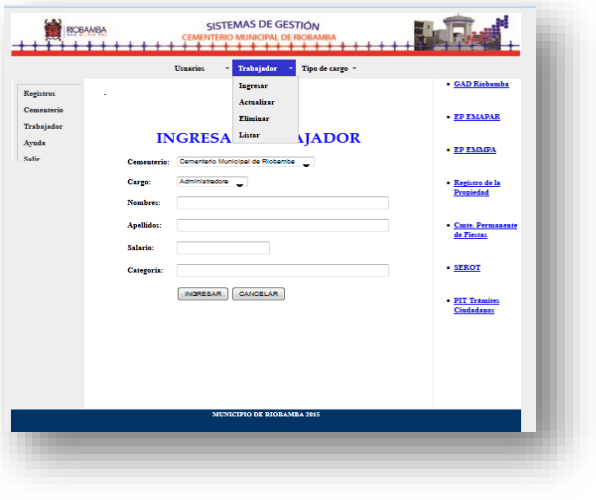


Figura 107. Registro deTrabajadores

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ DE TIPO DE CARGOS

El registro de Tipos de Cargos se realiza de la siguiente manera:

Debe hacer clic en el menu superior de tipo de cargos, luego se desplegara un submenú donde podrá ingresar, eliminar, listar y actualizar.

El campo que debe llenar será: El Cargo que tiene el trabajador.

Figura 108. Registro deTipo de Cargos

Adaptado: Marco Gavidia & Jessica Valle

REGISTRÓ DE USUARIOS

El registro de Usuarios se realiza de la siguiente manera:

Debe hacer clic en el menú superior de usuario, luego se desplegara un submenú donde podrá ingresar, listar y actualizar.

Los campos que deben llenar serán: Nombre, Apellido, Dirección, Teléfono y el Login. Además seleccionar el tipo de usuario si es Administrador o Usuario.

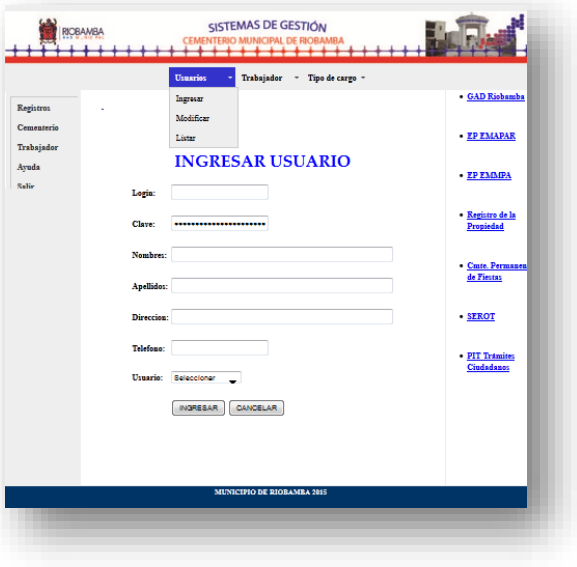


Figura 109. Registro de Usuarios

Adaptado: Marco Gavidia & Jessica Valle

MODULO DE REGISTRO

REGISTRO DE FAMILIARES

El registro de Familiares se realiza de la siguiente manera:

Debe hacer clic en el menu superior de Familiar, luego se desplegara un submenú donde podrá ingresar y actualizar.

Además realizará las siguientes operaciones: buscar, eliminar y listar

Los campos a llenar serán: Cédula, Nombre, Dirección, Teléfono y el Correo.

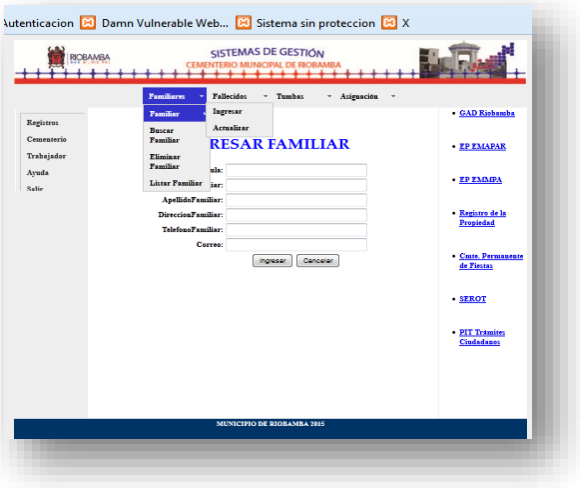


Figura 110. Registro de Familiares

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE FALLECIDOS

El registro de Fallecidos se realiza de la siguiente manera:

Debe hacer clic en el menu superior de Fallecidos, luego se desplegara un submenú donde podrá ingresar y actualizar.

Además realizará las siguientes operaciones: buscar, eliminar y listar

Los campos a llenar serán: Nombre, Apellido y la Fecha de Fallecido.

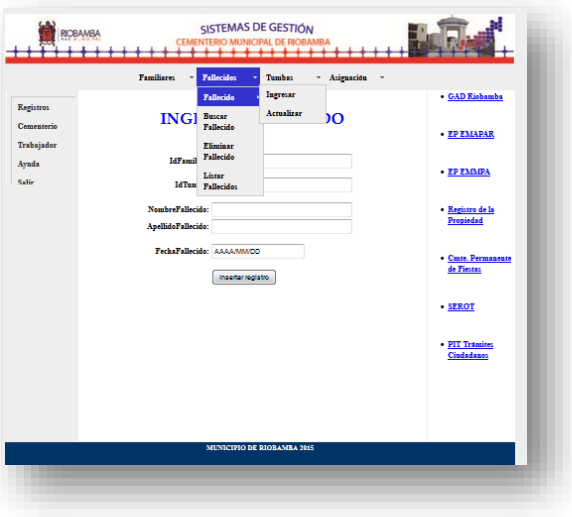


Figura 111. Registro de Fallecido

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE TUMBAS

El registro de Tumbas se realiza de la siguiente manera:

Debe hacer clic en el menu superior de Tumbas, luego se desplegara un submenú donde podrá ingresar y actualizar.

Además realizará las siguientes operaciones: buscar, eliminar y listar

Los campos a llenar serán: Nombre, Apellido y la Fecha de Fallecido.

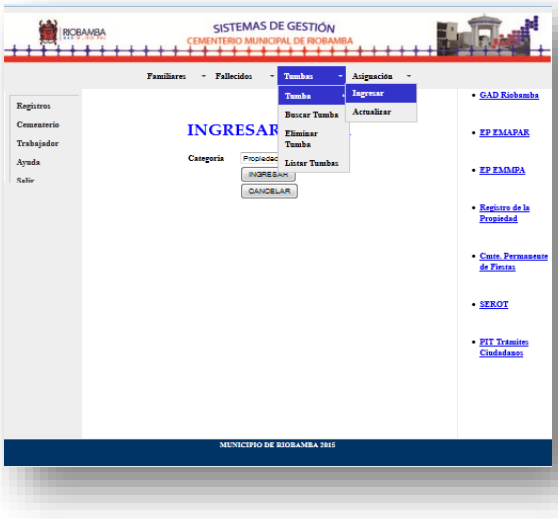


Figura 112. Registro de Tumbas

Adaptado: Marco Gavidia & Jessica Valle

REGISTRO DE ASIGNACIÓN

El registro de Asignación se realiza de la siguiente manera:

Debe hacer clic en el menu superior de Asignación, luego se desplegara un submenú donde podrá elegir nicho, sepultura y mausoleo.

Los campos que deben seleccionar serán: Cementerio, Sector y Sección con el fin de tener una tabla detallada de los datos requeridos.

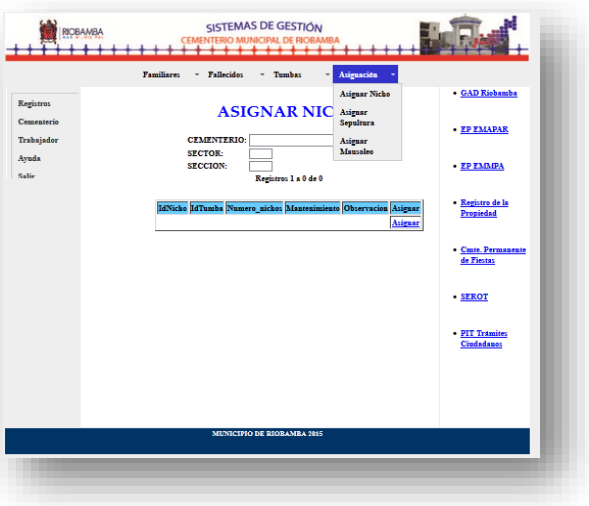


Figura 113. Registro de Asignación

Adaptado: Marco Gavidia & Jessica Valle

FUNCIONES PRINCIPALES DEL WEB SITE

AÑADIR UN NUEVO ARTÍCULO

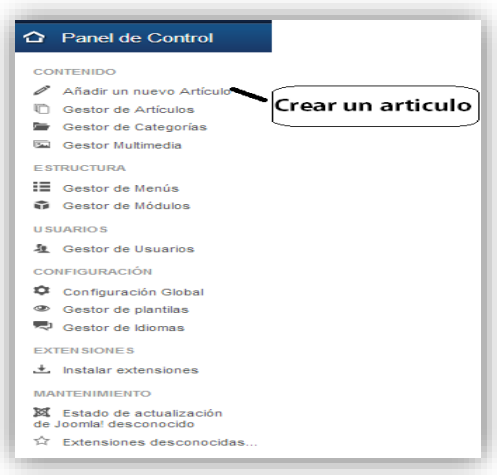


Figura 114. Añadir un nuevo Artículo

Adaptado: Marco Gavidia & Jessica Valle

Dar clic en Añadir un nuevo artículo

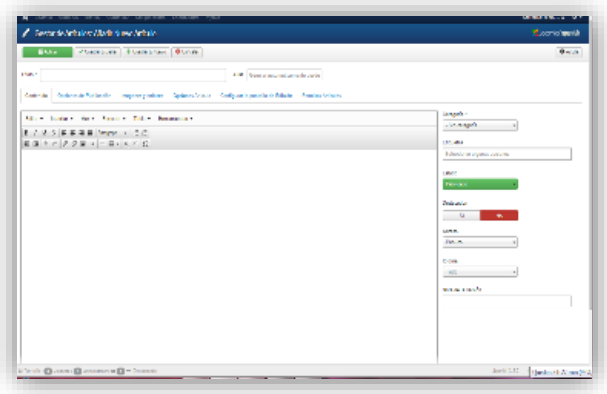


Figura 115. Ingresar los datos a un Artículo

Adaptado: Marco Gavidia & Jessica Valle

Se debe llenar correctamente los ítems que se observa en la figura anterior:

Título: El título que desea que tenga el artículo.

Categoría: Escoger la categoría que se crea para asignarle a este artículo

Estado: Si el artículo es publicado o despublicado en la dependerá de la necesidad del administrador.

Acceso: Quiere decir si el articulo va a ser visualizado por todo el público o clientes específicos.

Permisos: Le da al Cliente o a los usuarios los diferentes niveles de acceso o los permisos respectivos para la modificación de la información del Cementerio Municipal de Riobamba

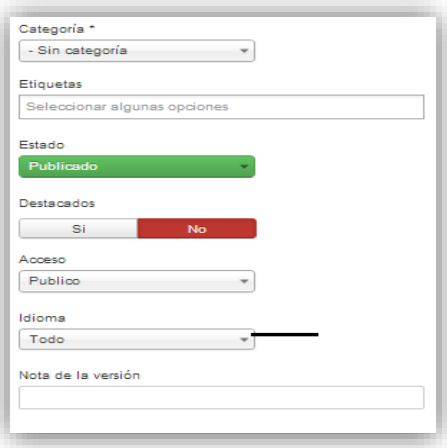


Figura 116. Pantalla de los Datos

Adaptado: Marco Gavidia & Jessica Valle

Características: Le da la opción de elegir si será o no con una característica específica.

Idioma: Elige el idioma a utilizar.

Texto Artículo.

Añadimos atreves la escritura normal y por medio de código HTML.

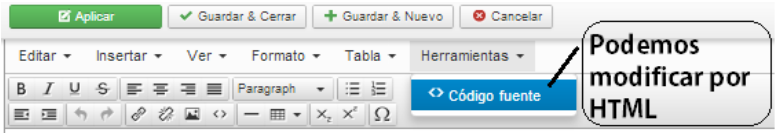


Figura 117. Ingreso de Texto al Artículo

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE ARTÍCULOS

Visualizar los artículos creados o los artículos existentes en el momento de ver el Sitio Web Informativo del Cementerio Municipal de Riobamba.

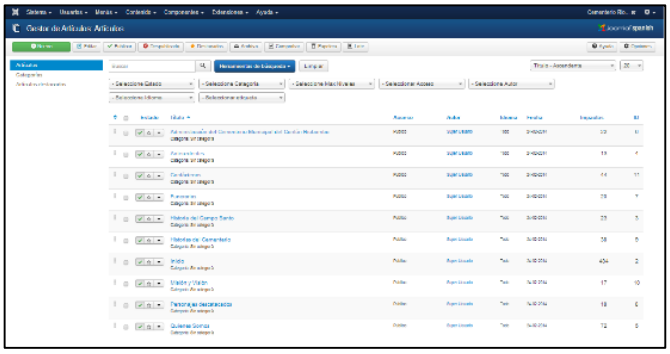


Figura 118. Gestor de Artículos

Adaptado: Marco Gavidia & Jessica Valle

Aquí se tiene las distintas opciones que podrán escoger en el gestor de artículos.

Figura 119. Opciones de los Gestores de Artículo

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE CATEGORÍAS

Crear y observar las categorías que contenga cada artículo, en este caso se muestra la posición del menú.

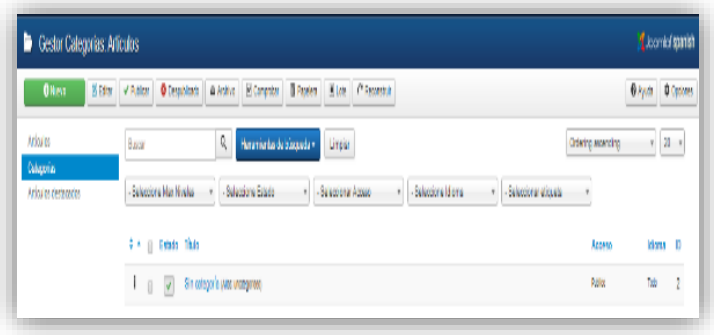


Figura 120. Gestor de Categorías

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE MULTIMEDIA

Figura 121. Gestor Multimedia

Adaptado: Marco Gavidia & Jessica Valle

Se puede agregar o eliminar las imágenes, los gráficos que desea que contenga la página web del Cementerio Municipal de Riobamba.

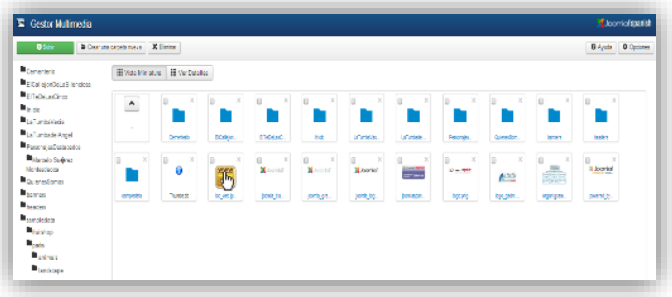


Figura 122. Gestor de Carpetas

Adaptado: Marco Gavidia & Jessica Valle

Se debe hacer clic en los cuadritos para seleccionar la imagen que se desea poner en los artículos.

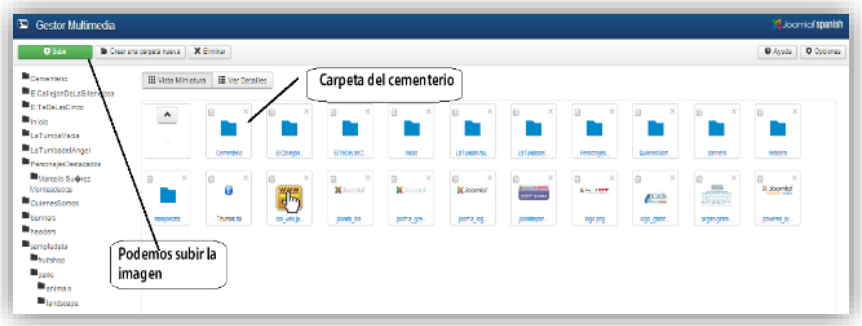


Figura 123. Ver la información de las Carpetas

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE MENÚS

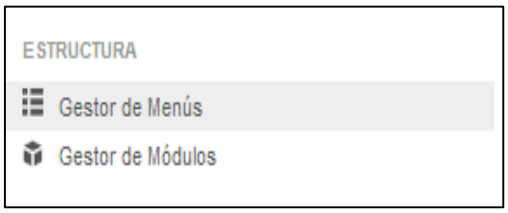


Figura 124. Gestor de Menús

Adaptado: Marco Gavidia & Jessica Valle

Observar los menús que contiene el Sitio Web Informativo del Cementerio Municipal de Riobamba, además se puede crear menús para poder visualizarlo en la página web.

Al hacer clic en Editar:

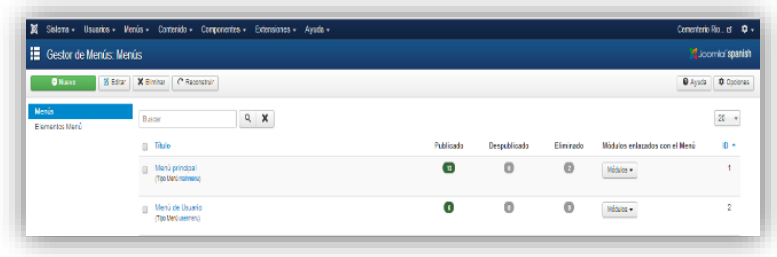


Figura 125. Crear Menús

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE USUARIOS

Figura 126. Gestor de Usuarios

Adaptado: Marco Gavidia & Jessica Valle

Al realizar clic en el Gestor de Usuario aparece la siguiente pantalla.

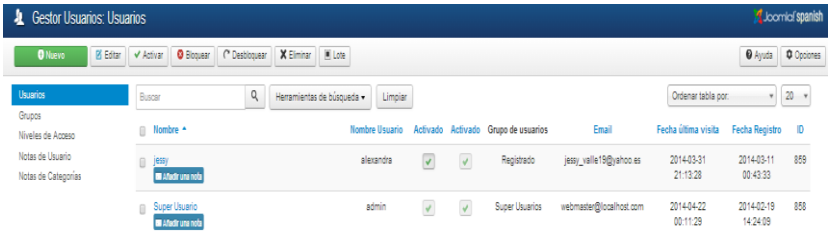


Figura 127. Gestor de Usuarios

Adaptado: Marco Gavidia & Jessica Valle

Observar los usuarios permitidos y no permitidos para el control del Sitio Web Informativo del Cementerio Municipal de Riobamba, dándole los niveles de acceso a los usuario creados por el administrador (Activado, Desactivado, Registrado, Email, Fecha que los visita o entra al sistema web.

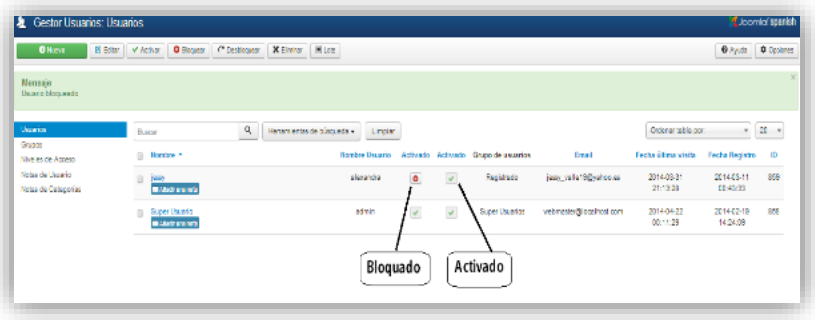


Figura 128. Activar a los Usuarios

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE MÓDULOS

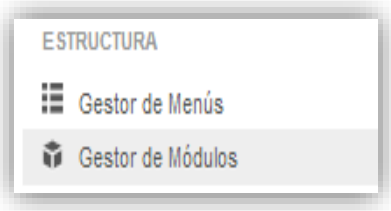


Figura 129. Gestor de Módulos

Adaptado: Marco Gavidia & Jessica Valle

Al realizar clic en Gestor de Módulos, se puede activar o desactivar los módulos que quiere que se visualice en el Sitio Web Informativo.

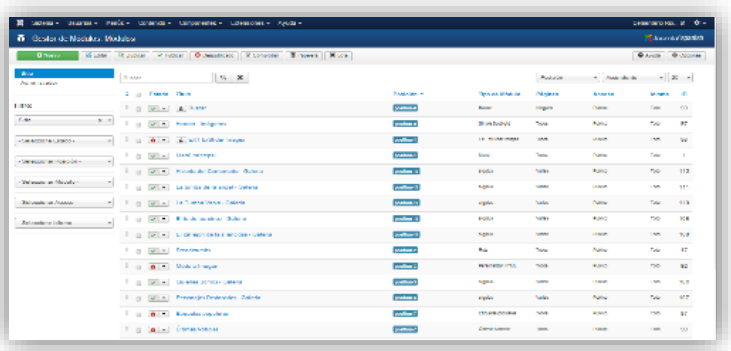


Figura 130. Instalación de Módulos

Adaptado: Marco Gavidia & Jessica Valle

Crear o instalar los módulos necesarios.

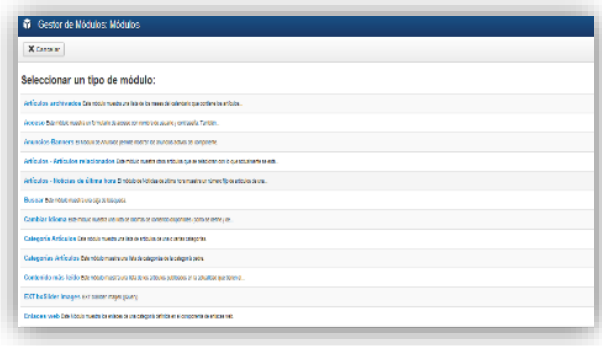


Figura 131. Gestor de Extensiones

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE EXTENSIONES

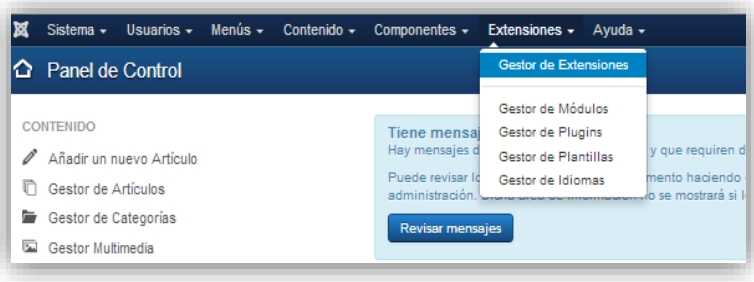


Figura 132. Instalar los Archivos

Adaptado: Marco Gavidia & Jessica Valle

Al realizar clic aparece la siguiente pantalla que nos indica:

El Archivo que desee instalar.

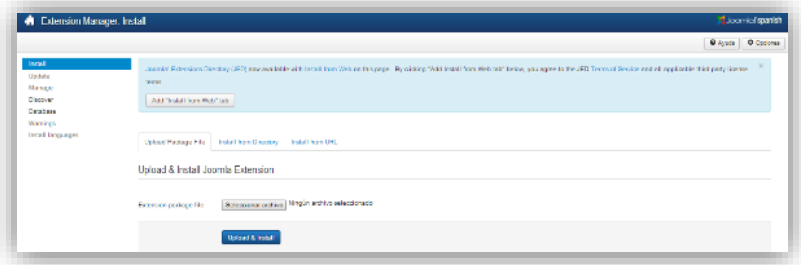


Figura 133. Examinar los Archivos

Adaptado: Marco Gavidia & Jessica Valle

Instalar:

Hacer clic en Examinar.

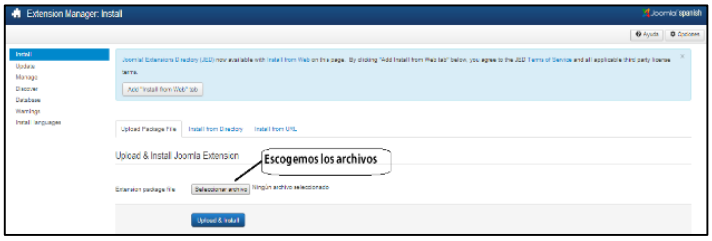


Figura 134. Buscar el Archivo

Adaptado: Marco Gavidia & Jessica Valle

Buscar el lugar donde se encuentra el Archivo para ser instalado**.**

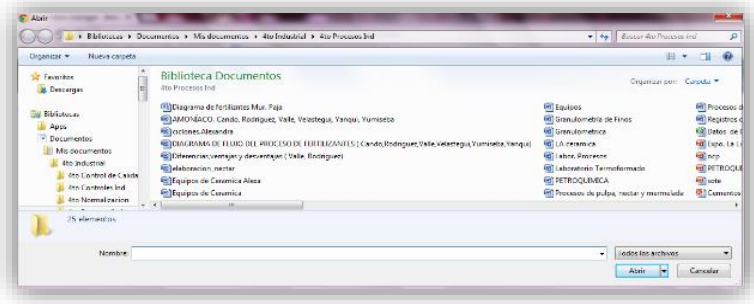


Figura 135. Gestor de Idiomas

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE IDIOMAS

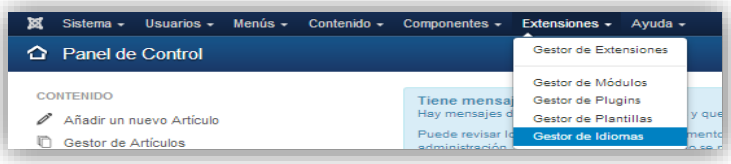


Figura 136. Elegir el Idioma

Adaptado: Marco Gavidia & Jessica Valle

Elegimos el idioma deseado para el Sistema.

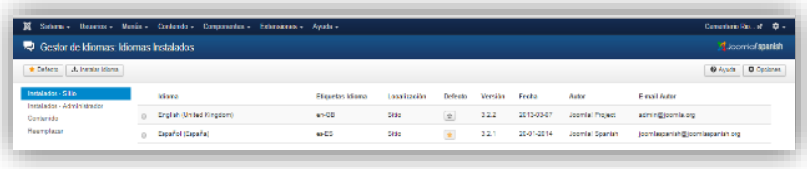


Figura 137. Configuración Global

Adaptado: Marco Gavidia & Jessica Valle

CONFIGURACIÓN GLOBAL

Figura 138. Asignación de Funciones

Adaptado: Marco Gavidia & Jessica Valle

Asignar las diferentes funciones y niveles adecuados para el Sistema

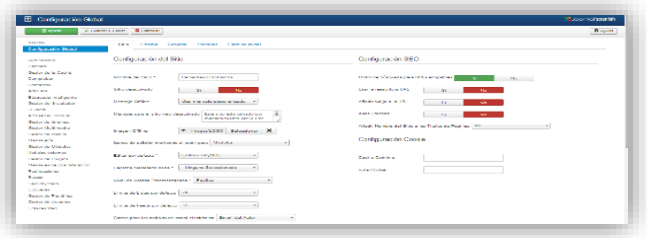


Figura 139. Gestor de Plantillas

Adaptado: Marco Gavidia & Jessica Valle

GESTOR DE PLANTILLAS

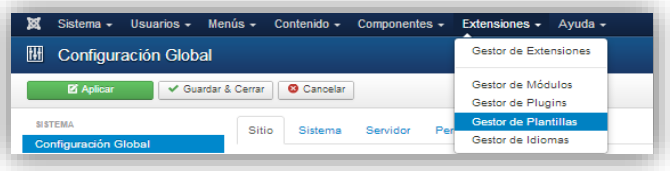


Figura 140. Visualizar las Plantillas

Adaptado: Marco Gavidia & Jessica Valle

Hacer clic en Gestor de Plantillas

Permite visualizar las plantillas que están subidas pero solo una de las plantillas esta elegida como predeterminada que esta con una estrella.

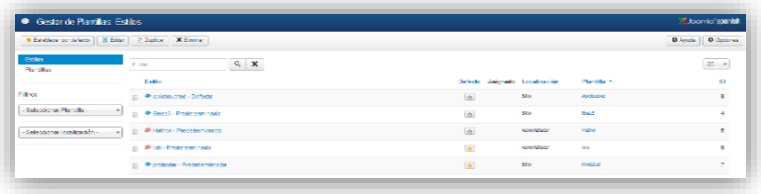


Figura 141. Interfaz Gestor de Plantilla

Adaptado: Marco Gavidia & Jessica Valle

Al hacer clic en Plantillas se observa cómo es la interfaz de cada plantilla predeterminada.

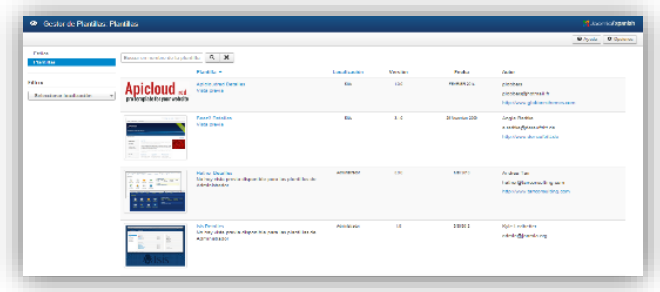


Figura 142. Interfaz del Módulo de Login

Adaptado: Marco Gavidia & Jessica Valle

GLOSARIO DE TERMINOS

A

APACHE: (Acrónimo de "a patchy server"). Servidor web de distribución libre y de código abierto, **APPSERVER: es** una herramienta OpenSource para Windows que facilita la instalación de Apache, MySQL y PHP en la cual estas aplicaciones se configuran en forma automática.

B

BACK-END: El front-end es la parte del software que interactúa con el o los usuarios y el back-end es la parte que procesa la entrada desde el front-end.

BANNER*:* Un ***banner*** (*en español*: banderola) es un formato publicitario en Internet.

C

CACHÉ: es una referencia por rango de inicio y otro de fin1 (/ˈkæʃ/ o /kaʃ/) usada por la unidad central de procesamiento de una computadora.

CHECK BOX: Elemento de interfaz gráfico (widget) que permite al usuario marcar múltiples selecciones de un número de opciones. Generalmente son mostrados en pantalla como cuadraditos que pueden estar vacíos (para falso) o tildados o rellenos (para verdadero). Por lo general al lado de los cuadrados hay un texto que explica el significado de que el casillero esté o no chequeado.

COMBOBOX: (lista desplegable con entrada). Elemento GUI que permite al usuario escribir sobre este o seleccionar una opción de una lista existente de opciones. Un ejemplo de combo box son las barras de direcciones usadas en los navegadores web.

F

FILEZILLA: es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de GNU. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS).

FILTRO: Un programa para acceder a una corriente de datos:

FORMULARIO: Se llama formulario a una página con espacios vacíos que han de ser rellenados con alguna finalidad, por ejemplo una solicitud de empleo en la que has de rellenar espacios libres con la información personal requerida.

FRONT-END: Es la parte del software que interactúa con el o los usuarios

FTP: (siglas en inglés de ***F****ile* ***T****ransfer* ***P****rotocol*, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

H

HOSTING: El alojamiento web (en inglés *web hosting*) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

L

LOGIN: (en español **ingresar** o **entrar**) es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario al momento de utilizar credenciales provistas por el usuario.

M

MÓDULO: Un **módulo de** Joomla es un mecanismo para usar bibliotecas de código externas a un sitio creado en Joomla.

P

PHP: es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas

PORTAL WEB: Un portal de Internet es un sitio web cuya característica fundamental es la de servir de *Puerta de entrada* (única) para ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema.

PLUG-IN: Un complemento es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API. También se lo conoce como **plug-in** (del inglés "enchufable"), **add-on** (agregado), complemento, conector o extensión.

S

SMTP: Simple Mail Transfer Protocol (**SMTP** Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.).

SQL: El lenguaje de consulta estructurado o SQL (por sus siglas en inglés *structured query language*) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en estas.

SUBFORMULARIO: Un formulario que se encuentra ubicado dentro de un formulario más grande.

U

UTF-8 (8-bit *Unicode Transformation Format*) es un formato de codificación de caracteres Unicode e ISO 10646 utilizar símbolos de longitud variable.

W

WAMP: es el acrónimo usado para describir un sistema de infraestructura de internet que usa las siguientes herramientas: Windows, como sistema operativo, Apache, como servidor web, MySQL, como gestor de bases de datos, PHP (generalmente), Perl, o Python, como lenguajes de programación.

X

XAMPP: es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl. El nombre proviene del acrónimo de **X** (para cualquiera de los diferentes sistemas operativos), Apache, MySQL, PHP, Perl.