ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"COMPARATIVO DE LAS PRINCIPALES TECNOLOGÍAS ORIENTADAS AL DESARROLLO DE APLICACIONES WEB DINÁMICAS SEGURAS"

ELVIS MARTIN FONSECA CHANGOLUISA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de Magíster en

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

Mayo – 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **COMPARATIVO DE LAS PRINCIPALES TECNOLOGÍAS ORIENTADAS AL DESARROLLO DE APLICACIONES WEB DINÁMICAS SEGURAS,** de responsabilidad del Ing. Elvis Martin Fonseca Changoluisa, ha sido minuciosamente revisado por los miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

Tribunal:

LUIS EDUARDO HIDALGO ALMEIDA

Firmado digitalmente por LUIS EDUARDO HIDALGO ALMEIDA
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=LUIS EDUARDO HIDALGO ALMEIDA
Fecha: 2021.05.26 01:02:27 -05'00'

ING. LUIS EDUARDO HIDALGO ALMEIDA PhD.
PRESIDENTE

RAUL HUMBERTO CUZCO NARANJO

Firmado digitalmente por RAUL HUMBERTO CUZCO NARANJO
Fecha: 2021.05.26 10:50:08 -05'00'

ING. RAUL HUMBERTO CUZCO NARANJO,Mag.
DIRECTOR

Firmado electrónicamente por:
SAUL YASACA PUCUNA

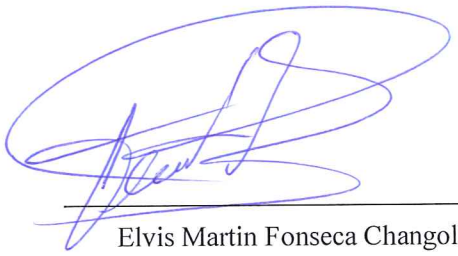
ING. SAÚL YASACA PUCUNA. Mag.
MIEMBRO

ING. BRAULIO ADRIAN CAISAGUANO VILLA. Mag
MIEMBRO

Mayo 2021

DERECHOS INTELECTUALES

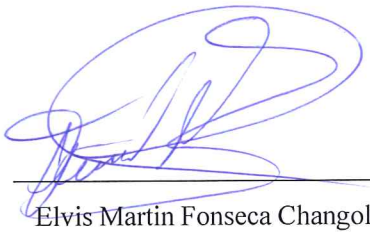
Yo, Elvis Martin Fonseca Changoluisa, con cédula de identidad 020190108-9, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.



Elvis Martin Fonseca Changoluisa
Nº de cédula 020190108-9

DECLARACIÓN DE AUTENTICIDAD

Yo, Elvis Martin Fonseca Changoluisa, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados. Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.



Elvis Martin Fonseca Changoluisa
Nº de cédula 020190108-9

DEDICATORIA

El presente trabajo lo dedico a Dios en primer lugar por ser dador de vida e inspiración, es quien nos permite despertar cada mañana y alcanzar nuestros sueños y a mi familia por estar siempre a mi lado brindándome apoyo incondicional, gracias a ustedes he logrado y alcanzado todas las metas que me he propuesto cada día.

Elvis Martin Fonseca Changoluisa.

AGRADECIMIENTO

Quiero agradecer a Dios por ser mi fuente de luz, a mis padres por ser el motor de mi vida, a la Institución por abrirme sus puertas para seguir con mi preparación académica y a mis maestros quienes me impulsaron a seguir preparándome y se convirtieron en mis guías para dirigir mi camino profesional, a mis amigos con quienes he compartido los mejores momentos en mi vida y a todos quienes aportaron con su granito de arena para cumplir esta meta.

Elvis Martin Fonseca Changoluisa.

TABLA DE CONTENIDO

RESUMEN xiii

ABSTRACT xiv

CAPIÍULO I 1

1 INTRODUCCIÓN 1

1.1 Planteamiento del problema 1

1.1.1 Situación problemática 1

1.2 Formulación del problema 2

1.3 Justificación de la investigación 2

1.3.1 Justificación teórica 2

1.4 Objetivos 3

1.4.1 Objetivo General 3

1.4.2 Objetivos Específicos 3

1.5 Hipótesis 3

1.6 IDENTIFICACIÓN DE VARIABLES 3

CAPÍTULO II 4

2 MARCO TEÓRICO 4

2.1 Antecedentes del problema 4

2.2 Bases Teóricas 5

2.2.1 Desarrollo de aplicaciones web dinámicas seguras 5

2.2.2 Tecnología Java (JSP) 6

2.2.3 Tecnología PHP 8

2.2.4 Tecnología ASP.net 11

2.2.5 Lenguajes de servidor 13

2.2.6 Seguridad en las comunicaciones 14

2.2.7 Seguridades a nivel de aplicaciones web 16

2.2.8 Seguridades en inicio de sesión 18

2.2.9 Seguridades con Java Script 19

2.2.10 Funciones de seguridad definidas por el usuario 21

2.2.11 Comparativo de tecnologías PHP, ASP.net y Java (JSP) 25

CAPÍTULO III 30

3 METODOLOGÍA DE INVESTIGACIÓN 30

3.1. Tipo y Diseño de la Investigación 30

3.1.1. Tipo de Investigación 30

3.1.2. Diseño de la Investigación 30

3.2. Métodos y Técnicas De Investigación *31*
3.2.1. Métodos 31
3.2.2. Técnicas 32
3.3. Instrumentos *32*
3.4. Planteamiento de la Hipótesis *33*
3.4.1. Hipótesis General 33
3.4.2. Identificación de variables 33
3.4.3. Operacionalización Conceptual de Variables 33
3.4.4. Operacionalización Metodológica de Variables 34
3.5. Población y Muestra *36*
3.5.1. Población y muestra 36
3.5.2. Plan de recolección de información. 36
3.5.3. Plan de procesamiento de información 37
3.5.4. Análisis e interpretación de resultados 38
CAPÍTULO IV 39
4. RESULTADOS 39
4.1. Plan de recolección de información *39*
4.2. Análisis e interpretación de resultados *40*
4.2.1. Encuesta dirigida a desarrolladores de software referente a la técnologia JAVA (JSP) 40
4.3. Verificación de la hipótesis *48*
4.3.1. Hipótesis 49
4.4. Identificación de variables *50*
CONCLUSIONES 56
RECOMENDACIONES 57
BIBLIOGRAFÍA

ÍNDICE DE FIGURAS

Figura 1-2 JSP modelo1 7
Figura 2-2 JSP modelo2 7
Figura 3-2 Arquitectura PHP.....9
Figura 4-2 Seguridades en las comunicaciones 14
Figura 5-2 Protocolo SSL.....14
Figura 6-2 Protocolo SSL.....15
Figura 7-2 Sesión SSL 16
Figura 8-2 Sesiones.....17
Figura 1-4 Categorías con niveles de clasificación.....51

ÍNDICE DE GRÁFICOS

Gráfico 1-4 Pregunta N° 1. Encuesta.....41
Gráfico 2-4 Pregunta N° 2. Encuesta.....41
Gráfico 3-4 Pregunta N° 3. Encuesta.....42
Gráfico 4-4 Pregunta N° 4. Encuesta.....43
Gráfico 5-4 Pregunta N° 5. Encuesta.....44
Gráfico 6-4 Pregunta N° 6. Encuesta.....45
Gráfico 7-4 Pregunta N° 7. Encuesta.....46
Gráfico 8-4 Pregunta N° 8. Encuesta.....46
Gráfico 9-4 Pregunta N° 9. Encuesta.....47
Gráfico 10-4 Pregunta N° 10. Encuesta.....48

ÍNDICE DE TABLAS

Tabla 1-2 Portabilidad en los servidores, según los sistemas operativos 25
Tabla 2-2 Arquitectura de software y hardware 26
Tabla 3-2 Grado de detección de fallas 26
Tabla 4-2 Grado de detección de fallas 26
Tabla 5-2 Calidad de fallas detectadas 27
Tabla 6-2 Integridad de la base de datos 27
Tabla 7-2 Complejidad en la programación 28
Tabla 8-2 Promedios de Tiempos de respuesta.....29
Tabla 1-3 Operacionalización Conceptual de Variables 33
Tabla 2-3 Operacionalización Metodológica de Variables 34
Tabla 3-3 Población y muestra 36
Tabla 4-3 Matriz de recolección de información 37
Tabla 1-4 Matriz de recolección de información 39
Tabla 2-4 Pregunta N° 1. Encuesta.....40
Tabla 3-4 Pregunta N° 2. Encuesta.....41
Tabla 4-4 Pregunta N° 3. Encuesta.....42
Tabla 5-4 Pregunta N° 4. Encuesta.....43
Tabla 6-4 Pregunta N° 5. Encuesta.....44
Tabla 7-4 Pregunta N° 6. Encuesta.....45
Tabla 8-4 Pregunta N° 7. Encuesta.....45
Tabla 9-4 Pregunta N° 8. Encuesta.....46
Tabla 10-4 Pregunta N° 9. Encuesta.....47
Tabla 11-4 Pregunta N° 10. Encuesta.....48
Tabla 12-4 Tabla de contingencia con las preguntas más alineadas a la investigación del cuestionario propuesto.....50
Tabla 13-4 Cálculo de Frecuencia Esperada.....51
Tabla 14-4 Calculo de frecuencias Esperadas con respuesta negativa 52
Tabla 15-4 Cálculo de Chi Cuadrado calculado 53

RESUMEN

Se realizó un estudio cuyo objetivo fue comparar las principales tecnologías orientadas al desarrollo de aplicaciones web dinámicas seguras, se aplicó una encuesta a 30 profesionales de la escuela de Ingeniería en Sistemas de la ESPOCH. Los resultados fueron un 57% de encuestados afirmaron que implementar estrategias debidamente estructuradas, para evitar accesos accidentales y deliberados a la gestión de los usuarios del sistema es indispensable. El 83 % acepto que la funcionalidad que JAVA ofrece ayuda sustancialmente a proteger la confidencialidad en los sistemas web. Para el 73% de los encuestados el modelo de programación orientado a objetos que ofrece JAVA ayuda a reducir los riesgos de vulnerabilidades por su característica potente y única. El 70 % de los encuestados aseguro que se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda OWASP. El 73%, afirmo que JAVA presta las facilidades para desarrollar nuevos módulos e incorporarlos a una aplicación ya desarrollada. Por lo tanto, JSP es la tecnología que cumple con un 93% con los parámetros propuestos por (OWASP) por encima de las tecnologías ASP.Net con un 50% y PHP 86%, es por ello por lo que la presente investigación puede ser útil para ser implementada en cualquier medio organizacional, en Instituciones de Educación Superior en procesos relacionados con servicios de Posgrado.

Palabras Clave: <SEGURIDAD INFORMÁTICA>, <TECNOLOGÍAS >, < APLICACIONES WEB>, <DINÁMICAS SEGURAS>, <JAVA >.

ABSTRACT

A study was carried out whose objective was to compare the main technologies oriented to the development of secure dynamic web applications, a survey was applied to 30 professionals from the ESPOCH School of Systems Engineering. The results were 57% of respondents affirmed that implementing properly structured strategies to avoid accidental and deliberate access to the management of system users is essential 83% accept that the functionality that JAVA offers substantially helps to protect confidentiality in web systems. For 73% of the respondents, the object-oriented programming model that JAVA offers helps to reduce the risks of vulnerabilities due to its powerful and unique feature. 70% of those surveyed said that completely secure web applications can be obtained if all the techniques and security standards recommended by OWASP are applied. 73% affirm that JAVA provides the facilities to develop new modules and incorporate them into an already developed application. Therefore, JSP is the technology that complies with 93% with the parameters proposed by (OWASP) over the ASP.Net technologies with 50% and PHP 86%, that is why this research can be Useful to be implemented in any organizational environment, in Higher Education Institutions in processes related to Postgraduate services.

Keywords: <COMPUTER SECURITY>, <TECHNOLOGIES>, <WEB APPLICATIONS>, <SAFE DYNAMICS>, <JAVA>.

CAPÍTULO I

1 INTRODUCCIÓN

La presente investigación se basa en el estudio de las principales tecnologías que existen para el desarrollo de aplicaciones web dinámicas, es decir aquí se analiza también como estas tecnologías se relacionan con los motores de bases de datos. En el desarrollo de aplicaciones uno de los objetivos principales es cumplir con los más altos estándares de rendimiento y seguridad, por estas razones se debe identificar los métodos, requerimientos y técnicas de seguridad de cada una de las tecnologías, con la finalidad de reducir la vulnerabilidad en estos entornos. Una de las industrias más evolutivas a nivel mundial es la de desarrollo de software incorporando nuevas herramientas, metodologías, lenguajes de programación y lo más importante nuevas seguridades al momento del desarrollo. Pero en sí que es lo más importante al momento de escoger una tecnología la respuesta es que cumpla con los principales requerimientos para el diseño, desarrollo e implementación de las aplicaciones web. Aquí algunas de las principales características: productividad, seguridad, mantenimiento, integridad, facilidad de escalabilidad.

1.1 Planteamiento del problema

1.1.1 Situación problemática

A medida que la tecnología avanza y se expande los IDES de desarrollo, los frameworks, las herramientas y las librerías se vuelven obsoletas con bastante rapidez, claro está que no en todos los lenguajes pasa esto existen plataformas que tardan mucho tiempo en presentar nuevas cosas importantes. Sin embargo, las versiones más populares se actualizan entre una y cuatro veces al mes resultando un gran problema para los desarrolladores el de estar actualizando el código de las aplicaciones a cada momento.

La utilización de una u otra tecnología sin realizar un análisis previo nos puede llevar a enfrentarnos a problemas de integración de código, que es algo común en las empresas de desarrollo, tecnologías que no dispongan de herramientas que necesites utilizar para conseguir un objetivo y el problema que se arma después de haber programado 1 mes, volver a programar desde cero son cuestiones que se debe analizar antes de decidirse por una tecnología de programación.

Otro problema muy común que se presenta en el desarrollo de aplicadores web es el de escoger una tecnología que no brinda los requerimientos de los usuarios o a su vez escoger una plataforma

sugerida por los usuarios sin ser estas las mejores alternativas. Pero más allá de todos los problemas antes mencionados se presenta el principal, del cual es objeto esta investigación y es la seguridad de la información que pueda brindar la plataforma escogida, en cualquier empresa sería los datos son el recurso más preciado y valioso y varias personas están dispuestas a pagar mucho por ello, incluyendo a los competidores de tu cliente. La seguridad de la información no es solo cuestión de los sistemas, los programadores tienen un papel incluso mucho más importante y la mayor parte de los problemas de seguridad que surgen en las aplicaciones tienen más que ver con el código utilizado para el desarrollo que con las comunicaciones. Los hackers buscan constantemente estas vulnerabilidades y las formas de penetrar en el código de las aplicaciones.

1.2 Formulación del problema

¿El estudio comparativo de las principales tecnologías dedicadas al desarrollo de aplicaciones web dinámicas permitirá escoger la que brinde los mejores mecanismos y herramientas de seguridad a la información?

1.3 Justificación de la investigación

1.3.1 Justificación teórica

Las nuevas tecnologías y el crecimiento vertiginoso del desarrollo de aplicaciones web han puesto en constante cambio la forma de gestionar la información en las instituciones, por lo cual han surgido numerosas formas de implementar soluciones informáticas de gran nivel y seguridad. Cada vez va tomando más fuerza mejorar las prestaciones de una arquitectura de sistemas web, la utilización de una arquitectura segura para implementar una solución web permitirá asegurar la calidad de los servicios a la que esté orientada, presentando una serie de ventajas y parámetros que deben cumplirse para mostrarse como eficaz y eficiente cuando entren en su fase de producción.

Es por eso por lo que; las aplicaciones web se han convertido en pocos años en complejos sistemas con interfaces de usuario cada vez más parecidas a las aplicaciones de escritorio, dando servicio a procesos de negocio de considerable envergadura y estableciéndose sobre ellas requisitos estrictos de accesibilidad y respuesta. Esto ha exigido reflexiones sobre la mejor arquitectura y las técnicas de diseño más adecuadas.

Cohabitamos en una sociedad tecnológica, donde prácticamente la inmensa totalidad de la población a nivel mundial está conectada a Internet y la utiliza a diario como herramienta de

trabajo o consulta. Pero que tiene que ver esto con las tecnologías de desarrollo web, todo ya que para poder comunicarnos en el internet necesitamos de aplicativos que brinden estos servicios, he ahí la importancia de conocer cuál es el lenguaje de programación que cuente con las mejores características de seguridad, rapidez, escalabilidad, soporte a la hora de desarrollar un sistema web con todas estas características importantes.

1.4 Objetivos

1.4.1 Objetivo General

Comparar las principales tecnologías orientadas al desarrollo de aplicaciones web dinámicas seguras.

1.4.2 Objetivos Específicos

- ✓ Investigar las principales tecnologías dedicadas al desarrollo de aplicaciones web dinámicas seguras.
- ✓ Analizar las principales características de seguridad que poseen cada una de las principales tecnologías de programación.
- ✓ Determinar la tecnología que permita mantener la confidencialidad, disponibilidad e integridad en los sistemas web dinámicos.

1.5 Hipótesis

La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, si incrementará el nivel de confidencialidad en los sistemas informáticos.

1.6 IDENTIFICACIÓN DE VARIABLES

Variable Independiente: Aplicación de la tecnología java (JSP).

Variable Dependiente: Incrementará el nivel de confidencialidad en los sistemas informáticos.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes del problema

La competitividad de la tecnología incrementa las opciones para el desarrollo de aplicaciones web a grandes pasos, el comportamiento que estas tengan radica en el análisis para su desarrollo, en las técnicas aplicadas para filtrar y recuperar información correctamente. Los grandes logros que se puedan llegar a obtener de un entorno web son gracias a la buena interactividad de sus componentes, los cuales garantizan: seguridad, confiabilidad, autenticidad, disponibilidad, consistencia de la información.

La seguridad de un entorno web va más allá de los elementos hardware (aunque son imprescindibles), la aplicación alojada en este sitio debe contar con ningún error, la implementación de código seguro tanto del lado del cliente como del servidor servirá para garantizar dicho objetivo, en los que los agujeros de seguridad deben ser nulos para poder administrar los recursos.

Pero como gran parte de la sociedad no está preparada para vivir en internet sin ningún tipo de seguridad y protección, es necesario basarse en 3 aspectos para actuar eficientemente en este mundo tecnológico: concientización (observar que las páginas web sean seguras), formación (conocimientos mayores acerca de los requisitos de seguridad que se deben implantar) y por último el despliegue de aplicaciones seguras, aquí se pone énfasis para trabajar administradores, analistas, desarrolladores y arquitectos informáticos por una óptima solución.

Ante la demanda creciente de productos tecnológicos de gran nivel, surge para el desarrollo de aplicaciones, arquitecturas o patrones que contemplan parámetros a seguir para satisfacer requerimientos en la construcción de soluciones; al momento de optar por una arquitectura se tiene 2 posibilidades: en 2 capas y 3 capas, cada una de ellas útiles para cumplir y superar retos a los nuevos tipos de aplicaciones que han surgido.

La tecnología de los frameworks que se utilice para su desarrollo tiene la obligación de dar soporte también a los nuevos clientes (móviles teléfonos inteligentes, tablets, etc.), sabiendo que el requisito es el mismo para todos clientes y una tarea muy compleja para el servidor. Entonces la existencia de múltiples aplicaciones para un mismo negocio hace que el éxito a alcanzar dependa de cuestiones arquitectoriales y de nuevas interfaces con más soporte.

Se está frente a una necesidad de elegir la mejor herramienta tecnológica que brinde seguridad, componentes para administrar archivos, proveer orden en todo nivel, facilidad para pasar de una

aplicación a otra en un entorno de desarrollo **JAVA (**Se ejecuta en más de 850 millones de ordenadores personales de todo el mundo y en miles de millones de dispositivos, comodispositivos móviles y aparatos de televisión, esto da una idea de su rapidísima expansión. Además, la mayoría de las empresas de software ha adoptado Java como plataforma de desarrollo estratégico, y muchas están ya programando aplicaciones en Java.Por otro lado, JavaSoft, la división de software de Sun dedicada a Java publicará en breve la nueva versión del Java Development Kit, la 1.2, la cual permitirá a los programadores diseñar interfaces de usuario más ricas que las posibles hasta ahora, con mayores capacidades gráficas y de manipulación de objetos multimedia; y que incluirá una nueva máquina virtual para incrementar la rapidez de ejecución de los programas escritos en Java, así como nuevas herramientas que faciliten el trabajo de los programadores. De esta manera, se prevé que las aplicaciones en Java sean cada vez más rápidas, fiables y sencillas de escribir.Por todo esto, no parece arriesgado aventurar que Java será pronto, si no el estándar, sí al menos una de las grandes referencias en programación.

La propia Sun está empeñada en ello, y de hecho tomó la iniciativa de solicitar a la ISO — International StandardsOrganizationque sus especificaciones sobre Java se reconozcan como una norma oficial disponible públicamente**)** con una arquitectura que supere a los conflictos de la aplicación.

2.2 Bases Teóricas

2.2.1 Desarrollo de aplicaciones web dinámicas seguras

Las aplicaciones cliente/servidor que utilizan el protocolo HTTP para interactuar con los usuarios u otros sistemas de forma segura, son el resultado del avance que han obtenido las tecnologías de desarrollo de software, siendo el servidor web el elemento fundamental al cual aplicar políticas de seguridad, para disponer de un sistema web seguro.

Las organizaciones que exponen sus servicios informáticos a redes de acceso tienen que realizar un esfuerzo significativo para asegurar que la información y recursos estén protegidos. Internet es un factor primordial en la comunicación y también un evidente riesgo potencial de acceso y mal uso de los servicios e información disponibles. Todas las aplicaciones web deben de estar protegidas y aseguradas ante los principales ataques.

En una aplicación web, la seguridad se divide en:

- ✓ **Disponibilidad:** Propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- ✓ **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- ✓ **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- ✓ **Confidencialidad**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- ✓ **Trazabilidad:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad

2.2.2 Tecnología Java (JSP)

Las páginas JSP son la solución de tercera generación, que se pueden combinar fácilmente con algunas soluciones de segunda generación, más fácil y rápido de construir aplicaciones basadas en la Web con contenido dinámico. Podemos crear aplicaciones que se ejecuten en varios servidores, de múltiples plataformas, por la razón que Java es en esencia un lenguaje multiplataforma (Conrado, 2015).

Las páginas JSP están compuestas de código HTML / XML mezclado con etiquetas especiales para programar scripts del servidor.El motor de JSP está basado en los Servlets de Java, dentro de un contenedor como Tomcat. Para crear las aplicaciones en JSP se generan los archivos con extensión .jsp que incluyen dentro la estructura de etiquetas HTML, las sentencias Java para ejecutar en el servidor. Antes de que las páginas sean funcionales, el motor lleva a cabo una fase de interpretación del archivo a un servlet, por lo general esta interpretación se realiza cuando se recibe la primera solicitud de la página (Conrado, 2015).

2.2.2.1 Enfoques de la tecnología JSP

La tecnología JSP presenta dos enfoques para la construcción de aplicaciones web: Las arquitecturas “JSP Model 1” y “JSP Model 2”. La diferencia entre estos dos modelos está donde tiene lugar el procesamiento. Para el modelo 1, la página web se encarga de tramitar las solicitudes y devolve r respuestas a los clientes (Conrado, 2015).

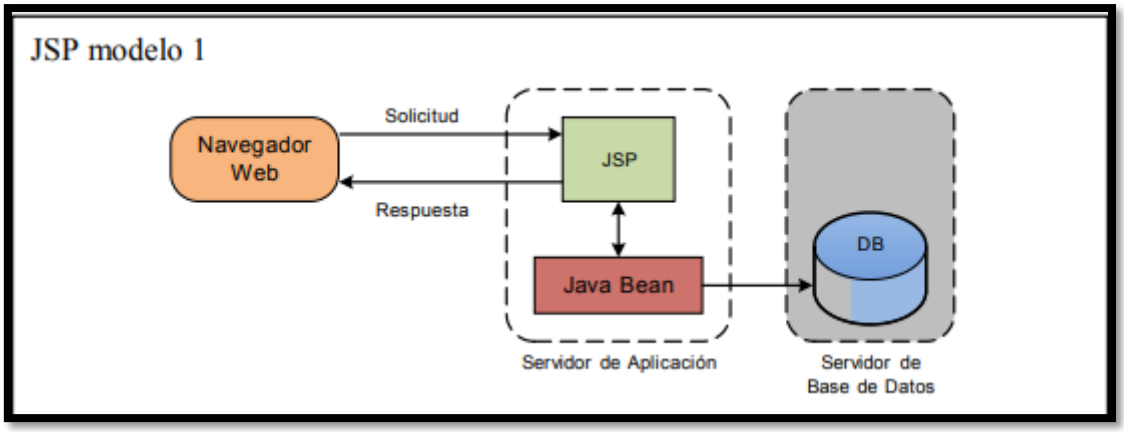


Figura 1-2 JSP modelo1

Fuente: (Conrado, 2015)

El modelo 2, integra el uso de los servlets y las páginas JSP. En este modelo las páginas JSP se usan para la capa de presentación, y los servlets para las tareas de procesamiento, o para la lógica del negocio. Los servlets son los responsables del procesamiento de las solicitudes y la creación de los Beans necesarios para la página JSP (Conrado, 2015).

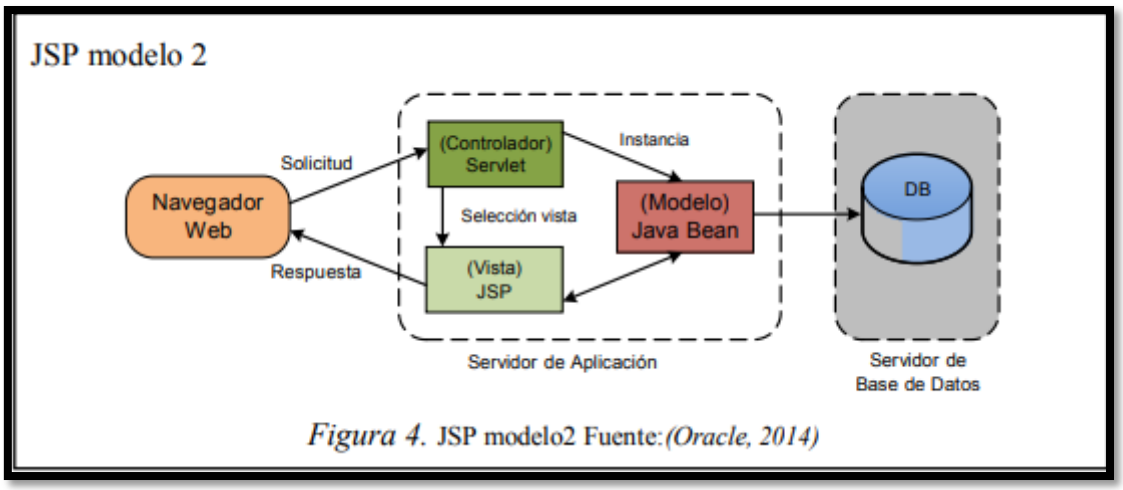


Figura 2-2 JSP modelo2

Fuente: (Conrado, 2015)

2.2.2.2 Características de la tecnología Java (JSP)

JSP sigue la filosofía de la arquitectura JAVA de "escribe una vez ejecuta donde quieras".

JSP se puede ejecutar en los sistemas operativos y servidores web más populares, como por ejemplo Apache, Netscape o Microsoft IIS (Cuello, 2016).

- ✓ **Proceso de desarrollo abierto** (Open Source). La API JSP se beneficia de la extendida comunidad JAVA existente.
- ✓ **Tags.** La tecnología JSP permite a los desarrolladores crear nuevos tags. Así los desarrolladores pueden crear tags y no depender tanto de los scripts.
- ✓ **Reusabilidad entre plataformas.** Los componentes JSP son reusables en distintas plataformas (Unix, Windows) (Cuello, 2016).

La ventaja JAVA. La tecnología JSP usa JAVA lenguaje de Script. Java es un lenguaje potente y escalable que los lenguajes de script (ASP). Las páginas JSP son compilados en Servlets por lo que actúan como una puerta a todos los servicios Java de Servidor y librerías Java para aplicaciones http. Java hace el trabajo del desarrollador más fácil ayuda a proteger al sistema de caídas, ayuda al manejo de la memoria protegiendo contra fallos de memoria y el duro trabajo de buscar los fallos de pérdida de punteros de memoria que pueden hacer más lento el funcionamiento de una aplicación (Cuello, 2016).

- ✓ **Mantenimiento.** Las aplicaciones que usan la tecnología JSP tienen un mantenimiento más fácil.

Java es un lenguaje estructurado y es más fácil de construir y mantenimientos grandes como aplicaciones modulares.

La tecnología JSP hace mayor énfasis en los componentes que en los Scripts, esto hace que sea más fácil de revisar el contenido sin que afecte a la lógica o revisar la lógica sin cambiar el contenido.

Debido a que la lógica JSP es abierta y multiplataforma, los servidores web, plataformas y otros componentes pueden ser fácilmente actualizados o cambiados sin que afecte a las aplicaciones basadas en la tecnología JSP (Cuello, 2016).

2.2.3 Tecnología PHP

El lenguaje PHP (PHP Hypertext Pre-Processor) es uno de los más antiguos (fue creado en 1995 por la empresa PHP Group) y utilizado en el diseño de páginas web que utilizan bases de datos

Se trata de un lenguaje interpretado en el lado del servidor que permite la creación de páginas web dinámicas que pueden estar dentro de páginas en HTML. Es uno de los lenguajes de programación web más populares por su rapidez y la facilidad de desarrollo.

El código PHP se incluye entre etiquetas especiales de comienzo y final que permiten entrar y salir del modo PHP, es simple para el principiante, pero a su vez, ofrece muchas características avanzadas para los programadores profesionales (Sierra, 2018).

2.2.3.1 Arquitectura de PHP

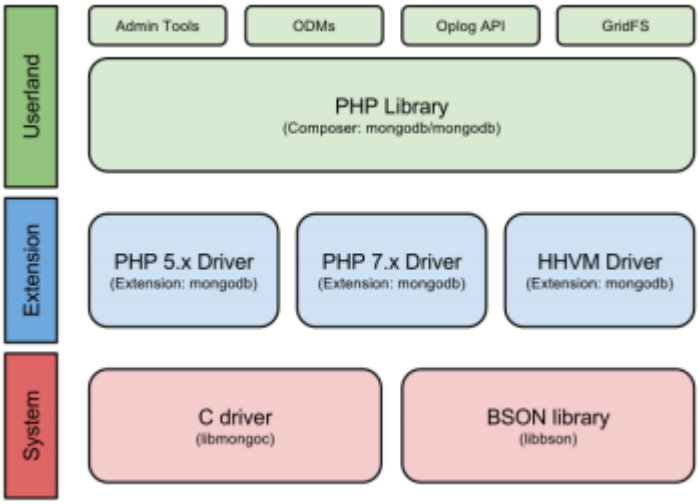


Figura 3-2 Arquitectura PHP

Fuente: (Sierra, 2018)

- ✓ En lo más alto se sitúa una biblioteca de PHP pura, la cual se distribuye como un paquete de Composer. Esta biblioteca proporcionará una API e implementa especificaciones comunes, para mejorar la consistencia de la API a través de todos los controladores mantenidos por MongoDB (Sierra, 2018).
- ✓ Luego se encuentran los controladores de nivel más bajo: uno por plataforma. Estas extensiones formarán de forma efectiva la unión entre PHP, HHVM y las bibliotecas del sistema (libmongoc y libbson). Estas extensiones expondrán una API pública idéntica para la funcionalidad más esencial y sensible al rendimiento:
    - Administración de conexiones
    - Codificación y decodificación de BSON
    - Serialización documentos de objetos (para dar soporte a bibliotecas ODM)
    - Ejecución de comandos y escritura de operaciones
    - Manejo de consultas y cursores (Sierra, 2018).

2.2.3.2 Características de la tecnología PHP

- ✓ Lo mejor de utilizar PHP es su extrema simplicidad para el principiante, pero a su vez ofrece muchas características avanzadas para los programadores profesionales.
- ✓ Una de las características más potentes y destacables de PHP es su soporte para un amplio abanico de bases de datos. Escribir una página web con acceso a una base de datos es increíblemente simple utilizando una de las extensiones específicas de bases de datos (p.ej., para mysql), o utilizar una capa de abstracción como PDO, o conectarse a cualquier base de datos que admita el estándar de Conexión Abierta a Bases de Datos por medio de la extensión ODBC. Otras bases de datos podrían utilizar cURL o sockets, como lo hace CouchDB (Sierra, 2018).
- ✓ Con PHP no se está limitado a generar HTML. Entre las capacidades de PHP se incluyen la creación de imágenes, ficheros PDF e incluso películas Flash (usando libswf y Ming) generadas sobre la marcha.
- ✓ También se puede generar fácilmente cualquier tipo de texto, como XHTML y cualquier otro tipo de fichero XML. PHP puede autogenerar estos ficheros y guardarlos en el sistema de ficheros en vez de imprimirlos en pantalla, creando una caché en el lado del servidor para contenido dinámico (Sierra, 2018).

Ventajas

Según PHP INFO-IUTEPI (2017), dentro de las ventajas de PHP se mencionarán las siguientes:

- ✓ Es un lenguaje sencillo y fácil de estudiar y aprender.
- ✓ Una de sus características es la rapidez.
- ✓ Lo soportan la mayoría de las plataformas de alojamiento web.
- ✓ Tiene ciertas características de los lenguajes orientados a objetos como la utilización de clases y herencias.
- ✓ Puede mezclarse con código HTML, aunque esto dificulta su lectura.
- ✓ Puede manejar ficheros y conectarse a distintas bases de datos (MySQL, Oracle, SQL Server, Informix, PostgreSQL, etcétera).
- ✓ El software que permite soportarlo en los servidores de hosting es libre y gratuito.
- ✓ Está en continuo desarrollo y soporta numerosas funcionalidades.
- ✓ Existe numerosa documentación sobre el lenguaje en Internet por lo que es relativamente sencillo resolver los problemas que nos puedan surgir durante el desarrollo de un sitio web.

- ✓ No requiere definición de tipos de variables, aunque sus variables se pueden evaluar también por el tipo que estén manejando en tiempo de ejecución (Sierra, 2018).

Desventajas

- ✓ Entre las desventajas de PHP se pueden mencionar las siguientes:
- ✓ PHP no es probablemente el mejor lenguaje para escribir aplicaciones gráficas, pero si es posible utilizando PHP-GTK para escribir dichos programas. Es también posible escribir aplicaciones independientes de una plataforma. PHP-GTK es una extensión de PHP, no disponible en la distribución principal.
- ✓ Para poder ver y testear las páginas que vayamos creando es necesario disponer de un servidor web que soporte PHP.
- ✓ Parte del contenido de las páginas puede no ser accesible a los navegadores, dificultando el posicionamiento de las páginas.
- ✓ Como es un lenguaje que se interpreta en ejecución, para ciertos usos puede resultar un inconveniente que el código fuente no pueda ser ocultado. La ofuscación es una técnica que puede dificultar la lectura del código, pero no necesariamente impide que el código sea examinado.
- ✓ Debido a que es un lenguaje interpretado, un script en PHP suele funcionar considerablemente más lento que su equivalente en un lenguaje de bajo nivel, sin embargo, este inconveniente se puede minimizar con técnicas de caché tanto en archivos como en memoria.
- ✓ En las versiones previas a la 7, las variables no son tipificadas, lo cual dificulta a los diferentes IDEs ofrecer asistencias para el tipificado del código, aunque esto no es realmente un inconveniente del lenguaje en sí. Esto es solventado por algunos IDEs añadiendo un comentario con el tipo a la declaración de la variable (Sierra, 2018).

2.2.4 Tecnología ASP.net

Es una tecnología del lado de servidor desarrollada por Microsoft para el desarrollo de sitio web dinámicos.ASP significa en inglés (Active Server Pages), fue liberado por Microsoft en 1996. Las páginas web desarrolladas bajo este lenguaje es necesario tener instalado Internet Information Server (IIS). ASP no necesita ser compilado para ejecutarse. Existen varios lenguajes que se pueden utilizar para crear páginas ASP. El más utilizado es VBScript, nativo de Microsoft. ASP

se puede hacer también en Perl andJscript (no JavaScript). El código ASP puede ser insertado junto con el código HTML. Los archivos cuentan con la extensión (ASP) (Sarmiento, 2017).

2.2.4.1 Características de la tecnología Tecnología ASP.net

- ✓ Programación Orientada a Objetos: La plataforma fue construida aplicando el paradigma de Programación Orientada a Objetos (POO). El núcleo de lenguajes como C# están basados en los principios OO.
- ✓ Soporte para múltiples lenguajes: En .NET, la verdadera interoperabilidad entre lenguajes es posible gracias a las capacidades que tiene la plataforma como herencia entre lenguajes (Cross-Language Interoperability) que junto con un sistema de tipos unificado (Common Type System), hace que la integración entre el código escrito en diferentes lenguajes sea total. Esto permite que se puedan usar otros paradigmas de programación tales como la programación funcional con F# o lenguajes dinámicos como Ruby o Python.
- ✓ Fácil desarrollo basado en componentes: En la plataforma .NET es más fácil implementar componentes o bibliotecas de componentes que comparten funcionalidades. La unidad de código compartido en .NET se denomina ensamblado (assembly), que lleva información de la versión y todos los metadatos necesarios para usarlo.
- ✓ Simplifica el despliegue de las aplicaciones: En contraste con las aplicaciones basadas en componentes COM, no es necesario el registro de los ensamblados, Con un "Xcopy Deployment" es suficiente, es decir con copiar los ensamblados es suficiente. Se ha eliminado por completo el clásico problema de DLL HELL, gracias a que múltiples versiones de un ensamblado pueden coexistir en la misma máquina. Un ejemplo de esto es el propio .NET Framework, que es posible tener diferentes versiones instaladas.
- ✓ Soporte para Biblioteca de Clases Base (Base Class Library): .NET Framework viene con un conjunto de bibliotecas de clases que proveen bloques básicos para construir aplicaciones, todas se proporcionan de manera consistente y están diseñadas bajo los principios de la POO. Ejemplos de estas bibliotecas incluyen el uso de colecciones, manipulación de texto, acceso a bases de datos, manipulación del sistema de archivos, etc.
- ✓ Implementación de varios tipos de aplicaciones: Gracias a la Biblioteca de Clases Base (BCL) es muy fácil el poder implementar cualquier tipo de aplicación. Ya sean basadas en escritorio (Windows Forms y Windows Presentation Foundation [WPF]), aplicaciones (Sierra, 2018)

VENTAJAS

- ✓ Completamente orientado a objetos.
- ✓ Controles de usuario y personalizados.
- ✓ División entre la capa de aplicación o diseño y el código.
- ✓ Facilita el mantenimiento de grandes aplicaciones.
- ✓ Incremento de velocidad de respuesta del servidor.
- ✓ Mayor velocidad.
- ✓ Mayor seguridad (Sarmiento, 2017).

DESVENTAJAS

- ✓ ASP.NET por las múltiples funciones que tiene es un poco más lento que por ejemplo PHP, pero para un proveedor inteligente es cuestión de potencia de servidores. Por ello el alojamiento Windows en Pixel Consultors tiene un coste superior a los alojamientos Linux (para PHP), que está justificado por todas las ventajas que se obtienen y además es mucho más estable que los servidores Linux.
- ✓ Intenta ser solución para un modelo de programación rápida ya que "programar en ASP es como programar en Visual Basic", por supuesto con muchas limitaciones y algunas ventajas específicas en entornos web.
- ✓ Mayor consumo de recursos (Sarmiento, 2017).

2.2.5 Lenguajes de servidor

- **ASP, JSP, PHP**
- Aumentan enormemente la potencia de los documentos HTML al permitir la comunicación con aplicaciones residentes en el servidor, y muy especialmente con servidores de bases de datos
- Esta potencialidad conlleva riesgos. Hay que revisar a fondo la configuración para eliminar funcionalidades no utilizadas y seguir prácticas adecuadas de programación, sobre todo en funciones con vulnerabilidades conocidas.

- Hay que proteger el código fuente para evitar que pueda ser visualizado, especialmente cuando contiene información sensible como pueden ser los datos de conexión al servidor de bases de datos
- Una medida razonable consiste en sacar el código fuente sensible fuera de la raíz de la web.

2.2.6 Seguridad en las comunicaciones

SSL: (Secure Socket Layer) es un protocolo para asegurar el transporte de datos entre el cliente y el servidor web. Diseñado inicialmente por Netscape, hoy día es soportado por la mayoría de los servidores web.Puede reconocer una conexión HTTP sobre SSL porque aparece el prefijo '**https**' en lugar de 'http' en la URL.

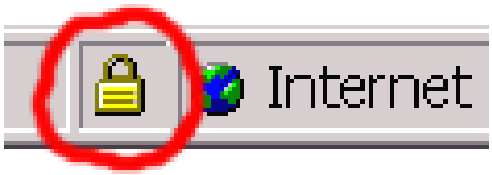


Figura 4-2 Seguridades en las comunicaciones

Fuente: Autenticación, Seguridad y Privacidad para su web y para sus clientes. Disponible en:http://www.iguanahosting.com/venezuela/es/certificados-ssl.php

La versión actual de SSL es la 3 y a partir de ella se está desarrollando un protocolo público por parte del Internet Engineering Task Force (IETF), que se conoce como TLS (Transport Layer Security) y es compatible con SSL.

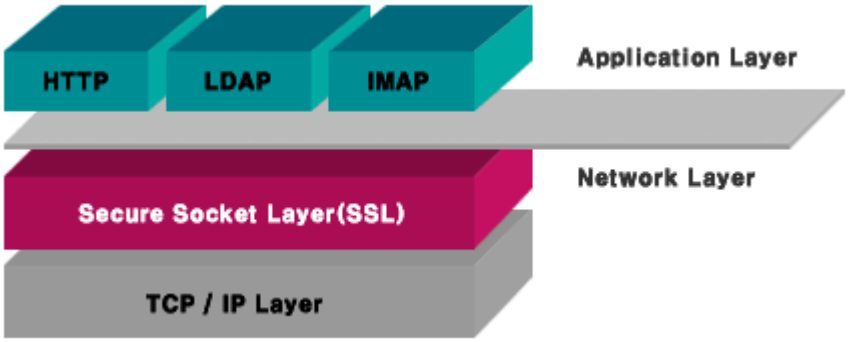


Figura 5-2 Protocolo SSL

Fuente: Utilizar el protocolo SSL. Disponible en: http://www.4d.com/docs/CMS/CMS02064.HTM

SSL no es un protocolo simple, sino que tiene dos niveles de protocolos

El protocolo Record proporciona servicios de seguridad básica a varios protocolos de nivel más alto, entre ellos HTTP.

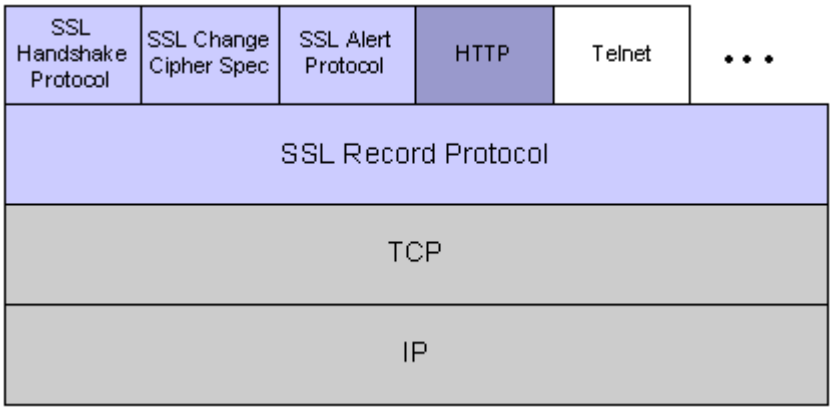


Figura 6-2 Protocolo SSL
Fuente: Pago electrónico. Disponible en:
Http: pago-electronico.html

SSL proporciona una comunicación segura entre cliente y servidor permitiendo la autentificación mutua, el uso de firmas digitales y garantizando la privacidad mediante encriptación. Una sesión SSL se establece según una secuencia de operaciones.

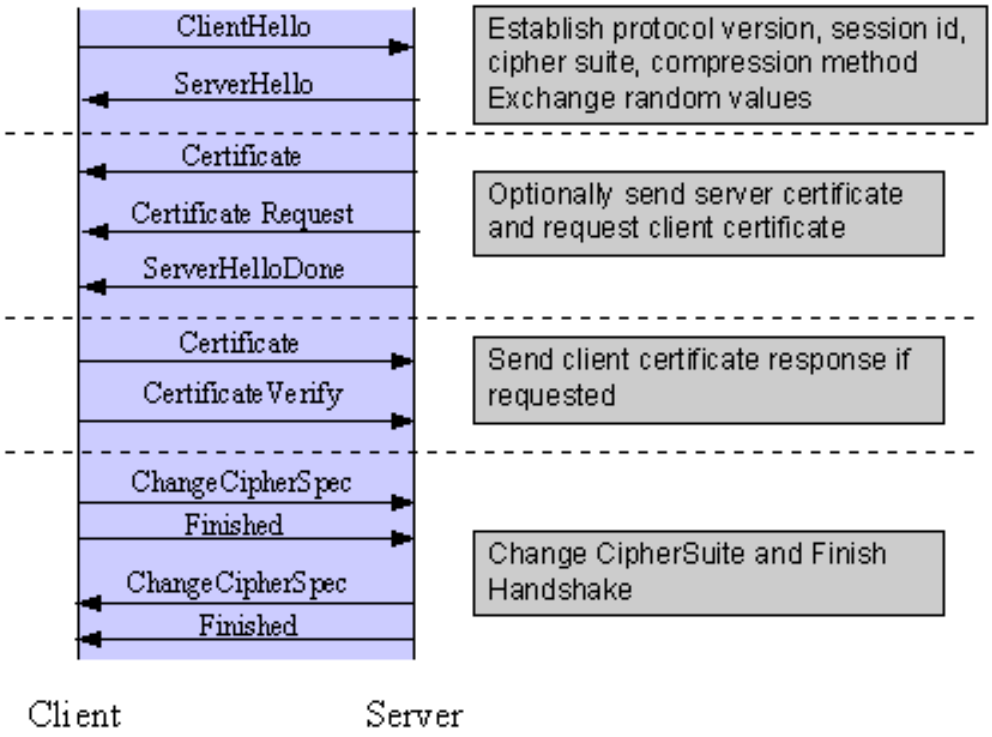


Figura 7-2 Sesión SSL
Fuente: Guía del usuario, como funciona SSL.
Disponible en: http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user277.htm

2.2.7 Seguridades a nivel de aplicaciones web

2.2.7.1 Seguridades con sesiones

El manejo de sesiones Web es una técnica o herramienta que permite vincular información a un usuario en concreto durante el proceso de visita a un sitio Web.Esta herramienta se utiliza habitualmente para labores de autenticación y seguimiento de la actividad de los usuarios en aplicaciones que tienen partes privadas para las que se necesita algún tipo de control de acceso. El manejo de sesión facilita y unifica las tareas de control y supervisión de accesos, pero si presenta alguna vulnerabilidad puede dar problemas con la seguridad de toda la aplicación.

Cookies y Sesiones: Una cookie es un fragmento de información que se almacena en el navegador del visitante de una página, a petición del servidor de esta. Esta información puede ser luego recuperada por el servidor en posteriores visitas para que se pueda conservar información entre una página y otra ya que el protocolo HTTP es incapaz de mantener información por sí mismo.

Los usos más frecuentes de las cookies son:

- Mantener opciones de visualización.
- Almacenar variables.
- Realizar un seguimiento de la actividad de los usuarios.
- Autenticación.

Una sesión web consiste en un array de datos que se mantiene en el servidor. Cada sesión viene identificada por un código único que se utiliza para hacer referencia a la misma. (Identificador de sesión)

En la sesión se pueden almacenar una serie de variables que serán conservadas hasta que se produzca su caducidad o sea explícitamente borrada

Cookies de Sesión: Cuando una cookie se usa para autenticación normalmente se hace mediante la utilización de sesiones. En la cookie se almacenará el identificador de una sesión que será asociada al usuario que accede a la aplicación.

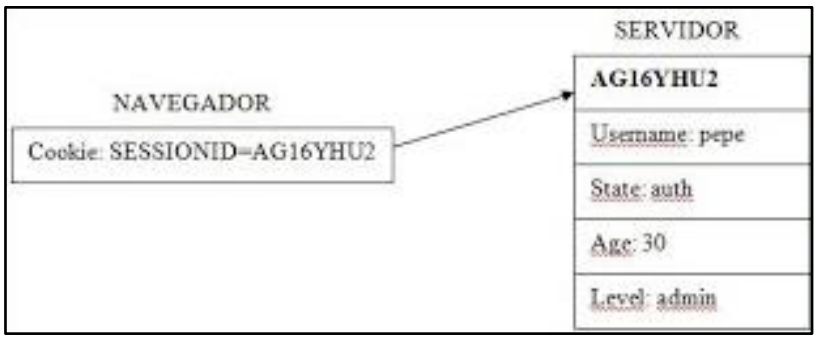


Figura 8-2 Sesiones
Fuente: cookies y sesión. Disponible en: http://www.aspnetya.com.ar/detalleconcepto.php?codigo=70

Para que una cookie de sesión se considere segura debe cumplir con algunas condiciones:

- La única información que debe contener será el identificador de la sesión asociada. El resto de las variables se almacenará internamente en el array que se encuentra en el servidor.
- El identificador de sesión debe ser único, aleatorio y no predecible. Con el fin de evitar suplantaciones de identidad.
- Las variables almacenadas en la sesión deben permanecer lo más protegidas posible del exterior. El usuario no debe conocer su nombre ni su valor, y tampoco podrá modificarlas a voluntad.
- Cuando el usuario ha terminado su actividad o ha transcurrido un periodo de tiempo prudencial, la sesión debe borrarse.

2.2.8 Seguridades en inicio de sesión

En muchas aplicaciones, los usuarios tienen acceso al sitio de forma anónima (sin tener que proporcionar credenciales usuario y clave). Si es el caso, la aplicación obtiene acceso a recursos al ejecutarse en el contexto de un usuario predefinido. De forma predeterminada, este contexto es el usuario local del equipo del servidor web. Para restringir el acceso únicamente a los usuarios que se hayan autenticado, hay que tomar en cuenta las siguientes instrucciones:

- Si la aplicación pertenece a una intranet, de ser configurada para usar la seguridad integrada del sistema operativo. De este modo, las credenciales de inicio de sesión de los usuarios se pueden usar para obtener acceso a los recursos.
- Si precisa proporcionar credenciales del usuario, hay que utilizar alguna de las estrategias de autenticación.

Nunca se debe dar por sentado que la entrada proveniente de los usuarios es segura. A los usuarios malintencionados les resulta fácil enviar información potencialmente peligrosa desde el cliente a la aplicación. Para protegerse contra las entradas malintencionadas, siga estas instrucciones:

- En las páginas Web hay que filtrar la entrada de los usuarios para comprobar si existen etiquetas HTML, que pueden contener un script.
- Nunca repita (muestre) entrada de los usuarios sin filtrar. Antes de mostrar información que no sea de confianza, codifique los elementos HTML para convertir cualquier script potencialmente peligroso en cadenas visibles, pero no ejecutables.
- No almacene nunca información proporcionada por el usuario sin filtrar en una base de datos.
- Si desea aceptar algún elemento de código HTML de un usuario, fíltrelo manualmente. En el filtro, defina explícitamente lo que aceptará. No cree un filtro que intente eliminar cualquier entrada malintencionada, ya que es muy difícil anticipar todas las posibilidades.
- No dé por sentado que la información obtenida del encabezado de solicitud HTTP (en el objeto HttpRequest) es segura. Proteja las cadenas de consulta, cookies, etc. Tenga en cuenta que la información que el explorador envía al servidor puede ser suplantada, en caso de que resulte importante para la aplicación en cuestión.
- Si es posible, no almacene información confidencial en un lugar accesible desde el explorador, como campos ocultos o cookies. Por ejemplo, no almacene una contraseña en una cookie.

2.2.9 Seguridades con Java Script

JavaScript es un lenguaje de programación estándar que se puede incluir en las páginas web para proporcionar nuevas funcionalidades como, por ejemplo, menús, sonidos y otras características interactivas. Por defecto, los exploradores permiten el uso de JavaScript y no requiere ningún tipo de instalación adicional. Por desgracia, JavaScript también se puede utilizar para cosas que determinados usuarios no desean. Aunque la configuración de JavaScript está configurada para proporcionar una experiencia segura en la web, entre las seguridades que Java Script se encuentra:

- **Acceso bloqueado a recursos externos**

JavaScript fue diseñado para cumplir ciertas normas básicas de seguridad, dirigidas fundamentalmente a proteger la integridad del sistema del usuario. Hay que observar que, tras cargar una página HTML, el navegador ejecuta el código que ésta contiene, sin que el usuario tenga por qué saber que esto está sucediendo.

La primera norma autoimpuesta por los diseñadores de JavaScript es la imposibilidad de acceder a elementos externos a la página web. De este modo, JavaScript no puede abrir o leer ficheros del PC del usuario, ni ejecutar programas externos. Tampoco es posible mediante JavaScript realizar conexiones con servidores externos desde el PC.

La única excepción a la regla anterior son las **cookies.** Un script JavaScript puede establecer cookies en el PC del usuario. Normalmente se guardan como ficheros especiales, aunque esto depende del navegador. De igual modo, JavaScript permite que un script lea las cookies que se correspondan con el mismo dominio desde el que se descargó la página que contiene el script.

Los navegadores de Microsoft incorporan formas de eludir estas restricciones usando controles ActiveX, por lo que la recomendación general es no utilizar el Internet Explorer, ya que es por diseño un navegador inseguro (a pesar de incorporar medidas de seguridad específicas para evitar que estas funciones extra supongan un riesgo).

- **Acceso limitado a objetos potencialmente peligrosos**

Si el mundo exterior queda fuera del alcance de un script JavaScript, algunos elementos de la propia página HTML también han sido protegidos por los diseñadores de JavaScript.

Para empezar, el objeto history, que contiene el historial de navegación del usuario, no puede leerse desde JavaScript. Es un error común intentar leer algún elemento de este objeto. Se puede

ir al elemento siguiente de la lista (history.forward()), o al anterior (history.back()), pero no conocer su valor.

Tampoco es posible establecer el valor de un campo de formulario de tipo file. Estos campos se usan para realizar descargas de ficheros de la máquina local al servidor (uploads), y resultaría peligroso que se pudiera establecer un valor mediante JavaScript para el nombre del fichero a descargar.

- **Confirmación del usuario antes de realizar ciertas acciones**

Finalmente, la definición de JavaScript especifica la necesidad de que el navegador pida la confirmación del usuario antes de realizar ciertas acciones. Entre ellas, cerrar cualquier ventana que no haya sido abierta desde un script JavaScript (es decir, que no haya abierto un comando window.open()), y enviar un mensaje de correo.

Otras limitaciones incluidas en el estándar son la imposibilidad de abrir ventanas con JavaScript de tamaño inferior a ciertos parámetros que las hagan no visibles (100 por 100 pixels es el límite), o fuera de las coordenadas de la pantalla (es decir, fuera del área de visión del usuario).

- **Acceso bloqueado a elementos descargados de otros servidores**

JavaScript tiene un mecanismo de seguridad por el cual ningún script puede acceder a las propiedades de documentos que procedan de un servidor distinto. Se basa en el concepto del mismo origen, según el cual cuando se carga un documento de un determinado origen, un script cargado de otro origen (y en otra ventana o marco) no puede obtener ni establecer propiedades de objetos del primer documento.

El origen en este contexto queda definido como la parte de la URL que contiene el protocolo, el nombre de la máquina, el dominio y el puerto. La política de seguridad por defecto, en todas las versiones de JavaScript, sigue la regla del mismo origen. No obstante, las versiones 1.1 y 1.2 de JavaScript introdujeron variaciones sobre este modelo:

JavaScript 1.1 introduce el marcado de datos, que sólo está disponible en esta versión. El marcado de datos otorgaba al desarrollador la potestad de decidir qué objetos de la página podían violar la norma del mismo origen, marcándolos con la función taint(), y su contraria untaint(). Cuando un objeto estaba marcado un script de otra ventana o marco podía acceder a sus propiedades. Para que esto fuera posible, el marcado de datos debía estar habilitado en el navegador, lo cual sólo podía hacerse en el Netscape Navigator, estableciendo el valor de la variable de entornoNS_ENABLE_TAINT a 1.

La versión 1.2 de JavaScript eliminó el marcado de datos, sustituyéndolo por el firmado de scripts, basado en el modelo de seguridad de Java para objetos firmados.

- **Scripts relacionados**

Proteger las imágenes de un documento (mejorado): Evita que las imágenes de una página se puedan guardar pulsando el botón derecho del ratón (con la opción de guardar como), pero permite sin embargo abrir un enlace en ventana nueva con el botón derecho.

Protección de una imagen mediante CSS: Impide la copia de una imagen con el "Guardar como..." del botón derecho del ratón mediante la colocación de una imagen transparente delante de ella.

Ocultar el código fuente de la página con control de dominio: Formulario que permite cifrar el código fuente de una página HTML para que no pueda ser copiada, añadiendo un script para impedir que se cargue desde un dominio que no sea el suyo.

2.2.10 Funciones de seguridad definidas por el usuario

- **Bloqueo de Usuarios**

Durante la implementación del SysPosgrado se crean en la base de datos una serie de entradas correspondientes a usuarios considerados `del sistema' (administrador, docente, estudiante); ninguno de estos usuarios tiene por qué acceder a cuentas que no le correspondan, de forma que una buena política es bloquear sus cuentas si exceden el número de intentos permitidos. Podemos comprobar qué usuarios tienen el acceso bloqueado consultando el estado de su contraseña o password en la base de datos específicamente en los campos ‘user’ si su valor es mayor que 3 y si el campo ‘paswword’ contiene la palabra ‘BLOQUEADO’, esto significara que la cuenta está bloqueada:

```
<jsp:forward page="IndexEstudiante.jsp"></jsp:forward>
<%
}
else
{
obj1= Estudiante.ObtenerEstudianteDadoCedula(request. getParameter("UserName"));
if(!(obj1==null))
{
if(obj1.getClave().equals("BLOQUEADO"))
{
%>
<jsp:forward page="LoginEstudiantes.jsp">
<jsp:param name="error" value="Usuario Bloqueado" />
</jsp:forward>
<%
```

A pesar de su estado, las cuentas bloqueadas son accesibles si ejecutamos la orden `Actualizar password' como administradores, por lo que si estamos bastante preocupados por nuestras cuentas podemos recuperarlas con una función que se ejecuta al actualizar el password:

```
CREATE DEFINER=`root`@`localhost` PROCEDURE `ACTUALIZAUSERESTUDIANTEBLOQUEO`(IN ID_ESTUDIANTEp INT, IN USERp VARCHAR(30),IN CLAVEp VARCHAR(300))
begin
UPDATE ESTUDIANTE set USER=USERp,PASSWORD=CLAVEp
WHERE ID_ESTUDIANTE=ID_ESTUDIANTEp;
end;
```

El usuario que actualiza su password tendrá la opción de cambiar la contraseña proporcionada por el administrador tan solo con actualizar su paswword desde su propia cuenta:

```
CREATE DEFINER=`root`@`localhost` PROCEDURE `ACTUALIZAESTUDIANTE`( IN PASSWORDp VARCHAR(300), IN USERp VARCHAR(30))
begin
UPDATE ESTUDIANTE set,PASSWORD=PASSWORDp,USER=USERp
WHERE ID_ESTUDIANTE=ID_ESTUDIANTEP;
end;
```

No obstante, muchísimo más importante que esto es eliminar o bloquear a cualquier usuario sin contraseña en el sistema; es recomendable comprobar de forma periódica que estos usuarios no existen, para lo cual también podemos utilizar `password = BLOQUEADO y user>3':

```
SELECT * FROM estudiante where password = BLOQUEADO and user>3;
```

- **Confirmación de Usuarios**

Otro tipo de seguridad implementado en el sistema es la confirmación de ser un usuario real con datos reales, ya que al momento de logearse recibe un código aleatorio de confirmación que será enviado a su correo electrónico y celular previamente registrados en su cuenta:

```
sesionOk=request.getSession();
        sesionOk.setAttribute("ciDocente",obj1.getCedula());
sesionOk.setAttribute("IdDocente",obj1.getIdDocente());
int numeroAleatorio = (int) (Math.random()*125598+1
String codigo =  String.valueOf(numeroAleatorio);
```

```
ubDocente.setUsuario(codigo);
        ubDocente.setIdDocente(obj1.getIdDocente());
        Docente.ActualizarDocenteAleatorio(ubDocente);

        String nom =obj1.getNombres()+" "+obj1.getApellidos();
        Circulares.mail.enviar(nom, obj1.getEmail(), codigo);
Circulares.SMSClient sms =new SMSClient();
        Integer aux=sms.sendMessage(obj1.getCelular().toString(),codigo);

<jsp:forward page="CodigoActivacion.jsp"></jsp:forward>
```

Luego de revisar su correo o celular tendrá que volver a loguearse en el sistema, pero en esta ocasión con el número que recibe para confirmación:

```
CREATE PROCEDURE `LoguearDocenteCodigoActivacion`(IN CEDULAp VARCHAR(10),IN USUARIOp VARCHAR(30))

begin

SELECT * FROM DOCENTE

WHERE DOCENTE.CEDULA=CEDULAp

AND DOCENTE.USUARIO=USUARIOp;

end;
```

- **Bloquear Conexiones remotas**

Tras estas medidas de seguridad iniciales, lo más probable es que en nuestro sistema comencemos a dar de alta usuarios reales; sin duda, lo primero que estos usuarios tratarán de hacer es conectar remotamente para lo cual nos aseguraremos de que el sistema no lo permita:

Nos logeamos mysql -u root –password=Password
Verificamos las conexiones remotas:
GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY "PASSWORD";
Mediante root@'%'

En este caso tiene todo el control y procedemos a quitarle los privilegios retirando el IP% que significa todas.

- **Parámetros al ingreso del password**

Otro aspecto interesante de cara a incrementar aspectos de la seguridad relacionados con los usuarios de nuestro sistema, se definieron parámetros para reforzar nuestra política de contraseñas; por ejemplo, la longitud mínima para los password de los usuarios es de 5 caracteres y máximo 20 entre números y caracteres:

var sprytextfield2 = new Spry.Widget.ValidationTextField("sprytextfield2", "none", {minChars:5, maxChars:20, validateOn:["blur"]});

- **Encriptación de Contraseñas**

La manera de asegurar la confidencialidad de los usuarios y su información se mantiene en el sistema el mecanismo de encriptación de contraseñas:

String clave=request.getParameter("Password");

String claveencriptada=DigestUtils.md5Hex(clave);

Esto lo realizamos a nivel de la aplicación obteniendo el resultado indicado en la base de datos:

password=’ 1262d42d86cd9f84ce2086c613fed8bd’

- **Privilegios a la base de datos de acuerdo al tipo de Usuario**

Un usuario que no sea administrador no tiene por qué tener acceso a procesos que no le han sido asignados para lo cual se posee diferentes tipos de usuarios:

<jsp:forward page="LoginAdministrador.jsp"></jsp:forward>

<jsp:forward page="LoginDocentes.jsp"></jsp:forward>

<jsp:forward page="LoginEstudiantes.jsp">

Peor aún a los procesos de la base de datos para lo cual se ha restringido sus privilegioscon; a creación de nuevos usuarios:

GRANT USAGE ON *.* TO 'Diego'@'localhost' IDENTIFIED BY PASSWORD '*58A53281961DAAF5CE57BA76149D8C4E2E249633';

GRANT SELECT, INSERT, UPDATE, DELETE, REFERENCES ON `gestionpostgrado`.* TO 'Diego'@'localhost';

2.2.11 Comparativo de tecnologías PHP, ASP.net y Java (JSP)

Cuadro comparativo, con una valoración de 1 a 4, donde 4 es la mejor valoración, estos valores son asignados a cada una de las tecnologías

Tabla 1-2 Portabilidad en los servidores, según los sistemas operativos

	Java (JSP)	**ASP.NET**	**PHP**
Bajo Costo	4	1	3
Portabilidad	4	3	4
Seguridad	2	4	4
Estabilidad	4	4	4
Acceso a Bases de Datos	4	4	4
Multiplataforma	4	3	4
Programación Orientado a Objetos	3	4	4
Bajo Requerimiento de Hardware	4	2	3
Aplicaciones con Alta Complejidad	3	4	4
Fácil Desarrollo	4	3	2
Facilidad de Ayuda	4	2	2
Soporte XML	4	4	4
Velocidad de Ejecución	4	3	3
Soporte Técnico	2	4	3
IDEs Disponibles	2	4	4
Curva de Aprendizaje	4	2	2
Servidores Web disponibles en Internet	4	2	1
TOTAL:	**60**	**53**	**55**

Fuente: (Comparativa Jsp, Php y Asp, 2016)

Elaborado por: Fonseca, Elvis 2020

Tabla 2-2 Arquitectura de software y hardware

Herramienta	Apache		IIS		Tomcat		One (Modulo)	ASP
	Windows	Linux	Windows	Linux	Windows	Linux	Windows	Linux
PHP	**x**	**x**	**X**					
ASP.net			**X**					**x**
Java (JSP)	**x**	**x**			**x**	**x**		

Elaborado por: Fonseca, Elvis 2020
Fuente: (Norte, Molinares y Olaciregui 2014)

Tabla 3-2 Grado de detección de fallas

	Herramientas		
Características necesarias para un funcionamiento adecuado	**PHP**	**ASP.net**	**Java (JSP)**
Sistema Operativo	Linux	Windows	Linux
Servidor	Apache	IIS	Tomcat
	128 o más	128 o más	256 o más

Elaborado por: Fonseca, Elvis 2020
Fuente: (Norte, Molinares y Olaciregui 2014)

Tabla 4-2 Grado de detección de fallas

Elaborado por: Elvis Fonseca, 2020

	Herramientas		
Detección de fallas	**PHP**	**ASP.net**	**Java (JSP)**
Óptimo			
No óptimo			

Fuente: (Norte, Molinares y Olaciregui 2014)

Tabla 5-2 Calidad de fallas detectadas

Herramienta	Hay error + Ubicación	Tipo de error
PHP	135 (90%)	23 (15%)
ASP.net	83 (55%)	69 (46%)
Java (JSP)	143 (95%)	140 (93%)

Elaborado por: Fonseca, Elvis 2020
Fuente: (Norte, Molinares y Olaciregui 2014)

Tabla 6-2 Integridad de la base de datos

Herramientas	Integridad	
	Windows	Linux
PHP	132 (88%)	141 (94%)
ASP.net	71 (47%)	68 (45%)
Java (JSP)	67 (46%)	74 (49%)

Elaborado por: Fonseca, Elvis 2020
Fuente: (Norte, Molinares y Olaciregui 2014)

Tabla 7-2 Complejidad en la programación

	PHP	ASP.net	Java (JSP)
ACTUALIZACIONES			
Artículo	41	43	66
Cliente	39	39	70
Vendedor	39	39	73
INSERCIONES			
Artículo	15	18	31
Cliente	12	18	31
Vendedor	12	19	37
CONSULTAS			
Artículo	31	48	71
Cliente	31	40	66
Vendedor	31	40	68
Listado	11	20	28
ELIMINACIONES			
Artículo	29	69	74
Cliente	28	53	71
Vendedor	28	60	70
VENTA	231	291	299

Elaborado por: Fonseca, Elvis 2020
Fuente: (Norte, Molinares y Olaciregui 2014)

Tabla 8-2 Promedios de Tiempos de respuesta

	PHP		ASP.net		Java (JSP)	
ACTUALIZACIONES						
	Linux	**Windows**	Linux	**Windows**	Linux	**Windows**
Artículo	0,0079	0,3949	0,3124	0,2121	0,0029	0,1772
Cliente/Vendedor	0,0081	0,4270	0,3902	0,4996	0,0036	0,1807
INSERCIONES						
Artículo	0,0070	0,2262	0,2456	0,1057	0,0028	0,0677
Cliente/Vendedor	0,0109	0,2212	0,1074	0,1030	0,0052	0,0458
CONSULTAS						
Artículo	0,0056	0,1430	0,1244	0,1007	0,0024	0,0927
Cliente/Vendedor	0,0061	0,1975	0,2596	0,3096	0,0034	0,0949
ELIMINACIONES						
Artículo	0,0314	0,6694	0,1123	0,1612	0,0104	0,2162
Cliente/Vendedor	0,0314	0,3378	0,5352	0,5184	0,0122	0,1744
VENTA	0,0398	0,3945	0,2860	0,3005	0,0181	0,1100
CONSILTA DE LISTADO	0,2228	6,3581	0,9455	7,7026	0,0324	0,1126

Elaborado por: Fonseca, Elvis 2020
Fuente: (Norte, Molinares y Olaciregui 2014)

CAPÍTULO III

3 METODOLOGÍA DE INVESTIGACIÓN

En el presente capitulo se detalla la metodología implantada en la siguiente investigación "Comparativo de las principales tecnologías orientadas al desarrollo de aplicaciones web Dinámicas seguras", Se indica a detalle las técnicas, métodos, mediciones mediante los cuales se seleccionó la información relevante con el objetivo de identificar la comprobación de la hipótesis en el presente trabajo.

Con el propósito de realizar la siguiente comparativa de las principales tecnologías orientadas al desarrollo de aplicaciones web Dinámicas seguras, que permita mejorar la seguridad y la confidencialidad en sistemas informáticos.

3.1. Tipo y Diseño de la Investigación

3.1.1. Tipo de Investigación

La presente investigación se realizará bajo en paradigma cuali – cuantitativo, pues se tomará en cuenta la problemática, estudiando su contexto y planteando una observación directa y la participación en el problema.

Se plantea también cuáles son las posibles causas que se presentan ante el problema y se crea además las posibles explicaciones como causa especifica. La investigación será orientada hacia la comprobación de la hipótesis para de este modo centrar el estudio sobre el fenómeno de forma general y global.

3.1.2. Diseño de la Investigación

La presente investigación del tipo experimental con un enfoque de carácter científico, donde un conjunto de variables se mantiene constantes, mientras que el otro conjunto de variables se mide como sujeto del experimento. Se utilizan los siguientes tipos de estudio:

- ✓ **Estudio exploratorio**

Ayuda a familiarizarse con fenómenos desconocidos, obtener información para realizar una investigación más completa en un contexto particular, investigar nuevos problemas, identificar conceptos o variables promisorias, establecer prioridades para investigaciones futuras, o sugerir afirmaciones y postulados.

Este estudio será de gran importancia para dar inicio la investigación para la recolección de información y selección de herramientas.

- ✓ **Estudio descriptivo**

Es útil para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación. Busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis.

Por este motivo, la etapa de extracción de características es la específica para la definición de la comparativa de las tecnologías.

- ✓ **Estudio Correlacional**

En cierta medida tiene un valor explicativo, aunque parcial, ya que el hecho de saber que dos conceptos o variables se relacionan aporta cierta información explicativa. Su finalidad es conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en un contexto específico.

3.2. Métodos y Técnicas De Investigación

3.2.1. Métodos

Los métodos de investigación científica a utilizar son los siguientes:

3.2.1.1. El método hipotético – deductivo

Este método es empleado ya que la investigación inicia a raíz de la observación de resultados de proyectos realizados, por medio de lo cual se genera hipótesis y luego se obtienen las conclusiones a partir de resultados.

3.2.1.2. Método Comparativo

Se establece un escenario sin la implementación del modelo de seguridad propuesto que pruebe una mayor confidencialidad a la información vulnerable de los usuarios en dispositivos móviles, frente al mismo escenario con la implementación del modelo de seguridad biométrico

3.2.1.3. Método de Análisis y Síntesis

Utilizado en la investigación sobre el estado del arte, la adopción de medidas a implementarse y la adquisición de parámetros sobre datos.

3.2.2. Técnicas

1. Consulta en base a documentos (Registros, Internet, bibliografía científica, investigaciones realizadas en el país y estadísticas oficiales).
2. Experimentación: Se recrearán distintas circunstancias en un ambiente controlado para la ejecución de pruebas, las cuales proveerán los resultados para la toma de decisiones y la definición del prototipo.
3. Análisis de la información.
4. Observación de campo: se harán distintas mediciones a los fenómenos recreados para la toma de decisiones.

3.3. Instrumentos

Los instrumentos son las herramientas utilizadas para realizar las pruebas dentro del escenario y a su vez facilitarán el análisis y el desarrollo de la prueba chi-cuadrado para validar el modelo de seguridad biométrica para disminuir las vulnerabilidades a la confidencialidad en dispositivos móviles.

Investigación bibliográfica – documental.

La presente investigación se basa en el estudio científico que se realiza a partir de la revisión de diferentes fuentes bibliográficas o documentales (literatura sobre el tema de investigación). En esta investigación predomina el análisis, la interpretación, las opiniones, las conclusiones y recomendaciones del autor o los autores.

3.4. Planteamiento de la Hipótesis

3.4.1. Hipótesis General

La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, si incrementará el nivel de confidencialidad en los sistemas informáticos.

3.4.2. Identificación de variables

Variable Independiente: Aplicación de la tecnología java (JSP).

Variable Dependiente: incrementará el nivel de confidencialidad en los sistemas informáticos.

3.4.3. Operacionalización Conceptual de Variables

Tabla 1-3 Operacionalización Conceptual de Variables

Hipótesis	Variables	Indicadores
La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, si incrementará el nivel de confidencialidad en los sistemas informáticos.	Independiente: Aplicación de la tecnología java (JSP). Dependiente: Incrementará el nivel de confidencialidad en los sistemas informáticos.	-Identificación de datos verificables bibliográficos. - Cuantificación de resultados efectivos -Porcentaje de vulnerabilidades -Eficiencia respecto a otras tecnologías de acceso.

Elaborado por: Fonseca, Elvis 2020

3.4.4. Operacionalización Metodológica de Variables

Tabla 2-3 Operacionalización Metodológica de Variables

Formulación del problema	Objetivo General	Hipótesis General	Variables	Indicadores	Índice	Técnicas	Instrumentos
¿El estudio comparativo de las principales tecnologías dedicadas al desarrollo de aplicaciones web dinámicas permitirá escoger	Comparar las principales tecnologías orientadas al desarrollo de aplicaciones web dinámicas seguras.	*Ho:* La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, si incrementará el nivel de confidencialidad en los sistemas informáticos. *H1:* La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, no incrementará el nivel	**Variable Independiente:** Aplicación de la tecnología java (JSP).	-Identificación de datos verificables bibliográficos. - Cuantificación de resultados efectivos -Porcentaje de vulnerabilidades	-Tanto por ciento % -Tanto por ciento %	- Observación científica. - Observación científica	Cuestionario estructurado para aplicarse a profesionales de seguridad de la información.

la que brinde los mejores mecanismos y herramientas de seguridad a la información?		de confidencialidad en los sistemas informáticos.				- Observación científica	
			Variable Dependiente: Incrementará el nivel de confidencialidad en los sistemas informáticos.	-Mecanismos de seguridad. -Intentos de inicio de sesión. -Seguridades con sesiones. -Seguridades en inicio de sesión. -Funciones de seguridad definidas por el usuario.	Tanto por ciento %	- Observación científica	Comparación Prueba chi-cuadrado

Elaborado por: Fonseca, Elvis 2020

3.5. Población y Muestra

3.5.1. Población y muestra

La investigación se realizará en una población de 30 encuestados que estará orientado profesionales de la escuela de Ingeniería en sistemas de la Escuela Superior Politécnica de Chimborazo.

Por lo tanto, por tratarse de una población pequeña no hace falta utilizar cálculo estadístico alguno para obtener una muestra, se trabajará con la totalidad de la información.

Tabla 3-3 Población y muestra

Nivel	Estudiantes
Profesionales	30

Elaborado por: Fonseca, Elvis 2020

3.5.2. Plan de recolección de información.

Para recolectar la información se utilizó profesionales de la escuela de ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo, con el fin de reducir los resultados y ver la factibilidad de una tecnología de aplicación web segura para la gestión de los servicios.

Tabla 4-3 Matriz de recolección de información

N°	Preguntas	Respuestas
1	¿Para qué?	Para alcanzar los objetivos de la investigación.
2	¿A qué personas u objetos?	Profesionales de la escuela de Ingeniería en Sistemas Superior Politécnica de Chimborazo
3	¿Sobre qué aspecto?	Desarrollo de aplicaciones web seguras con JAVA, técnicas de programación y niveles de seguridad que se pueden implementar en una aplicación web.
4	¿Quién? ¿Quiénes?	Elvis Fonseca
5	¿Cuándo?	Período académico 2020
6	¿Lugar de recolección de la información?	Escuela Superior Politécnica de Chimborazo.
7	¿Cuántas veces?	30 encuestas.
8	¿Qué técnicas de recolección?	Encuesta estructurada.
9	¿Con qué?	Cuestionario.
10	¿En qué situación?	Favorable, ya que existe la debida colaboración por parte de la comunidad Politécnica.

Elaborado por: Fonseca, Elvis 2020

3.5.3. Plan de procesamiento de información

- ✓ Diseño del material de recolección de información.
- ✓ Aplicación de la encuesta.
- ✓ Revisión de la información, selección de la información que ayude en la investigación.
- ✓ Tabulación según variables de la hipótesis, manejo de la información, estudio estadístico de los datos para la presentación de resultados.
- ✓ Representaciones gráficas.
- ✓ Análisis e interpretación de resultados.
- ✓ Análisis de resultados estadísticos, destacando las relaciones fundamentales de acuerdo con la hipótesis.
- ✓ Interpretación de resultados, con el apoyo del marco teórico.

- ✓ Comprobación de hipótesis
- ✓ Conclusiones y recomendaciones.

3.5.4. Análisis e interpretación de resultados

De acuerdo con el proyecto de investigación se aplicó la encuesta a profesionales de la de la escuela de ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo

Luego se realizó la codificación de las respuestas, logrando obtener resultados cuantitativos, los mismos que servirán para el análisis e interpretación, siendo necesarios para la verificación de hipótesis.

CAPÍTULO IV

4. RESULTADOS

4.1. Plan de recolección de información

Al tratarse de una investigación no aplicativa sino más bien de conocimiento, el proceso de recolección de la información se obtuvo mediante encuestas a varios profesionales que tienen experiencia en el área de desarrollo y han utilizado las tecnologías que aquí se proponen, con el fin de lograr mejores resultados y ver la factibilidad de construir aplicaciones web más seguras.

Tabla 1-4 Matriz de recolección de información

N°	Preguntas	Respuestas
1	¿Para qué?	Para alcanzar los objetivos de la investigación.
2	¿A qué personas u objetos?	Profesionales especializados en el área de desarrollo de aplicaciones web.
3	¿Sobre qué aspecto?	Desarrollo de aplicaciones web seguras con JAVA, técnicas de programación y niveles de seguridad que se pueden implementar en una aplicación web.
4	¿Quién? ¿Quiénes?	Elvis Martin Fonseca Changoluisa
5	¿Cuándo?	Período académico Octubre 2020 – Noviembre 2020
6	¿Lugar de recolección de la información?	Entidades que cuentan con sistemas informáticos
7	¿Cuántas veces?	30 encuestas.
8	¿Qué técnicas de recolección?	Encuesta estructurada.
9	¿Con qué?	Cuestionario.
10	¿En qué situación?	Favorable, ya que existe la debida colaboración por parte de la comunidad informática.

Elaborado por: Fonseca, Elvis 2020

Plan de procesamiento de información

- Diseño del material de recolección de información.

- Aplicación de la encuesta.
- Revisión de la información, selección de la información que ayude en la investigación.
- Tabulación según variables de la hipótesis, manejo de la información, estudio estadístico de los datos para la presentación de resultados.
- Representaciones gráficas.
- Análisis e interpretación de resultados.
- Análisis de resultados estadísticos, destacando las relaciones fundamentales de acuerdo con la hipótesis.
- Interpretación de resultados, con el apoyo del marco teórico.
- Comprobación de hipótesis
- Conclusiones y recomendaciones.

4.2. Análisis e interpretación de resultados

De acuerdo al proyecto de investigación se aplicó la encuesta a profesionales especializados en el área de desarrollo de aplicaciones web

Luego se realizó la codificación de las respuestas, logrando obtener resultados cuantitativos, los mismos que servirán para el análisis e interpretación, siendo necesarios para la verificación de hipótesis (Fonseca, 2020).

4.2.1. Encuesta dirigida a desarrolladores de software referente a la tecnología JAVA (JSP)

Pregunta 1. ¿Es una ventaja de JAVA ser una tecnología multiplataforma, es decir que funcione en prácticamente cualquier dispositivo, servidor o sistema operativo?

Tabla 2-4 Pregunta N° 1. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	21	83.3
NO	9	16.6
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

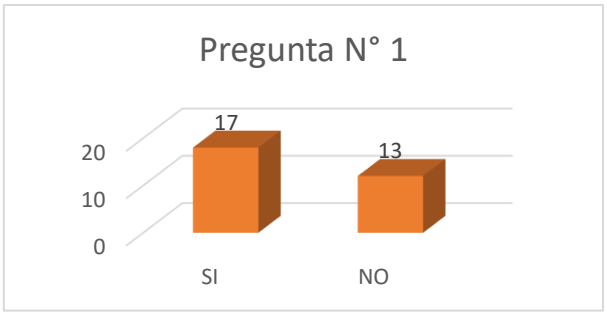


Gráfico 1-4 Pregunta N° 1. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Para la mayor parte de encuestados, la tecnología JAVA posee una característica muy importante sobre las demás tecnologías que es la de ser open source y multiplataforma es decir que las aplicaciones desarrolladas en este lenguaje funcionasen en cualquier sistema operativo o dispositivo ya que posee su propia máquina virtual y eso ya es una ventaja muy significativa.

Pregunta 2. ¿Incorpora JAVA mecanismos o funciones para ofrecer seguridad a sus aplicaciones?

Tabla 3-4 Pregunta N° 2. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	20	67
NO	10	33
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

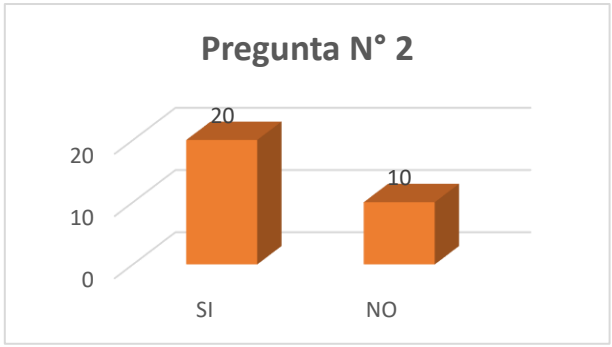


Gráfico 2-4 Pregunta N° 2. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

JSP tiene funciones para gestionar recursos del lado del cliente y servidor, manejar peticiones, persistencia para el manejo de base de datos y sesiones.

Java está diseñado para ser un lenguaje de programación seguro, entre varias funciones tenemos el control total para acceder a los recursos, encriptación y uso de certificados para firmar el código, de manera que los usuarios puedan verificar quien es el propietario del código y que este no ha sido modificado después de ser firmado, Class Loader que garantiza que los componentes del sistema no han sido reemplazados, Class file verifier que garantiza que el código tiene el formato correcto, que el bytecode no viola las restriciones de seguridad de tipos de la JVM, Security Manager que controla el acceso a los recursos en tiempo de ejecución. (https://www.uv.es/~sto/cursos/seguridad.java/html/sjava-32.html)

Pregunta 3. ¿Presta capacidades de desarrollo de métodos, funciones, procedimientos y configuraciones para proteger información y datos?

Tabla 4-4 Pregunta N° 3. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	22	73
NO	8	27
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

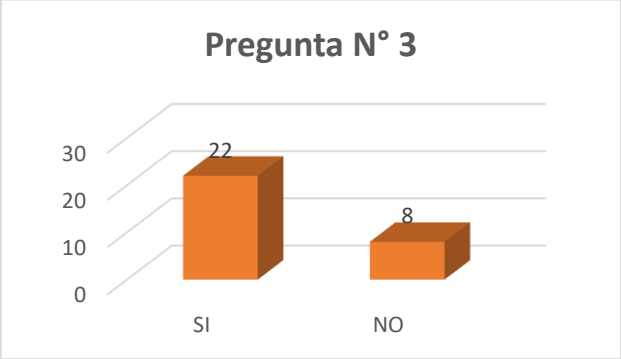


Gráfico 3-4 Pregunta N° 3. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

La misma programación aplicada a una página JSP permite construir funciones y procedimientos (definidas por el usuario) que ayuden a proteger a datos e información. En una página JSP, en una clase JSP se puede aplicar técnicas de seguridad a nivel de la aplicación web.

Pregunta 4. ¿Permite implementar estrategias para prevenir accesos no autorizados ya sea accidental o deliberado, a programas y datos?

Tabla 5-4 Pregunta N° 4. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	17	57
NO	13	43
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

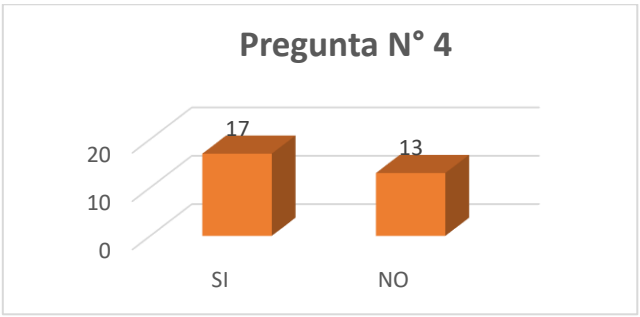


Gráfico 4-1 Pregunta N° 4. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Con un 57% de aceptación se afirma que implementar estrategias debidamente estructuradas, para evitar accesos accidentales y deliberados a la gestión de los usuarios del sistema se puede aplicar estrategias de seguridad, mediante un logueo con códigos aleatorios a más de sus credenciales de usuario, bloqueos de usuario por fallidos de inicio de sesión, entre otros.

Pregunta 5. ¿El servicio de criptografía y chequeo de seguridad que ofrece JAVA es una estrategia de prevención frente a la vulnerabilidad de la confidencialidad de los sistemas web?

Tabla 6-4 Pregunta N° 5. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	25	83
NO	5	17
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

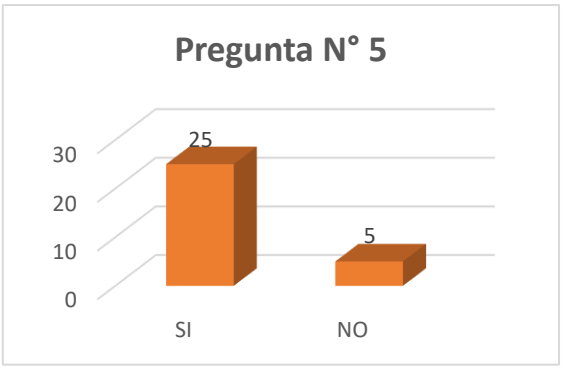


Gráfico 5-4 Pregunta N° 5. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Con un 83 % de aceptación por parte de los encuestados, la funcionalidad que JAVA nos ofrece como es la utilización de claves cifradas por parte de los usuarios y por parte del administrador ayuda sustancialmente proteger la confidencialidad en los sistemas web, ya que se dispone de un almacén de claves únicas y específicas para ese sistema que deberán ser verificadas y certificadas por el sistema para poder disponer de la información requerida.

Pregunta 6. ¿Para validar un acceso seguro a un sistema web, él envió de mensajes con códigos aleatorios al celular y correo permite validar la Identidad del usuario certificando que el código ingresado además del usuario y contraseña es propio del sistema?

Tabla 7-4 Pregunta N° 6. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	23	77
NO	7	23
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

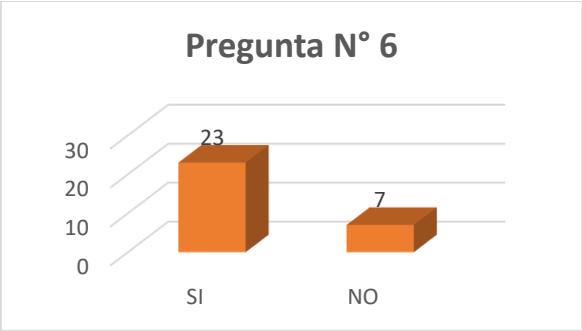


Gráfico 2-4 Pregunta N° 6. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Con un 77% de aceptación se considera que la validación de acceso seguro es importante para cualquier sistema web ya que en caso de no ser el usuario original será alertado a su celular y correo, mediante notificaciones que respalden dicha actividad sospechosas (Caisaguano & Miranda, 2013)

Pregunta 7. ¿La tecnología JAVA dispone de mecanismos seguros y compatibles para el intercambio de información con otras tecnologías?

Tabla 8-4 Pregunta N° 7. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	15	50
NO	15	50
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

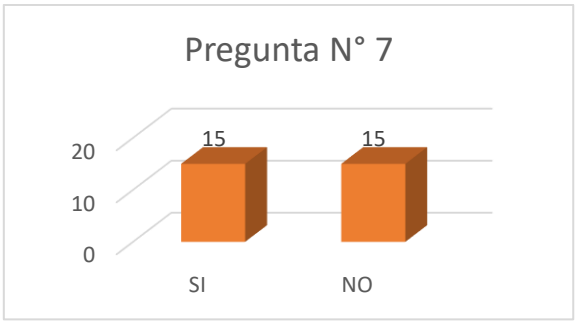


Gráfico 7-4 Pregunta N° 7. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Según se puede apreciar los encuestados consideran que la tecnología JAVA presta facilidades para el desarrollo de mecanismos que puedan servir para compartir información con otros sistemas que no se hayan desarrollados en esta misma tecnología, estos elementos se llaman servicios web y que existe herramientas para hacerlos seguros.

Pregunta 8. ¿Al ser JAVA un lenguaje de programación orientado a objetos y la no utilización de punteros disminuye el riesgo de vulnerabilidades a las aplicaciones?

Tabla 9-4 Pregunta N° 8. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	22	73
NO	8	27
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

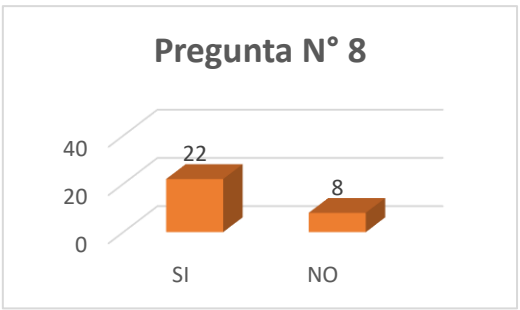


Gráfico 4:3: Pregunta N° 8. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Para el 73% de los encuestados el modelo de programación orientado a objetos que ofrece JAVA si ayuda a reducir los riesgos de vulnerabilidades ya que este método consta de una característica potente y única como es el encapsulamiento de sus funciones y variables, además al no utilizar punteros eliminamos el riesgo de que los atacantes puedan acceder a los espacios de memoria de los computadores que a menudo se utiliza para el robo de información sensible.

Pregunta 9. ¿Se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project*) y la tecnología JAVA?

Tabla 10-4 Pregunta N° 9. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	21	70
NO	9	30
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

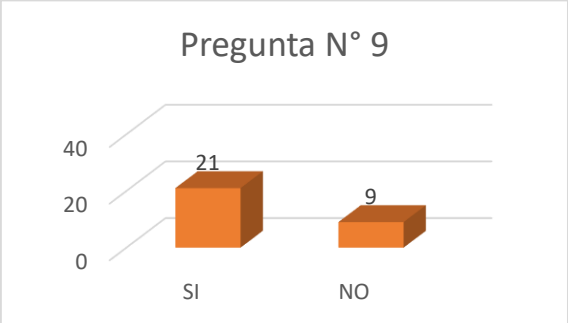


Gráfico 9-4 Pregunta N° 9. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Con un 70 % de los encuestados se asegura que si se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project).*

Pregunta 10. ¿Existe flexibilidad, escalabilidad en la tecnología JAVA para el desarrollo de aplicaciones web permitiendo mantener una estructura compacta además de la integridad de la información?

Tabla 11-4 Pregunta N° 10. Encuesta

Alternativas	Frecuencia	Porcentaje
SI	22	73
NO	8	27
TOTAL	30	100

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

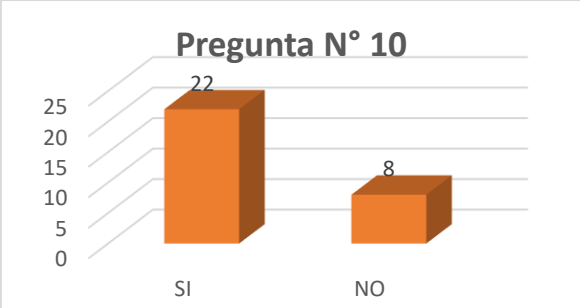


Gráfico 10-4 Pregunta N° 10. Encuesta

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Análisis e interpretación de resultados:

Con un porcentaje del 73%, los encuestados aseguran que JAVA presta las facilidades en el caso que así se lo requiera para desarrollar nuevos módulos e incorporarlos a una aplicación ya desarrollada, esto se debe a la metodología de la programación que utiliza como es la programación orientada a objetos.

4.3. Verificación de la hipótesis

Para comprobar la predicción o explicación provisoria, en relación con las dos variables planteadas utilizaremos el estadígrafo Ji Cuadrado perteneciente a la estadística descriptiva (se dedica la estudio de un conjunto de datos) aplicada al estudio de dos variables, en esta investigación se considera al universo a todos los administradores y desarrolladores de sistemas web dinámicos, para obtener una muestra se elaboró una encuesta de 10 preguntas relacionadas a la seguridad que ofrece la tecnología JAVA, esta se aplicó a 30 ingenieros en sistemas que laboran

en instituciones de educación, entidades financieras, entidades gubernamentales, FreeLancer de la provincia de Bolívar.

El índice Ji Cuadrado se basa en la comparación de las frecuencias bivariadas obtenidas a partir de los datos (frecuencias empíricas) con las frecuencias que resultarían si NO hubiere relación de asociación entre las variables (frecuencias teóricas).

$$X=\Sigma \frac{(fo - Fe)^2}{Fe}$$

X^2	Chi-cuadrado
Fo	Frecuencia observada
Fe	Frecuencia esperada o teórica
Σ	Sumatoria

Para aceptar o rechazar la hipótesis necesitamos encontrar el resultado el ji cuadrado calculado aplicando la formula, es decir remplazando los valores obtenidos en la encuesta y los obtenidos después de la implementación en los sistemas web y el ji cuadrado tabla utilizando la fórmula de grados de libertad y un margen de error del 5% el cual se convierte en un nivel de confianza de 0.05 El nivel de significación en 0.05 es solo una convención, basada en el argumento de Ronald Aylmer Fisher, un estadístico/matemático y biólogo británico quien dijo que «una de cada veinte (1/20=0.05) oportunidades representa un suceso muestral inusual.

Grados de libertad $G1= (f-1) (c-$

G1	Grado de libertad
F	Filas
C	Columnas

Para aceptar o rechazar la hipótesis, luego de los cálculos realizados se aplicará el criterio que si ji cuadrado calculado es mayor o igual que la ji cuadrado tabla se acepta la hipótesis de trabajo y se rechazara la hipótesis nula.

4.3.1. Hipótesis

La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, si incrementará el nivel de confidencialidad en los sistemas informáticos.

4.4. Identificación de variables

Variable Independiente: Aplicación de la tecnología java (JSP).

Variable Dependiente: Incrementará el nivel de confidencialidad en los sistemas informáticos.

Tabla 12-4 Tabla de contingencia con las preguntas más alineadas a la investigación del cuestionario propuesto.

N°	Pregunta	Alternativas		Total
		SI	NO	
1	¿Es una ventaja de JAVA ser una tecnología multiplataforma, es decir que funcione en prácticamente cualquier dispositivo, servidor o sistema operativo?	19	11	30
2	¿Incorpora JAVA mecanismos o funciones para ofrecer seguridad a sus aplicaciones?	20	10	30
7	¿La tecnología JAVA dispone de mecanismos seguros y compatibles para el intercambio de información con otras tecnologías?	15	15	30
9	¿Se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project*) y la tecnología JAVA?	21	9	30
10	¿Existe flexibilidad, escalabilidad en la tecnología JAVA para el desarrollo de aplicaciones web permitiendo mantener una estructura compacta además de la integridad de la información?	22	8	30
Subtotal		97	53	150

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Cálculo de las frecuencias Esperadas

Cuando tenemos un solo criterio de clasificación dividido en varias categorías el cálculo de las frecuencias teóricas o esperadas es sencillo:

$$Fe = N/K$$

N= número de eventos

K=número de oportunidades

En este caso todos tienen la misma oportunidad

Cuando hay dos criterios de clasificación como en nuestro caso (cuadros de doble entrada).

Las frecuencias teóricas de cada casilla son iguales al producto de las sumas marginales dividido por el número total de sujetos.

En el caso de dos categorías con dos niveles de clasificación (podrían ser más) tendríamos:

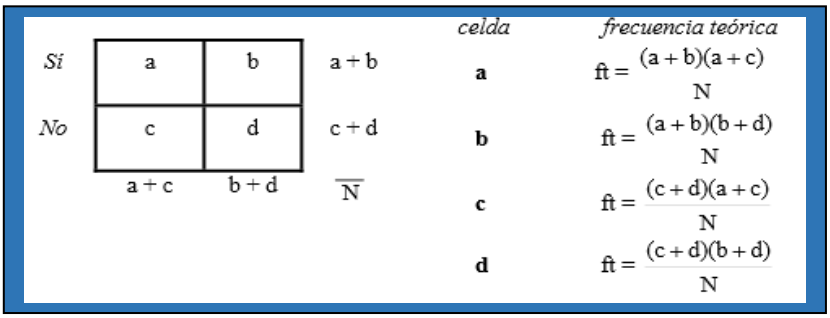


Figura 1-4 Categorías con niveles de clasificación

Fuente: Morales Vallejo, Pedro (2008) Estadística aplicada a las Ciencias Sociales.

Cálculo de frecuencias Esperadas con respuesta afirmativa

Tabla 13-4 Cálculo de Frecuencia Esperada

N°	Pregunta	Alternativas		Frecuencia Esperada (Fe) Positivas
		SI	NO	
1	¿Es una ventaja de JAVA ser una tecnología multiplataforma, es decir que funcione en prácticamente cualquier dispositivo, servidor o sistema operativo?	19	11	7.8
2	¿Incorpora JAVA mecanismos o funciones para ofrecer seguridad a sus aplicaciones?	20	10	7
7	¿La tecnología JAVA dispone de mecanismos seguros y compatibles para el intercambio de información con otras tecnologías?	15	15	7.2
9	¿Se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project*) y la tecnología JAVA?	21	9	8.6
10	¿Existe flexibilidad, escalabilidad en la tecnología JAVA para el desarrollo de aplicaciones web permitiendo mantener una estructura compacta además de la integridad de la información?	22	8	15.9

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Tabla 14-4 Cálculo de frecuencias Esperadas con respuesta negativa

N°	Pregunta	Alternativas		Frecuencia Esperada (Fe) Negativas
		NO	SI	
1	¿Es una ventaja de JAVA ser una tecnología multiplataforma, es decir que funcione en prácticamente cualquier dispositivo, servidor o sistema operativo?	11	19	4.2
2	¿Incorpora JAVA mecanismos o funciones para ofrecer seguridad a sus aplicaciones?	10	20	5
7	¿La tecnología JAVA dispone de mecanismos seguros y compatibles para el intercambio de información con otras tecnologías?	15	15	4.8
9	¿Se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project*) y la tecnología JAVA?	9	21	3.4
10	¿Existe flexibilidad, escalabilidad en la tecnología JAVA para el desarrollo de aplicaciones web permitiendo mantener una estructura compacta además de la integridad de la información?	8	22	2

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Tabla de Contingencia

Tabla 15-4 Cálculo de Chi Cuadrado calculado

Pregunta	**Fo**	**Fe**	**Fo-Fe**	**$(Fo-Fe)^2$**	**$\frac{(Fo-Fe)^2}{Fe}$**
¿Es una ventaja de JAVA ser una tecnología multiplataforma, es decir que funcione en prácticamente cualquier dispositivo, servidor o sistema operativo?	21	7.8	13.2	174.24	22.33
¿Incorpora JAVA mecanismos o funciones para ofrecer seguridad a sus aplicaciones?	20	7	13	169	24.14
¿La tecnología JAVA dispone de mecanismos seguros y compatibles para el intercambio de información con otras tecnologías?	15	7.2	7.8	60.84	8.45
¿Se puede obtener aplicaciones web completamente seguras si se aplican todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project*) y la tecnología JAVA?	21	8.6	12.4	153.76	17.87
¿Existe flexibilidad, escalabilidad en la tecnología JAVA para el desarrollo de aplicaciones web permitiendo mantener una estructura compacta además de la integridad de la información?	22	15.9	6.1	37.21	2.3
¿No es una ventaja de JAVA ser una tecnología multiplataforma, es decir que funcione en prácticamente cualquier dispositivo, servidor o sistema operativo?	9	4.2	4.8	23.04	-5.48

¿JAVA no incorpora mecanismos o funciones para ofrecer seguridad a sus aplicaciones?	10	5	5	25	-5
¿La tecnología JAVA no dispone de mecanismos seguros y compatibles para el intercambio de información con otras tecnologías?	15	4.8	10.2	104.04	-21.67
¿No se puede obtener aplicaciones web completamente seguras así se apliquen todas las técnicas y normas de seguridad que recomienda organismos como OWASP (*Open Web Application Security Project*) y la tecnología JAVA?	9	3.4	5.6	31.36	-9.22
¿No existe flexibilidad, escalabilidad en la tecnología JAVA para el desarrollo de aplicaciones web permitiendo mantener una estructura compacta además de la integridad de la información?	8	2	6	36	-18
	TOTAL JI CUADRADO CALCULADA				15.72

Fuente: Encuesta Estructurada

Elaborado por: Fonseca, Elvis 2020

Chi-Cuadrado Calculado $X^2c = 15.72$

Ahora Calculamos Chi-Cuadrado Tabla

Grado de libertad

Gl: (f-1) (c-1)

f= número de filas y

c = número de columnas

(5-1) (2-1)

(4) (1) = 4

Gl: 4

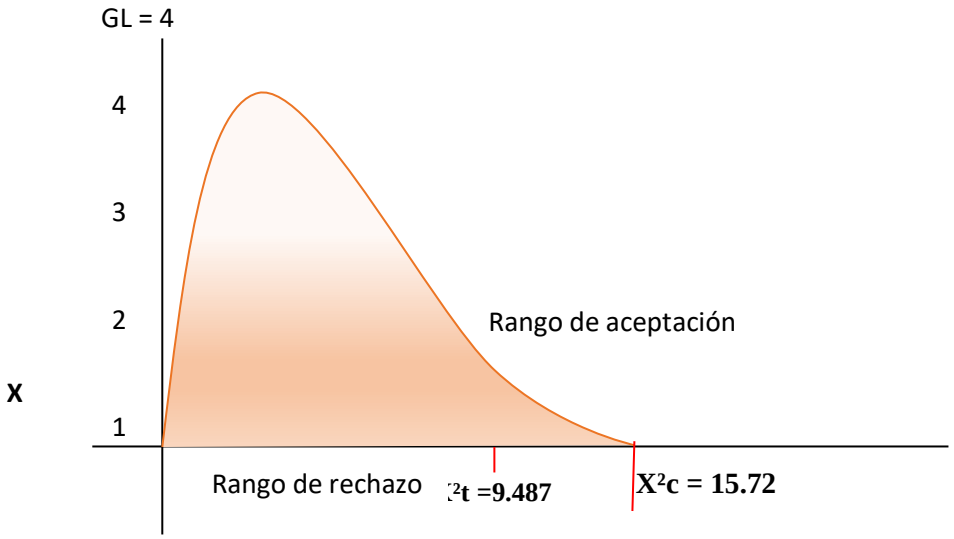
Nivel de confianza=0.05

Chi-Cuadrado Tabla.

X^2t = **9.487** Valor encontrado en la tabla de probabilidad Chi Cuadrado (Anexo F)

$X^2c = 15.72 > X^2t = 9.487$

De acuerdo con estos resultados pudo comprobarse que el chi-cuadrado calculado es mayor que el chi-cuadrado tabla, por lo cual se acepta la Hipótesis de trabajo y se rechaza la Hipótesis nula, Es decir **"**La aplicación de la tecnología java (JSP) para el desarrollo de sistemas web dinámicos seguros, si incrementará el nivel de confidencialidad en los sistemas informáticos**". (**Fonseca, 2020**)**



Gráfio de la Comprobación de la Hipótesis
Elaborado por: Fonseca, Elvis 2020

CONCLUSIONES

- Los criterios de seguridad propuestos por The Open Web Application Security Project (OWASP)a considerar para el desarrollo de aplicaciones web dinámicas son: Disponibilidad, Autenticidad, Integridad, Confidencialidad, Trazabilidad de los datos a nivel del cliente, servidor, aplicación y comunicación siendo JSP la tecnología que cumple con un 93% de estos parámetros por encima de las tecnologías ASP.Net con un 50% y PHP 86%.

- La metodología CRAIG LARMAN aplicada al sistema de Posgrado de la UNACH considera un modelo Orientado a Objetos Interactivo e Incremental, utilizado por Microsoft, HewlettPackard, Oracle o IBM, así como grupos de analistas y desarrolladores en sistemas nuevos como es el caso de SYSPOSGRADO ya que define una serie de actividades tales como: Diseño del software, Generación de código, Prueba del software, y cumple con las fases de Planificación y especificación de requisitos, Análisis, Diseño e Implementación.

- La aplicación de técnicas de seguridad tales como: encriptación de contraseñas, bloqueo de cuentas al superar el número de intentos permitidos, confirmación de logeos vía MSN y correos electrónicos, sesiones, validación al ingreso de datos, usuarios con privilegios restringidos a nivel de base de datos disminuye la vulnerabilidad al sistema web del instituto de Posgrado.

- La investigación realizada en la tesis, puede ser útil para ser implementado en cualquier medio organizacional, considerando aspectos tales como**:** balancear riesgo y usabilidad, filtrar entradas, evitar ataques SQL Injection, Cross-SiteRequestForgeries, Ataques URL de tipo Semántico, además de ser un sistema open source que ayudaráal desenvolvimiento de Instituciónes de Educación Superior en procesos relacionados con servicios de Posgrado.

RECOMENDACIONES

- La tecnología JSP simplifica el proceso de construcción de sitios web dinámicos seguros, es necesario realizar una buena definición de requerimientos del sistema y utilizar la metodología CRAIG LARMAN para el desarrollo del sistema web, haciendo énfasis que la seguridad y escalabilidad son características que un producto software debe mantener, independientemente de la tecnología que se aplique.

- En la elaboración de sistemas web para la gestión de información se sugiere realizar validaciones a nivel de usuarios del sistema, mediante funciones y procedimientos que aporten seguridad en la interactividad usuario – sistema mediante la encriptación de contraseñas, restricciones de privilegios a las diferentes cuentas de usuarios, validación de datos con java script, bloqueos de usuarios no identificados.

- Se recomienda a la Universidad Nacional de Chimborazo la utilización del SysPosgrado, para con ello agilizar el flujo de trabajo en el Instituto de Posgrado reduciendo el tiempo de ejecución de los procesos, haciendo uso eficiente del recurso tiempo.

- Integrar la infraestructura informática con la aplicación y procesos administrativos en el Instituto de Posgrado de la Universidad Nacional de Chimborazo.

BIBLIOGRAFÍA

Al-Waisy, R. (2015). A Fast and Accurate Iris Localization Technique for Healthcare Security System. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.

Ávila, C. (2012). Aplicaciones de la Biometría a la Seguridad. Obtenido de http://www.criptored.upm.es/descarga/TASSI2012_CarmenSanchez.pdf

Cantoni, V. (2017). Capítulo 9 - Autenticación biométrica para acceder a áreas controladas a través del seguimiento ocular. Reconocimiento humano en entornos sin restricciones.

Castro, C. (2017). Modelo de seguridad para garantizar. Ecuador. Recuperado el septiembre de 2019, de http://dspace.espoch.edu.ec/bitstream/123456789/7842/1/20T00952.pdf

Chiavenato, I. (2018). Administración de recursos humanos. Obtenido de http://repositorio.utc.edu.ec/bitstream/27000/458/1/T-UTC-1027.pdf

CMITECH. (2019). CMI-TECH. Obtenido de https://www.cmi-tech.com/wp-content/uploads/2018/06/cmitech-data_sheet-ef-45-2019.pdf

Cohn, M. (2007). Biometrics: Key to securing consumer trust. Biometric Technology Today.

Comparativa Jsp, Php y Asp. (2016). Comparativa Jsp, Php y Asp. Obtenido de https://www.buenastareas.com/ensayos/Comparativa-Jsp-Php-y-Asp/2792878.html

Conrado, E. (2015). Desarrollo de una aplicación web de administración de clientes y desarrollo de un plan de ejercicios de entrenamiento físico personalizado, y módulo de facturación del gimnasio "absolut gym". Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/10107/6/UPS%20-%20ST001637.pdf

Cortés, J., y Medina, F. (2010). Sistemas de seguridad basados en biometría. obtenido de security systems based on biometrics: https://www.redalyc.org/pdf/849/84920977016.pdf

Cuello, M. (2016). Análisis de las principales tecnologías multiplataforma para aplicaciones web. Aplicado al Sistema de seguimiento de graduados y egresados de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo. Obtenido de http://dspace.unach.edu.ec/bitstream/51000/1630/1/UNACH-EC-ISC-2016-0010.pdf

Ejaz, S. (2018). Performance Comparison of Partition Based Clustering Algorithms on Iris Image Preprocessing. 2017 2nd International Conference on Electrical & Electronic Engineering (ICEEE).

Florian, L. (2006). Reconocimiento del iris. Tópicos especiales en procesamiento gráfico.

Gumaei, A. (2019). Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation. Journal of Parallel and Distributed Computing

Hernàndez, J. C. (2016). Autenticación biométrica a través de huellas digitales e iris en una empresa industrial. Obtenido de http://ri.uaemex.mx/bitstream/handle/20.500.11799/64996/JUAN%20CARLOS%20HERN%C3%81NDEZ%20REYES-split-merge.pdf?sequence=3&isAllowed=y

Instituto Nacional De Ciberseguridad. (2016). Tecnologías biométricas aplicadas a la ciberseguridad. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Menotti, D. (2015). Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. IEEE Transactions on Information Forensics and Security.

NUO. (2015). Reconocimiento de iris y escaneo de retina. Obtenido de Reconocimiento de iris y escaneo de retina: https://nuoplanet.com/blog/reconocimiento-de-iris-y-escaneo-de-retina/

Pricop, E. (2019). Biometrics the secret to securing industrial control systems. Biometric Technology Today.

Proença, H. (2018). A Reminiscence of "Mastermind": Iris/Periocular Biometrics by "In-Set" CNN Iterative Analysis. IEEE Transactions on Information Forensics and Security.

Rajput, G. (2018). Iris Biometric Technique for Person Authentication Based on Fusion of Radon and 2D Multi-Wavelet Transform. 2018 International Conference On Advances in Communication and Computing Technology (ICACCT).

Ratha, J. (2001). Enhancing security and privacy in biometrics-based. IBM Systems Journal.

Sarmiento, B. (2017). Nuevas Tendencias del Software. Obtenido de http://nuevastendsw.blogspot.com/2010/03/cuadro-comparativo.html

Sierra, A. (2018). Comparative Analysis between ASP.NET and PHP. Obtenido de file:///C:/Users/1410107-C158/Desktop/Dialnet-AnalisisComparativoEntreASPNETYPHP-6779622.pdf

Vanthana, S. (2015). Iris authentication using Gray Level Co-occurrence Matrix and Hausdorff Dimension. 2015 International Conference on Computer Communication and Informatics (ICCCI).