ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

GENERACIÓN DE POLÍTICAS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE

RENNY GEOVANNY MONTALVO ARMIJOS

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 Seguridad Telemática

RIOBAMBA - ECUADOR
JULIO 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado "**GENERACIÓN DE POLÍTICAS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE**", de responsabilidad del Sr. Renny Geovanny Montalvo Armijos, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

ING. MIGUEL DUQUE MSC. **PRESIDENTE**	FIRMA
ING. FERNANDO MEJIA MSC. **DIRECTOR**	FIRMA
ING. VINICIO RAMOS VALENCIA MSC **MIEMBRO**	FIRMA
ING. OSWALDO MARTINEZ MSC. **MIEMBRO**	FIRMA

Riobamba, julio de 2017

DERECHOS INTELECTUALES

Yo, Renny Geovanny Montalvo Armijos, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

FIRMA

0602750341

DECLARACIÓN DE AUTENTICIDAD

Yo, Renny Geovanny Montalvo Armijos, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría, y que los resultados del mismo, son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica, de los contenidos de este proyecto de investigación de maestría.

Riobamba, julio de 2017

_____

Renny Geovanny Montalvo Armijos

FIRMA

0602750341

DEDICATORIA

Este trabajo va dedicado a mi esposa, Paola Manya, quien ha sabido brindarme el apoyo necesario, quien compartió conmigo todo el esfuerzo realizado mientras duró el curso de los estudios y se desarrollaba este trabajo de investigación, a mi madre Magdalena Montalvo, a mis hermanos y sin dejar de lado a los amigos, quienes apoyaron de diferentes maneras para que este reto llegue a feliz término.

Renny Montalvo

AGRADECIMIENTO

Es necesario agradecer sinceramente, a todos los maestros, quienes sin restricciones compartieron sus conocimientos, especialmente quienes conformaron el tribunal de la tesis y fueron un gran aporte para la realización de la investigación, a la Escuela Superior Politécnica de Chimborazo, por haber permitido que este programa de maestría culmine con éxito. A mi esposa, padres y hermanos, quienes compartieron su tiempo para poder culminar los estudios. Y, no puedo dejar de agradecer a mis amigos Christian y Fabián, equipo de arduo trabajo y con quienes compartimos gratos momentos durante el tiempo de estudios.

Renny Montalvo

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

El objetivo fue generar políticas para la gestión de riesgos de seguridad en el desarrollo de software en el Consejo de la Judicatura, la investigación empieza al generar un ambiente de pruebas en el que se encuentran configurados en el mismo servidor dos aplicaciones prototipo, los mismos que se configuran, una aplicando las políticas generadas, y otra sin aplicar las políticas. Como resultado de la investigación, al aplicar las políticas y utilizarlas durante la etapa de desarrollo de software, se logró reducir del 39,2% al 12,5% en las pruebas realizadas, para poder seguir mitigando las vulnerabilidades existentes en las aplicaciones desarrolladas. Al aplicar las políticas hacia un prototipo de prueba, antes de ser puesto en producción, se logró observar que, sin las políticas de seguridad, la aplicación es menos segura que cuando se logra aplicar las políticas. Se recomienda al Consejo de la Judicatura, aplicar a través de la Subgerencia de Desarrollo, las políticas generadas para gestionar y mejorar la seguridad de sus activos informáticos sensibles, logrando mejora y mitigar las vulnerabilidades existentes en sus aplicativos.

Palabras Clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INFORMÁTICA>, <SEGURIDAD TELEMÁTICA>, <DESARROLLO DE SOFTWARE>, <SEGURIDAD DE LA INFORMACIÓN>

ABSTRACT

The objective was to generate policies for security risk management in software development at the National Judicial Council, the investigation begins by generating a test environment in which two prototype extensions are configured on the same server, the same ones are configured, one applying the policies generated and another without applying the policies. As a result of the research, when applying the policies and using them during the software development stage, it was possible to reduce from 39.2% to 12.5% in the tests performed, in order to continue to mitigate the existing vulnerabilities in the applications developed. When applying the policies toward a test prototype, before being put into production, it was observed that, without security policies, the application is less certain when policies are implemented. It is recommended that the Judiciary Council apply, through the development Sub-Management, the policies generated to manage and improve the security of its sensitive computer assets, and to improve and mitigate vulnerabilities in its applications.

Key Words: <ENGINEERING TECHNOLOGY AND SCIENCES>, <INFORMATICS>, <TELEMATIC SECURITY>, <SOFTWARE DEVELOPMENT>, <INFORMATION SECURITY>

CAPÍTULO I

1 MARCO REFERENCIAL

1.1. Antecedentes

Las diferentes metodologías para evaluar y gestionar el riesgo, son herramientas que no son muy utilizadas para proceder a desarrollar Software, esto, puede ser por la dificultad, desconocimiento o su poca difusión, etc.

Dentro del ámbito de los sistemas de gestión de la seguridad de la información nos encontramos con diferentes herramientas tales como: las Normas ISO 27005 (Gestión de la seguridad de la información), OWASP (Open Web Application Security Project), metodologías tales como MAGERIT, CORAS, OCTAVE, entre otros.

Al referirse a la norma ISO 27005, hay que tomar en consideración que, la norma en sí, brinda diferentes directrices que se deben utilizar para la gestión de los riesgos, tomando en consideración los requisitos establecidos, particularmente para un Sistema de Gestión de la Seguridad de la Información (SGSI), de acuerdo con la norma ISO/IEC 27001.

Se puede establecer que, la norma no brinda metodología alguna para la Gestión de los Riesgos de la Seguridad en la Información en alguna empresa, debiendo ser ésta, la que genere sus propias políticas de acuerdo al alcance que se le quiera otorgar.

Cuando se habla acerca de MAGERIT, hace referencia a una de las metodologías más utilizadas para este propósito, el mismo que permite realizar diferentes actividades, las mismas que se encaminan a una mejor evaluación de los riesgos.

El desarrollo de aplicaciones de software ha evolucionado en las últimas décadas, de una manera que, las empresas en la actualidad necesitan de por lo menos una aplicación que les permita reducir tiempos, costos, y, que también logre mantener datos históricos que puedan servir de control para saber con exactitud la información almacenada.

Se ha venido desarrollando software a nivel nacional e internacional, de una manera inadecuada, sin respetar las diferentes etapas del ciclo de vida, y es por eso que, se ha desencadenado ataques

a las empresas, a través de las aplicaciones que han sido creadas para sim mismas, en particular aquellas que se encuentran presentes en la web.

Existen diferentes Estándares, Normas, Modelos y, Métodos a seguir, los mismos que, son pasados por alto, haciendo que esto provoque riesgos que en cualquier momento la información contenida en las bases de datos empresariales sea violentada y extraída con diferentes finalidades.

De acuerdo con el método de la investigación en ciencias de diseño, las construcciones deben ser evaluadas por la totalidad, la sencillez, la elegancia, la comprensibilidad y facilidad de uso.

Encontrar los activos y el valor de los activos en riesgo es una parte importante de la evaluación del riesgo. Los Token son activos, y su valor en riesgo puede contribuir a los riesgos de seguridad y privacidad.

Esto ha generado una grave incidencia de riesgos de seguridad de la información, los mismos que, dan paso a vulnerabilidades en el momento de desarrollar software, poniendo en riesgo los diferentes activos informáticos de la empresa, puesto que, no se toman en consideración los diferentes elementos que puedan provocar fallos de seguridad, ataques externos, que violenten la seguridad de la información de la empresa, fuga de información y otro tipo de atentados contra la confidencialidad dentro de la empresa.

Este tipo de ataques, deberían mitigarse para lograr un mayor índice de seguridad de la información, permitiendo mantener un mejor nivel de seguridad de la información empresarial, tomando en consideración que no existe sistema 100% seguro.

El Consejo de la Judicatura de Tungurahua no ha estado exento de los riesgos ni vulnerabilidades que se mencionan anteriormente, tomando como antecedente que en el año 2014 en el mes de noviembre los servidores sufren un ataque, dejando abajo todos los servicios que se brindan a través de los portales web de la judicatura.

Un nuevo ataque es registrado en el mes de febrero del año 2015, de la misma manera se pierde la funcionalidad de los servicios que brinda el Consejo de la Judicatura al público, en esta ocasión no fueron únicamente los servicios web, al haber sido efectuado el ataque en horas laborables, también se caen los servicios para los usuarios internos, quedándose sin poder ejecutar ninguna de las tareas de justicia que brinda la institución.

Al no existir políticas que establezcan un nivel de seguridad que se puedan aplicar para mitigar los riesgos de quedar vulnerabilidades expuestas y que sean aprovechadas por los atacantes, y dada la delicadeza de la información que se maneja en la institución, se justifica el desarrollo del presente proyecto.

1.2. Problematización

1.2.1. Formulación del problema.-

¿De qué manera contribuye la generación de políticas para evaluar y administrar los riesgos de seguridad en el desarrollo de software?

1.2.2. Sistematización del problema.-

¿Cuáles son las políticas existentes en la seguridad de los sistemas de información para el desarrollo de software?
¿Cuáles son las coincidencias entre las Normas ISO 27001, 27002, 27005 y OWASP?
¿Cómo evaluar y administrar los riesgos de seguridad de la información?
¿Qué políticas se pueden generar para mejorar la seguridad de la información durante del desarrollo de software?

1.3. Justificación

1.3.1. Justificación Teórica

Como se ha establecido en los estudios realizados y, según el avance desmesurado que tiene la tecnología y su uso en los diferentes ambientes empresariales, se ha visto la necesidad, de identificar, etiquetar y, mantener la seguridad de ellos.

Al momento de desarrollar software de diferente tipo, no se toma en consideración varios aspectos, llámese esto: definición de objetivos, análisis de requerimientos y su viabilidad, diseño general, diseño detallado. Todos estos puntos son muy importantes para que, luego de cumplidas todas las etapas, momento en el que, ya debemos tener muy bien establecidos todos los aspectos a ejecutar dentro de la siguiente etapa que es la programación.

En la actualidad, a las diferentes fases del desarrollo de software, no se le da la importancia que se les debe dar, puesto que, se lo realiza sin llevar la investigación necesaria para, poder poner a

buen recaudo la información empresarial que, es uno de los activos más valiosos y como activo valioso, se lo debe cuidar de la mejor manera, y así mejorar la productividad de las empresas.

Los estudios anteriores acerca de los riesgos de seguridad y vulnerabilidades, han demostrado que, los mayores efectos de fuga de información y ataques hacia los activos informáticos de una empresa, por parte de quienes realizan estas actividades que pueden llevarlas a la quiebra, son aquellos que se presentan durante la etapa de programación, porque no se toma en consideración, ningún modelo existente, obviando pasos que no se pueden obviar.

Sin embargo, el Consejo de la Judicatura de Tungurahua, al no contar con políticas y prácticas que sean fáciles de acceder u obtener para desarrollar software seguro, y siendo la información que almacena muy importante para los usuarios en todo el país, es necesario realizarlas y socializarlas, para procurar mantener lo más seguro posible los activos sensibles que tiene la Judicatura.

Estos deberían estar bien protegidos debido a la sensibilidad de los mismos en manos que no deberían estar, porque la manipulación indebida de la información almacenada, puede cambiar la vida de quienes se encuentren inmersos en los diferentes casos de justicia.

Es por eso que, se ha planteado, realizar las políticas de evaluación y administración de los riesgos (gestión de riesgos), que, sin ser una camisa de fuerza, deberán llegar a ser una guía, la cual, permitirá desarrollar software seguro y, sin ser la solución definitiva para evitar ataques, sustracción de información, y otras vulnerabilidades, nos permitirá aplacarlas, para poder mantener con menor riesgo los activos sensibles de la institución.

Utilizando las metodologías existentes para gestión de los riesgos de la seguridad de la información, se podrán determinar políticas que permitan a los desarrolladores realizar el trabajo de mejor manera, involucrándose directamente en la seguridad de los activos existentes en la empresa, integrando un equipo de trabajo con las diferentes áreas que la conforman y, volviéndose una parte muy necesaria, sin descuidar la mitigación de los riesgos.

1.3.2. Justificación Metodológica

La metodología que se va a utilizar en la presente investigación es la metodología MAGERIT, es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.

Otra metodología que se va a utilizar es la metodología CORAS (Construct a platform for Risk Analysis of Security critical system) Construir una plataforma para el análisis de riesgos del sistema de seguridad crítica, la misma que proporciona:

Una metodología de análisis de riesgos basado en la elaboración de modelos, basados fundamentalmente en entrevistas con los expertos.

- Un lenguaje gráfico basado en UML
- Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos, que permite su gestión y reutilización

Y adicional a estas metodologías también la presente investigación estará basada en la metodología OCTAVE, (Operationally Critical Threat, Asset and Vulnerability Evaluation)

- Metodología de análisis de riesgos (seguridad de TI)
- Su enfoque se basa en que la organización sea capaz de:
    - Dirigir y enfocar sus evaluaciones de riesgos
    - Tomar decisiones con base en los riesgos
    - Proteger los activos claves de información.
    - Comunicar de manera efectiva la información clave de seguridad
- Coadyuvante en el aseguramiento de la continuidad del negocio
- Definición del riesgo y amenazas que se basan en los activos críticos
- Estrategias de recopilación y mitigación de riesgos a través de prácticas
- Recopilación de datos en función de los objetivos
- Base para la mejora de la seguridad.

1.3.3. Justificación Práctica

Para poder determinar una buena seguridad de la información como uno de los activos informáticos que tiene una empresa, primero se debe tomar en consideración que: existen varias maneras de vulnerar las seguridades de un sistema de información, llámese esto, ddns, sqlinjection, los que en muchas de las ocasiones por no decir en la mayoría, son provocados por la falta de controles en el momento de desarrollar el software.

Para poder brindar una buena protección de los sistemas de información, el primer paso será, el presentar al público que utiliza las aplicaciones creadas por la organización, una aplicación de Software que nos permita mantener un nivel de seguridad que no siendo el 100% segura, por lo menos retrase los intentos de vulnerar las seguridades organizacionales.

En este sentido, se realizará un estudio de las políticas existentes, normas ISO 27001, 27005 y OWASP; además de establecer las herramientas para evaluar y administrar los riesgos de seguridad de la información, generando con esto las políticas a implementarse en el desarrollo de un prototipo con y sin estas políticas investigadas.

1.4. Objetivos

1.4.1. Objetivo General

Generar políticas para la gestión de riesgos de seguridad en el desarrollo de software

1.4.2. Objetivos Específicos

- Evaluar las políticas existentes para seguridad de los sistemas de información a través del desarrollo de software
- Definir las coincidencias y discrepancias entre las Normas ISO 27001, 27005 y OWASP
- Establecer las herramientas para evaluar y administrar los riesgos de seguridad de la información
- Generar las políticas para mejorar la seguridad de la información por medio del desarrollo de software
- Realizar un prototipo de prueba, utilizando las políticas de seguridad investigadas y sin políticas de seguridad

1.5. Hipótesis

La generación de políticas para gestionar los riesgos de seguridad de la información, permitirán mejorar la mitigación de vulnerabilidades existentes en el desarrollo de software.

CAPÍTULO II

2 REVISIÓN DE LITERATURA

2.1. Metodologías para la evaluación de Riesgos

La evaluación de riesgos, es el primer paso que se debe dar, en procura de obtener las diferentes vulnerabilidades que se puedan presentaren una entidad.

Para realizar la evaluación de los riesgos, existen diferentes metodologías, entre las más conocidas que se pueden encontrar se mencionan las siguientes:

- Metodología MAGERIT
- Metodología OCTAVE
- Metodología CORAS
- Metodología NIST SP 800-30

Las mismas que serán analizadas más adelante

2.1.1. Antecedentes

Dentro del ámbito de la evaluación de Riesgos de Seguridad de la Información, se han realizado varios estudios anteriormente, enfocado a los Riesgos de Seguridad en la Nube (Choo, 2014).

Varios autores al realizar su trabajo "**DISTRIBUCIÓN Y COORDINACIÓN DE ACTIVOS CON ADVERTENCIAS DINÁMICAS EN LA GESTIÓN DE RIESGOS"**, muestra un Framework para poder realizar un plan estratégico para la distribución de los activos de una empresa de ferrocarriles, que presenten advertencias dinámicas en la gestión de los riesgos, en el departamento de mecanismo y control de vías, gestionando los riesgos para la distribuir los activos evitando riesgos cada vez más grandes que puedan causar accidentes. (Yifeng et al., 2012)

2.1.2. Cómo evaluar riesgos

Para evaluar riesgos tenemos varias metodologías, las mismas que serán descritas y utilizadas en el transcurso del presente trabajo, para listar las más conocidas tenemos las siguientes:

- Metodología MAGERIT
- Metodología OCTAVE
- Metodología CORAS
- Metodología NIST SP 800-30

Además de las que hemos listado, podemos mencionar el trabajo científico "**Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios**" (Castro & Bayona, 2011), el mismo que será un aporte importante, puesto que se basa en las Normas ISO que tratan acerca de los diferentes riesgos de seguridad informática que podrían presentarse en una empresa, y como realizar su evaluación, se lo tratará más adelante.

Para poder evaluar los riesgos, se debe tomar en consideración, tanto su frecuencia como su incidencia y el impacto que tendría su vulneración, de acuerdo a estos parámetros que son los que más nos podrían afectar con los activos más importantes que tienen las empresas y que son los activos informáticos.

2.1.3. Enfoques de las metodologías de evaluación de riesgos

Como ya se explicó anteriormente, existen diferentes metodologías o estándares para evaluar los riesgos de la seguridad de la información, desglosándose en:

- Cuantitativo
- Cualitativo

2.1.3.1. Enfoque Cuantitativo del análisis de riesgos

"Este enfoque emplea dos elementos fundamentales, la probabilidad de que se produzca un evento y el impacto que ocasionaría la probable pérdida en caso de que ocurra el citado evento.

El enfoque cuantitativo de análisis de riesgos consiste en la obtención de un valor a partir del producto de estos elementos. La forma de calcularlo, para un evento dado, es realizando la multiplicación del valor de la pérdida potencial por el valor de la probabilidad de ocurrencia. De esta manera es prácticamente concreto y posible valorar los eventos y calcular el riesgo a fin de tomar las decisiones correspondientes.

Son numerosas las organizaciones que han adoptado y aplicado con éxito el análisis de riesgo cuantitativo. De hecho se recomienda fuertemente comenzar con un análisis de riesgo cuantitativo y luego, si el negocio lo amerita, hacer un análisis cualitativo." (Eterovic & Pagliari, n.d.)

Habiendo determinado los enfoques que se le da al análisis del riesgo, se describe a continuación las principales características de las metodologías MAGERIT, OCTAVE y MEHARI.

2.1.3.2. MAGERIT

MAGERIT, tiene la posibilidad de realizar lo siguiente:

- Análisis de Riesgos
- Gestión de Riesgos

Los principales elementos que utiliza MAGERIT son:

- *Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio.*
- *Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.*
- *Escala alternativa de estimación del riesgo.*
- *Catálogos de amenazas*
- *Catálogos de medidas de control* ("Seguridad Informatica - MAGERIT," n.d.; Syalim, Hori, & Sakurai, 2009)

2.1.3.3. OCTAVE

- Construcción de los Perfiles de Amenazas Basados en Activos
- Identificación de la Infraestructura de Vulnerabilidades
- Desarrollo de Planes y Estrategias de Seguridad

Las actividades más relevantes de OCTAVE se muestran a continuación.

- *Realiza medidas de probabilidad dentro de un rango de frecuencias.*
- *Realiza el análisis del límite entre niveles de probabilidad*. (Mera D., Villamarín C., Arteaga L., & Sosa R., n.d.)

2.1.3.4. MEHARI

La metodología MEHARI comprende:

- Diagnóstico de Seguridad
- Análisis de los Intereses Implicados por la Seguridad
- Análisis de Riesgos

Del estudio de esta metodología extraemos sus principales elementos:

1. *Niveles de categorías de controles*
2. *Niveles de calidad de los servicios de seguridad*
3. *Evaluación de la calidad del servicio por medio de cuestionarios*
4. *Tabla modelo de impactos* (CLUSIF, 2010)

2.1.3.5. CORAS

CORAS es una metodología basada en el modelo para análisis de riesgos. La meta de CORAS es desarrollar una mejor metodología para el análisis de riesgos de seguridad de sistemas de IT críticos de una manera más precisa y efectiva. Esto prevendrá que las compañías, utilicen grandes sumas en problemas de seguridad, y al utilizar esta metodología en un período más temprano, se verá que tipos de riesgos existen, y cómo tratarlos.

La metodología CORAS puede ser dividida en:

- *Identificar el contexto: Caracterizar el objetivo con los análisis, cual es el enfoque y el alcance del análisis. ¿Qué pérdidas puede tolerar el cliente, ya que siempre estará involucrado un riesgo?*
- *Identificar los riesgos: Identificar las amenazas a los activos como por ejemplo lluvia de ideas, y también identificar sus vulnerabilidades.*
- *Estimar el nivel del riesgo, evaluar los riesgos: No todos los riesgos pueden ser eliminados, y tenemos que decidir cuál es el riesgo que necesita tratamiento. Tenemos que conocer acerca de los niveles del riesgo.*
- *Tratar los riesgos: identificar el tratamiento de los riesgos indeseados. Evaluar y priorizar diferentes tratamientos* (Yaqub, 2007)

2.1.4. Determinación de la metodología base

De acuerdo a los estudios realizados, se puede determinar que la metodología que más podrá ayudar a la evaluación y gestión de riesgos de seguridad de la información, por contar con la mayoría de elementos que nos permitan evaluar y gestionar de mejor manera los riesgos antes mencionados, es la metodología MAGERIT.

No se descarta también, utilizar elementos existentes en otras metodologías que se hayan tomado en cuenta en MAGERIT, en vista de la necesidad de desarrollar Software más seguro de lo que se desarrolla en la actualidad

2.2. Normas de Seguridad

Dentro de los aspectos que se deben considerar para poder realizar la gestión de riesgos existen varias normas de seguridad, las mismas que, serán la base para el presente trabajo, con el estudio de ellas, se pretende establecer las mejores políticas que se deberán utilizar por desarrolladores, para que el producto que se vaya a entregar, reduzca de mejor manera las vulnerabilidades que puedan significar pérdidas de los activos (información) en una empresa.

Para ello, se realizarán los estudios de lo siguiente:

- Estudio de las Normas ISO 27001
- Estudio de las Normas ISO 27002
- Estudio de las Normas ISO 27005
- Estudio de las OWASP

2.2.1. Estudio de las Normas ISO 27001

La parte más importante que podemos establecer de esta Norma, es el análisis y la gestión del Riesgo, basado en los procesos del negocio y los servicios de TI (Carlos Manuel Fernández Coordinador de TIC & de AENOR, n.d.), en su artículo "**La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información**".

De acuerdo con Fernández, esta norma de mejora continua, es la más adecuada para poder evaluar el Riesgo, tanto físico como el lógico, que es el que se va a tratar de proteger con el presente trabajo, puesto que, lo que se va a presentar serán las políticas que rijan el Desarrollo de Software.

La Norma ISO/IEC 27001, permite ver al Sistema de Gestión de Seguridad de la Información, como una de las partes más importantes para proteger los activos de la organización, englobando e involucrando a todas las áreas que se encuentran formando parte de la misma. (Anexo 1)

2.2.1.1. Enfoque del Proceso

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a) Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) Monitorear y revisar el desempeño y la efectividad del SGSI; y
d) Mejoramiento continuo, en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

En la figura 1-2. (Comité Técnico Conjunto ISO/IEC JTC 1 Tecnología de la información & Subcomité SC 27 Técnicas de seguridad TI, n.d.), se puede apreciar el ciclo en el cual se basa esta norma para la Seguridad de la información, recalcando que ésta se aplica para un SGSI.

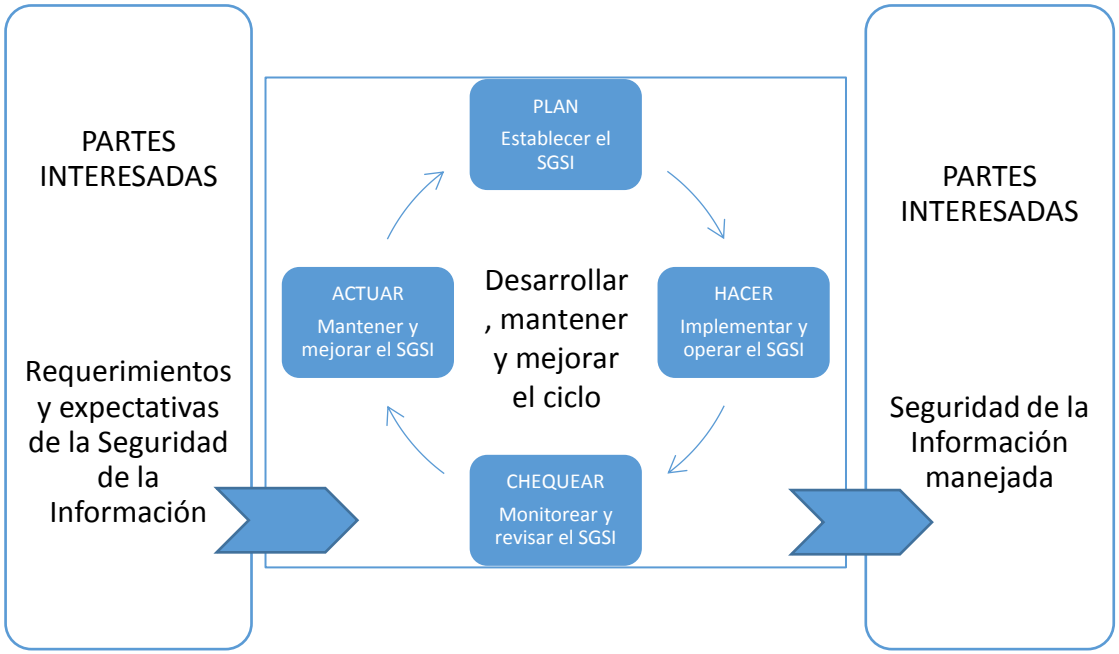

Figura 1-2: Modelo PDCA aplicado a los procesos SGSI
Fuente: Norma ISO/IEC 27001 (Comité Técnico Conjunto ISO/IEC JTC 1 Tecnología de la información & Subcomité SC 27 Técnicas de seguridad TI, n.d.)

2.2.2. Estudio de las normas ISO 27002

Las Norma ISO 27002, es el nombre que toma en lugar de la Norma ISO/IEC 17799:2005(E), sin variar su contenido y su relación a través del Anexo A del estándar ISO 27001.

Publicada en el año 2007, este conjunto de controles, publicado desde el 1 de julio de 2007, pero manteniendo como año de edición 2005, actualmente tiene la revisión del 2013, en ésta, podemos tener una lista de controles que contiene:

- 14 Dominios
- 35 Objetivos de Control
- 114 Controles

A diferencia del anterior que contenía:

- 11 Dominios
- 39 Objetivos de Control
- 133 Controles

Permitirá verificar cuales son los controles que se tienen que cumplir, para que los desarrolladores de Software, realicen sus actividades y su producto tenga una terminación adecuada en seguridad. La hoja de los controles la podremos observar en los Anexos 1 y 2.

Ante todo lo descrito, cabe resaltar que, esta norma no es certificable, y no lo es por una sencilla razón, la ISO 27002 no es una norma de gestión, así como lo es la ISO 27001, para darse cuenta, únicamente se debe ver que, en la norma ISO 27002, los controles tienen la misma denominación que los controles del Anexo A de la ISO 27001.

2.2.3. Estudio de las normas ISO 27005

La norma ISO/IEC 27005 fue elaborada por el Comité Técnico Conjunto ISO/ IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad en la tecnología de la información.

La primera edición de la norma ISO/IEC 27005 cancela y reemplaza a las normas ISO/IEC TR 13335-3:1998, e ISO/IEC TR 13335-4:2000, de las cuales constituye una revisión técnica.

Habiendo sido publicada en junio de 2008, tiene la función de establecer lineamientos para la administración (gestión) de los riesgos de seguridad de la información (RSI). Brinda el apoyo necesario a los conceptos generales descritos en la norma ISO/IEC 27001, y ha sido diseñada para aplicar de manera satisfactoria la seguridad de la información (SI) orientándose hacia la gestión de riesgos.

La comprensión de los conceptos, modelos, procesos y terminología existentes en las normas ISO/IEC 27001 e ISO/IEC 27002 es muy importante para entender de mejor manera la norma ISO/IEC 27005. (Fernando Moreno, n.d.)

Se la puede aplicar en todas las organizaciones conocidas, llámese estas, empresas de tipo comercial, de gobierno, o sin fines de lucro, las mismas que, han puesto interés en la gestión de los riesgos que puedan comprometer los activos informáticos de la organización. (Anexo 3)

2.2.4. Estudio de las OWASP

“Es un proyecto iniciado en el año 2000. Está conformado por una comunidad abierta de empresas, organizaciones educativas y particulares de todo el mundo, que crean artículos,

metodologías, documentación, herramientas y tecnologías que pueden ser usadas libre y gratuitamente. Usar OWASP permite a las organizaciones tomar mejores decisiones sobres sus riesgos de seguridad. Los proyectos OWASP se dividen en dos categorías principales: proyectos de desarrollo y proyectos de documentación." (Mosquera et al., 2015)

Para realizar un estudio de las OWASP, se debe realizar el cuestionamiento de, en donde se va a encontrar el riesgo, aquí se puede determinar que, el riesgo se encuentra en cualquier lugar en el que se desarrolla una actividad, cualquier empresa que mantenga activos, se encuentra propensa para tener riesgos. (Anexo 4)

Habiéndose determinado en donde se encuentra el riesgo, hay que clasificar los riesgos existentes en la organización, teniendo varios tipos, de los que se realizará un gráfico a continuación.

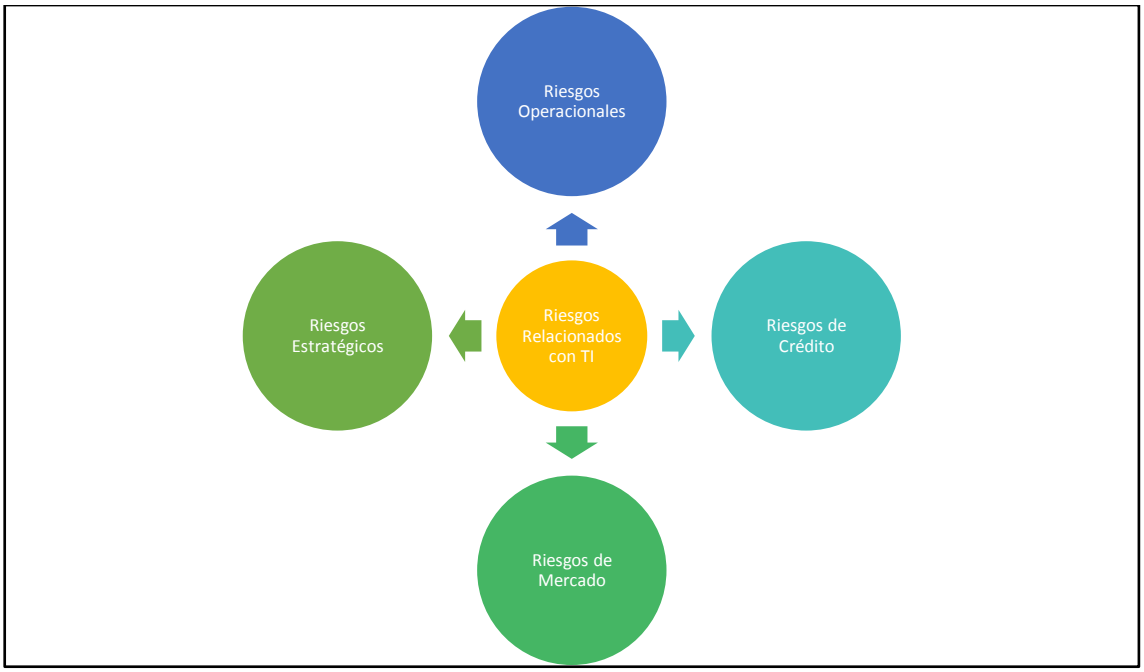

Figura 1-2: Modelo PDCA aplicado a los procesos SGSI
Fuente: Análisis de Riesgo utilizando la metodología OWASP (Alvaro Machaca, n.d.)

2.2.4.1. Riesgos en las aplicaciones

"Para el estudio que compete en la presente investigación, de acuerdo con el manual de, ***Los 10 Riesgos Más Críticos en Aplicaciones Web***, los atacantes pueden usar potencialmente rutas diferentes a través de la aplicación para hacer daño al negocio u organización, estas rutas representan un riesgo que puede, o no, ser lo suficientemente grave como para justificar la atención.

Así mismo describe que: El software inseguro está debilitando las finanzas, salud, defensa, energía, y otras infraestructuras críticas. A medida que la infraestructura digital se hace cada vez más compleja e interconectada, la dificultad de lograr la seguridad en aplicaciones aumenta exponencialmente. No se puede dar el lujo de tolerar problemas de seguridad relativamente sencillos, como los que se presentan en este OWASP Top 10" (The OWASP Foundation, 2013)

En el libro "OWASP Top 10 – 2013, Los diez riesgos más críticos en Aplicaciones Web (The OWASP Foundation, 2013)", presenta, como lo dice el título, los 10, pero, debemos tener mucho cuidado, porque existen aún más riesgos que podrían presentarse para afectar la seguridad de una aplicación web, y a través de ésta, violentar la integridad de los activos de la organización.

2.2.5. Análisis Comparativo de las Normas estudiadas

Al haber realizado el estudio de las diferentes normas que se pueden aplicar para la Gestión de la Seguridad de la Información, se puede establecer que, no se puede seguir una norma única, en vista de que cada una tiene pasos que son comunes, así como, pasos que son diferentes, en base a los que, se seguirá aplicando para lograr una política general, que coadyuve para la prevención de los riesgos que puedan afectar la integridad de los activos organizacionales.

Tabla 1-2: Tabla comparativa de las normas ISO 27001, 27002, 27005 y OWASP

NORMA ESTUDIADA	GESTION	CATEGORIZA	IDENTIFICA	CERTIFICA
ISO/IEC 27001	SI	NO	NO	SI
ISO/IEC 27002	NO	NO	NO	NO
ISO/IEC 27005	NO	NO	NO	NO
OWASP	NO	SI	SI	NO

Realizado por: Renny Montalvo 2017

Fuente: Personal

De acuerdo a los resultados que se han obtenido y tomando en consideración lo expuesto ya con anterioridad (No existe sistema 100% seguro, en este caso aplicación 100%segura), para generar políticas de seguridad, no se puede descartar ninguna propuesta de seguridad existente, ya que, todas las medidas que se puedan tomar para prevenir riesgos de seguridad se deben tomar en consideración para poder mejorar los niveles de seguridad.

Y si bien es cierto, no se podrá combatir completamente los riesgos de seguridad, si se podrá hacer más difícil la tarea de quien intente vulnerar las seguridades de la organización, tengan las intenciones que tengan.

CAPÍTULO III

3. MÉTODOS Y TÉCNICAS

3.1. Tipo de investigación

Dentro del mundo de la Investigación Científica, existen diferentes tipos, los mismos que se podrán utilizar dependiendo de las necesidades que se requieren para cada tipo.

Se pueden definir dos enfoques:

- Cuantitativo y,
- Cualitativo.

*"El **enfoque cuantitativo** es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar o eludir" pasos, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y determinan variables; se desarrolla un plan para probarlas (diseño); se miden las variables en un determinado contexto; se analizan las mediciones obtenidas (con frecuencia utilizando métodos estadísticos), y se establece una serie de conclusiones respecto de la(s) hipótesis.* (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010a, p. 20)

El enfoque cuantitativo tiene las siguientes características:
***1.** El investigador o investigadora plantea un problema de estudio delimitado y concreto. Sus preguntas de investigación versan sobre cuestiones específicas.*

***2.** Una vez planteado el problema de estudio, el investigador o investigadora considera lo que se ha investigado anteriormente (la revisión de la literatura) y construye un marco teórico (la teoría que habrá de guiar su estudio), del cual deriva una o varias hipótesis (cuestiones que va a examinar si son ciertas o no) y las somete a prueba mediante el empleo de los diseños de investigación apropiados.*

Si los resultados corroboran las hipótesis o son congruentes con éstas, se aporta evidencia en su favor. Si se refutan, se descartan en busca de mejores explicaciones y nuevas hipótesis. Al apoyar

las hipótesis se genera confianza en la teoría que las sustenta. Si no es así, se descartan las hipótesis y, eventualmente, la teoría.

3. *Así, las hipótesis (por ahora denominémoslas creencias) se generan antes de recolectar y analizar los datos.*

4. *La recolección de los datos se fundamenta en la medición (se miden las variables o conceptos contenidos en las hipótesis). Esta recolección se lleva a cabo al utilizar procedimientos estandarizados y aceptados por una comunidad científica. Para que una investigación sea creíble y aceptada por otros investigadores, debe demostrarse que se siguieron tales procedimientos. Como en este enfoque se pretende medir, los fenómenos estudiados deben poder observarse o referirse en el "mundo real".*

5. *Debido a que los datos son producto de mediciones se representan mediante números (cantidades) y se deben analizar a través de métodos estadísticos.*

6. *En el proceso se busca el máximo control para lograr que otras explicaciones posibles distintas o "rivales" a la propuesta del estudio (hipótesis), sean desechadas y se excluya la incertidumbre y minimice el error. Es por esto que se confía en la experimentación y/o las pruebas de causa-efecto.*

7. *Los análisis cuantitativos se interpretan a la luz de las predicciones iniciales (hipótesis) y de estudios previos (teoría). La interpretación constituye una explicación de cómo los resultados encajan en el conocimiento existente.*

8. *La investigación cuantitativa debe ser lo más "objetiva" posible.4 Los fenómenos que se observan y/o miden no deben ser afectados por el investigador. Éste debe evitar en lo posible que sus temores, creencias, deseos y tendencias influyan en los resultados del estudio o interfieran en los procesos y que tampoco sean alterados por las tendencias de otros.*

9. *Los estudios cuantitativos siguen un patrón predecible y estructurado (el proceso) y se debe tener presente que las decisiones críticas se efectúan antes de recolectar los datos.*

10. *En una investigación cuantitativa se pretende generalizar los resultados encontrados en un grupo o segmento (muestra) a una colectividad mayor (universo o población). También se busca que los estudios efectuados puedan replicarse.*

11. *Al final, con los estudios cuantitativos se intenta explicar y predecir los fenómenos investigados, buscando regularidades y relaciones causales entre elementos. Esto significa que la meta principal es la construcción y demostración de teorías (que explican y predicen).*

12. *Para este enfoque, si se sigue rigurosamente el proceso y, de acuerdo con ciertas reglas lógicas, los datos generados poseen los estándares de validez y confiabilidad, y las conclusiones derivadas contribuirán a la generación de conocimiento.*

13. *Esta aproximación utiliza la lógica o razonamiento deductivo, que comienza con la teoría y de ésta se derivan expresiones lógicas denominadas hipótesis que el investigador busca someter a prueba.*

14. *La investigación cuantitativa pretende identificar leyes universales y causales.*

15. *La búsqueda cuantitativa ocurre en la realidad externa al individuo. Esto nos conduce a una explicación sobre cómo se concibe la realidad con esta aproximación a la investigación.*(Hernández Sampieri et al., 2010a, p. 5,6)

El ***enfoque cualitativo*** *se selecciona cuando se busca comprender la perspectiva de los participantes (individuos o grupos pequeños de personas a los que se investigará) acerca de los fenómenos que los rodean, profundizar en sus experiencias, perspectivas, opiniones y significados, es decir, la forma en que los participantes perciben subjetivamente su realidad. También es recomendable seleccionar el enfoque cualitativo cuando el tema del estudio ha sido poco explorado, o no se ha hecho investigación al respecto en algún grupo social específico. El proceso cualitativo inicia con la idea de investigación.*(Hernández Sampieri et al., 2010a, p. 364)

Los objetivos de investigación expresan la intención principal del estudio en una o varias oraciones. Se plasma lo que se pretende conocer con el estudio.

Algunas sugerencias de Creswell para plantear el propósito de una investigación cualitativa son:

1. *Plantear cada objetivo en una oración o párrafo por separado.*

2. *Enfocarse en explorar y comprender un solo fenómeno, concepto o idea. Tomar en cuenta que conforme se desarrolle el estudio es probable que se identifiquen y analicen relaciones entre varios conceptos, pero por la naturaleza inductiva de la investigación cualitativa no es posible anticipar dichas vinculaciones al inicio del proyecto.*

3. Usar palabras que sugieran un trabajo exploratorio ("razones", "motivaciones", "búsqueda", "indagación", "consecuencias", "identificación", etcétera).

4. Usar verbos que comuniquen las acciones que se llevarán a cabo para comprender el fenómeno. Por ejemplo, los verbos "describir", "entender", "desarrollar", "analizar el significado de", "descubrir", "explorar", etcétera, permiten la apertura y flexibilidad que necesita una investigación cualitativa.

5. Usar lenguaje neutral, no direccionado. Evitar palabras (principalmente adjetivos calificativos) que puedan limitar el estudio o implicar un resultado específico.

6. Si el fenómeno o concepto no es muy conocido, proveer una descripción general de éste con la que se estará trabajando.

7. Mencionar a los participantes del estudio (ya sea uno o varios individuos, grupos de personas u organizaciones). En ocasiones pueden ser animales o colectividades de éstos, así como manifestaciones humanas (textos, edificaciones, artefactos, etcétera).

8. Identificar el lugar o ambiente inicial del estudio" (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010b, pp. 364,365).

De acuerdo a lo expuesto en los párrafos anteriores, y tomando en consideración cada uno de los tipos de investigación, la presente investigación se enfocará hacia el tipo cuantitativo, derivándose dentro de ella hacia la investigación experimental.

La investigación experimental manipula al menos una variable no comprobada, cuya finalidad es la de describir "el modo" o "la causa" que podría producir un acontecimiento particular. El experimento provocado por el investigador, le permite introducir variables de estudio manipuladas por él, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas.

3.2. Diseño de la Investigación

Se define al diseño como, al plan o estrategia que se desarrolla para obtener la información que se requiere en una investigación. En el enfoque cuantitativo, el investigador utiliza su diseño para analizar la certeza de las hipótesis formuladas en un contexto en particular o para aportar

evidencia respecto a los lineamientos de la investigación (si es que no se tiene hipótesis). (Hernández Sampieri et al., 2010b, p. 120)

Aquí se define la estrategia que se utilizará para obtener la mayor cantidad de resultados que se necesitan para que la investigación culmine de la mejor manera.

El trabajo que se realizará, toma por diseño uno de los diseños básicos de la investigación cuantitativa, éste es el diseño experimental, por las características presentadas aquí para poder obtener los resultados que nos lleven a determinar la validez de la hipótesis planteada.

3.3. Métodos y técnicas

El presente trabajo de investigación utiliza los siguientes métodos y técnicas:

3.3.1. Métodos

"La investigación científica se encarga de producir conocimiento, el conocimiento científico tiene diferentes características, las mismas que se listan a continuación.

- Sistemático.
- Ordenado.
- Metódico.
- Racional (Reflexivo).
- Crítico.

Para desarrollar el presente trabajo se ha tomado en consideración el método científico el mismo que propone las siguientes etapas:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis
- Difusión de resultados" (Pablo Méndez, 2015, p. 47)

3.3.2. Técnicas

"Las técnicas que serán utilizadas en la presente investigación son:

- **Búsqueda de información:** permite obtener la información necesaria acerca del objeto de estudio de la investigación para su desarrollo, utilizando las fuentes secundarias disponibles.
- **Pruebas:** permite realizar experimentos en escenarios de laboratorio.
- **Observación:** permite determinar resultados de las pruebas realizadas en los escenarios de laboratorio.
- **Análisis:** permite determinar los resultados de la investigación" (Pablo Méndez, 2015).

3.4. Instrumentos

Se ha tomado en consideración los diferentes instrumentos que se pueden encontrar para realizar investigación científica, ellos permitirán recopilar la información necesaria de los indicadores planteados.

En la presente investigación, se han tomado en consideración herramientas de Software Libre, tanto para el desarrollo de una aplicación DEMO, la que permitirá realizar las diferentes pruebas para la obtención de los datos de los indicadores planteados, como en los Sistemas Operativos y Servidores Web.

Con el uso de las presentes herramientas se podrá formar un laboratorio de pruebas que permitirá obtener los resultados necesarios para determinar la validez de las políticas generadas para poder desarrollar Software seguro.

3.4.1. JBOSS

¿Qué es JBOSS?

JBoss developer estudio (JBDS), es un conjunto de herramientas de desarrollo de software, basadas en la plataforma eclipse, y en Linux Red Hat Enterprise.

Este conjunto de herramientas de licencia de código abierto, nos permite desarrollar varias aplicaciones en diferentes ambientes tales como Angular js, JAVA, html, etc.

Al instalar JBDS, tenemos a nuestro alcance un sinnúmero de herramientas, incluyendo un servidor web, el mismo que nos permitirá ejecutar nuestras aplicaciones directamente en el servidor que se ha utilizado para su desarrollo.

Para poder instalar, debemos descargarnos la aplicación desde su página nativa de descarga, en developers.redhat.com

Para realizar el prototipo para las pruebas del presente trabajo de investigación, se ha realizado con la versión 10.2.

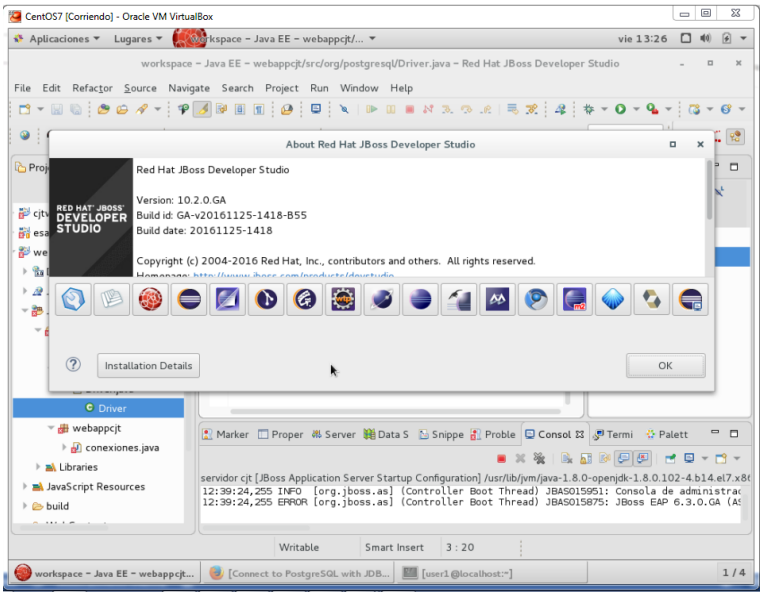

Figura 1-3: JBOSS Developer Studio
Realizado por: Renny Montalvo 2017

3.4.2. Eclipse.

Eclipse, es el entorno que nos permite desarrollar aplicaciones para el uso personal o empresarial, por lo general se lo está utilizando para aplicaciones del tipo empresarial.

Se ha determinado el uso de este entorno, por ser una herramienta de código abierto, por la facilidad que se tiene de utilizar el ambiente de desarrollo que más se acomode a las necesidades y aptitudes de la persona que vaya a iniciar en el campo de las aplicaciones de software.

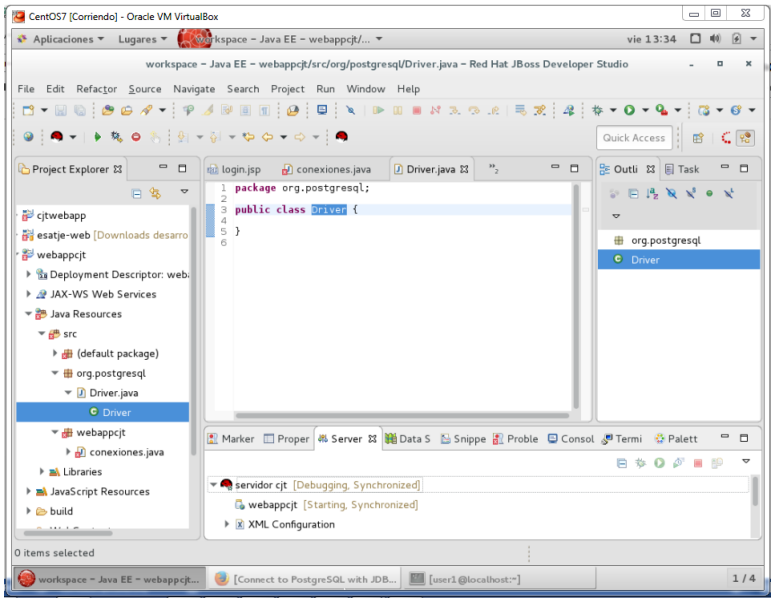

Figura 2-3: JBOSS Developer Studio
Realizado por: Renny Montalvo 2017

3.4.3. OWASP ZAP

Dentro de las actividades a cumplirse para determinar si las políticas han podido utilizarse para ser una solución, tenemos la herramienta OWASP ZAP.

Esta herramienta, nos permite realizar ataques a las páginas que se encuentran activas, determinando si:

- La aplicación tiene vulnerabilidades.
- Cuáles son las vulnerabilidades.
- Qué posibles soluciones se pueden realizar para que esas vulnerabilidades sean corregidas y mitigadas para que no vayan a causar problemas de ataques severos cuando se encuentren en producción.

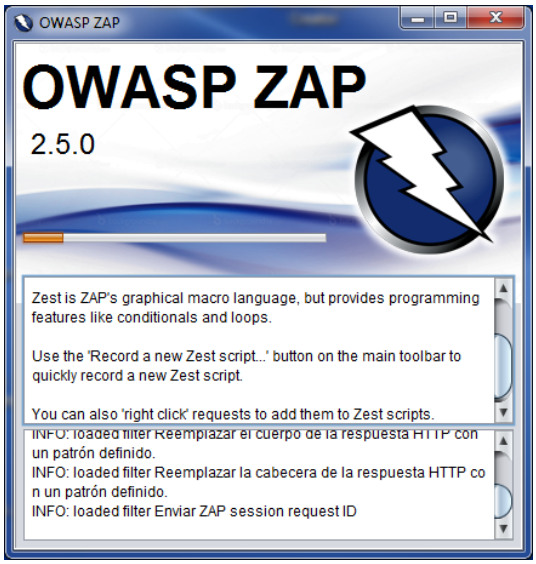

Figura 3-3: OWASP ZAP
Realizado por: Renny Montalvo 2017

3.4.4. PostgreSQL

Es un motor de Base de Datos de código abierto, el mismo que nos permitirá generar el almacenamiento adecuado para poder verificar y realizar los accesos necesarios con los que cuenta en la actualidad una aplicación de software mínima, es decir la más pequeña.

Se ha tomado en consideración el hecho que las herramientas que se van a utilizar sean de código abierto, puesto que, actualmente, la mayoría de las personas que desarrollan software, se orientan por utilizar este tipo de herramientas, porque además no ser o no necesitar de un costo por su mantenimiento o actualización, tienen la robustez necesaria como para poder trabajar de mejor manera con los servidores que alojan las aplicaciones, brindando mayor seguridad y estabilidad para quienes desarrollan aplicaciones o soluciones de software.

3.5. Validación de instrumentos

Los instrumentos de software que se utilizarán en la presente investigación, han sido seleccionados por las ventajas que se obtienen de ellos y por ser la tendencia que se está presentando para el desarrollo de aplicaciones.

Tomando además en consideración el hecho de que se encuentran disponibles al más bajo costo, siendo uno de los factores por lo cual se utiliza este tipo de herramientas Software, además de su disponibilidad son herramientas robustas, simples y con una adecuada configuración acerca la

posibilidad de que vaya reduciendo las diferentes vulnerabilidades que van presentándose a nivel de desarrollo.

3.6. Hipótesis

La generación de políticas para gestionar los riesgos de seguridad de la información, permitirán mejorar la mitigación de vulnerabilidades existentes en el desarrollo de software.

3.6.1. Determinación de variables

Para poder demostrar la hipótesis que se ha formulado, hay que determinar las variables que serán utilizadas para este fin, es por eso que se presentan como:

- Las políticas generadas para la gestión de los riesgos de seguridad durante el desarrollo de Software.
- Los riesgos a los que están expuestas las aplicaciones desarrolladas.

3.6.2. Operacionalización conceptual

La operacionalización conceptual se muestra en la tabla 1-3.

Tabla 1-3: Operacionalización Conceptual

VARIABLE	**TIPO**	**CONCEPTO**
Políticas de seguridad.	Independiente	Conjunto de normas de seguridad del modelo propuesto adaptado en base a normas existentes.
Riesgos de la seguridad de la información.	Dependiente	Nivel de protección de la información contra riesgos en los servicios web

Realizado por: Renny Montalvo 2017

Fuente: Personal

3.6.3. Operacionalización metodológica

La operacionalización metodológica se encuentra en la tabla 1.5.2.

Tabla 2-3: Operacionalización Metodológica

HIPOTESIS	VARIABLES	INDICADORES	INDICES	TECNICA
La generación de políticas para gestionar los riesgos de seguridad de la información, permitirán mejorar la mitigación de vulnerabilidades existentes en el desarrollo de software	**V. Independiente.** Propuesta de Políticas de Seguridad.	Confidencialidad	Políticas y reglamentos	Observación, Análisis
		Integridad	Salvaguardias físicas y técnicas	Observación, Análisis
		Procedimientos adecuados	Requisito organizacional y requisitos de documentación	Observación, Análisis
	V. Dependiente. Riesgos de la seguridad de la información.	Acceso no autorizado	Estrategia relacionada con el cumplimiento de Políticas	Recopilación de información
		Vulneración de perímetro informático en servidores	Seguridad de la información	Recopilación de información
		Cantidad de vulneraciones realizadas por un atacante	Vulnerabilidades de la aplicación.	Recopilación de información

Realizado por: Renny Montalvo 2017

Fuente: Personal

3.6.3.1. Población.

La característica principal de la población está basada en los grupos que se forman para producir cada uno de los módulos asignados, dentro del consejo de la Judicatura, por cada nuevo módulo que se inicia, cada grupo tiene nuevas responsabilidades de desarrollo, dependiendo de las necesidades que se vayan generando para los nuevos productos.

Por ser que, cada módulo que se desarrolla, lo realiza todo el grupo, se ha determinado que, todos van a realizar las diferentes pruebas de vulnerabilidad, tomando en consideración, el tiempo que se demora cada uno para determinar si, la aplicación de las políticas ha prestado el contingente necesario para mitigar el riesgo de vulneración, y así determinar si se debe o no aplicar el presente trabajo de investigación

3.6.3.2. Selección de la muestra

Para seleccionar una porción representativa de la población, que permita generalizar los resultados de la investigación, y por motivos de factibilidad relacionados con la disponibilidad de recursos se establece una muestra del tipo probabilístico tomada de los 12 desarrolladores.

3.6.3.3. Tamaño de la muestra

Tomando en consideración que la población de programadores en el Consejo de la Judicatura a nivel nacional es baja (12 personas), se establece el tamaño de la muestra al cien por ciento de la población, con quienes se realizarán las diferentes pruebas y poder determinar la efectividad de la investigación.

3.6.3.4. Instrumentos de recolección de datos

La recolección de datos utilizada en la presente investigación, es determinar el acceder a la vulnerabilidad antes y otra después de haberse implementado las “Políticas de Seguridad Para el Desarrollo de Software”, y la verificación de un análisis documental que se aplica en un momento en particular, con la finalidad de buscar información que será útil para evaluar los indicadores de las variables planteadas.

3.6.3.5. Instrumentos para procesar datos recolectados.

Como instrumentos para procesar los datos recolectados se utiliza el software Microsoft Excel y SPSS para la tabulación y análisis estadístico de las encuestas aplicadas, y los resultados de los ataques realizados a través del OWASP ZAP.

3.6.3.6. Identificación y Priorización de Riesgos.

Se denomina **INCIDENCIA** a, un hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

Riesgo: Es la probabilidad de que exista algún evento que se pueda producir un contratiempo o una desgracia de una manera inesperada.

3.6.3.7. Análisis del Riesgo

El análisis de riesgo, está basado en la información que se genera en la fase de identificación, que luego será utilizada para la toma de decisiones.

Hay que considerar tres elementos que se permiten aproximar un valor objetivo para la lista de la incidencia de riesgos los cuales son: probabilidad que ocurra, impacto en caso de ocurrir y la exposición. A través de esto, se puede categorizar el riesgo, y a su vez poder administrar los más importantes

3.6.3.8. Probabilidad del Riesgo

Es la probabilidad de ocurrencia de un evento, para el estudio es muy importante determinar cuál es la posibilidad de que este evento, se presente realmente. La probabilidad de que el riesgo ocurra, debe ser superior a cero, caso contrario el riesgo no se presenta como una amenaza, así mismo, debe ser inferior a uno, o el riesgo llegaría a darse por verdadero, es decir, se presentaría de cualquier manera.

Tabla 3-3: Probabilidad de Ocurrencia

PROBALIDAD DE OCURRENCIA	DESCRIPCION
ALTA	Vulnerabilidad que si es explotada comprometería la seguridad de la información ocasionando un impacto negativo sobre la empresa. Debe solucionarse inmediatamente.
MEDIA	Vulnerabilidad que si es explotada tendría un impacto leve sobre la operativa del negocio. Puede
BAJA	Vulnerabilidad que si es explotada no ocasionaría mayores inconvenientes. Su solución no

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d., p. 11)

3.6.3.9. Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida.

Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto. Para nuestro caso, se clasifica el impacto con una escala numérica del 1 al 4.

Tabla 4-3: Impacto del riesgo

IMPACTO	VALOR
Bajo Impacto	0 a < 3
Medio Impacto	3 a < 6
Alto Impacto	6 a < 9

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d., p. 17)

3.6.3.10. Ponderación del Riesgo

La ponderación al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que

también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento.

Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

3.6.3.11. Identificación de Riesgos

Después de haber ponderado y validado objetivamente las probabilidades de ocurrencia de riesgos comunes en los Hospitales de Nivel 1 del IESS se observa que los siguientes riesgos, indicados en la siguiente tabla, son los que con mayor frecuencia ocurren.

Tabla 5-3: Riesgos identificados

Ítem	**Vulnerabilidad**
1	A1 – Inyección
2	A2 – Pérdida de Autenticación y Gestión de Sesiones
3	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)
4	A4 – Referencia Directa Insegura a Objetos
5	A5 – Configuración de Seguridad Incorrecta
6	A6 – Exposición de Datos Sensibles
7	A7 – Ausencia de Control de Acceso a las Funciones
8	A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)
9	A9 – Uso de Componentes con Vulnerabilidades Conocidas
10	A10 – Redirecciones y reenvíos no validados

Realizado por: Renny Montalvo 2017

Fuente: (The OWASP Foundation, 2013, p. 4)

3.7. Definición de los escenarios de pruebas

Para continuar con el desarrollo de la presente investigación, se definen los escenarios de pruebas.

Estos escenarios permitirán simular las condiciones en las que van a funcionar las aplicaciones para obtener y verificar los resultados necesarios que se necesitan en esta investigación.

3.7.1. Ambiente de pruebas

Se genera un ambiente de pruebas en el que estarán configuradas en el mismo servidor dos aplicaciones prototipo, las mismas que estarán configuradas una aplicando las políticas generadas y otra sin aplicar las políticas,

3.7.2. Escenarios.

Dentro del ambiente de pruebas se configurarán dos escenarios.

3.7.2.1. Escenario 1

El primer escenario estará configurado con el *Prototipo No. 1*, este prototipo estará realizado sin utilizar las políticas generadas en la presente investigación.

3.7.2.2. Escenario 2

El siguiente escenario estará definido por el *Prototipo No. 2*, este prototipo estará configurado con las políticas generadas, esto permitirá conocer si programar utilizando políticas de seguridad

3.7.3. Resultados

Posteriormente se realizarán las pruebas en los dos escenarios planteados con la finalidad de demostrar la mejora de la seguridad de las nuevas políticas generadas para desarrollar software seguro.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Creación e implementación de las políticas para evaluación y gestión de riesgos

Dentro de la investigación que se encuentra en curso, se deben generar las diferentes políticas que rijan dentro del Consejo Nacional de la Judicatura, para la creación de nuevas Aplicaciones Software, para realizar esta actividad, se basa en la hoja de controles de la ISO 27002: 2013, la misma que guiará el desarrollo de las aplicaciones.

La hoja de control de la ISO 27002:2013, en la parte pertinente hacia el desarrollo de Software presenta lo que se versa en el objetivo de control 14.2. el mismo que se detalla a continuación:

4.1.1. Objetivo

El objetivo es garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información (Objetivo 14).

4.1.1.1. Seguridad en los procesos de desarrollo y soporte (Objetivo 14.2)

Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

Los directivos responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.

Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios.

Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).

4.1.1.2. Actividades de control del riesgo

4.1.1.2.1. Política de desarrollo seguro de software (14.2.1):

Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.

4.1.1.2.2. Procedimientos de control de cambios en los sistemas (14.2.2):

En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.

4.1.1.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo (14.2.3):

Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.

4.1.1.2.4. Restricciones a los cambios en los paquetes de software (14.2.4):

Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.

4.1.1.2.5. Uso de principios de ingeniería en protección de sistemas (14.2.5):

Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

4.1.1.2.6. Seguridad en entornos de desarrollo (14.2.6):

Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

4.1.1.2.7. Externalización del desarrollo de software (14.2.7):

La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.

4.1.1.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas (14.2.8):

Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.

4.1.1.2.9. Pruebas de aceptación (14.2.9):

Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.

4.1.1.3. Métricas Asociadas

"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc. ("BSI - BS ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management," 2015) ("ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información," n.d.)

4.1.2. Políticas de Seguridad para el Desarrollo de Software

Antes de empezar a escribir acerca de políticas de seguridad, se deberá establecer la definición de política, para esto, se hace referencia a un documento establecido por la Universidad Nacional de Colombia que dice lo siguiente:

"*Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por las directivas de la organización, y deben ofrecer direccionamientos a toda la*

organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción". (Universidad de Colombia, 2003)

4.1.2.1. ¿Por qué políticas de seguridad para el desarrollo?

Al implementar nuevas Políticas de Seguridad para enfrentar los riesgos que se podrían generar en el momento de desarrollar Software, se debe enfocar en los diferentes aspectos a tomar en consideración para su prevención.

Existen muchas más razones que se podrían describir, pero la principal dentro de la investigación es, la preservación del activo más importante que se encuentra en riesgo elevado si se llegaría a dar un ataque hacia los equipos informáticos dentro del Consejo de la Judicatura, que es la Información que se mantiene almacenada en los servidores de la institución.

4.1.2.2. Objetivo

El objetivo principal de la generación de las Políticas de Seguridad para el Desarrollo de Software está orientado a que el Software que se cree dentro del Consejo Nacional de la Judicatura, cumpla con los elementos básicos, que permitan proteger a los funcionarios que hagan uso del Software dentro de sus actividades diarias.

Así mismo, colaborar con el personal que, sin dedicarse al Desarrollo de Software, tienen que trabajar en la seguridad de la información, tarea que no resulta muy sencilla, por el incremento de agentes externos e internos con los que tienen que enfrentarse tanto los encargados de la seguridad como los usuarios finales en la institución.

4.1.2.3. Propósito

El propósito principal de aplicar las políticas de seguridad dentro del Consejo de la Judicatura, es el de mantener protegida la información generada dentro de la institución, la misma que, si bien es cierto se mantiene pública, no todo lo generado se encuentra visible para todas las personas que acceden a revisar ésta.

Esta política cubre todas las evaluaciones de seguridad en aplicaciones solicitadas por cualquier persona, grupo o departamento que tenga como finalidad mantener la seguridad, cumplimiento, gestión de riesgos y control de cambios de las tecnologías en uso en el Consejo de la Judicatura.

En las revisiones previas, se ha visto que, el Consejo de la Judicatura sufre, como la mayoría de las empresas, fallos en la Seguridad de la Información, revisando estos fallos, se ha podido generar las políticas siguientes:

- **Política No. 1: Trabajar en equipo**

DESCRIPCIÓN

Para poder trabajar de mejor manera todo lo descrito, no se debe dejar de lado el trabajo en equipo, es muy importante el presente ítem en vista de que, si las diferentes áreas trabajan por su lado, no se podrá lograr avances importantes, cada una de las áreas que conforman la DNTIC's, deberán estar comprometidas con la Seguridad de la Información, y deberá ser un aspecto primordial, por la naturaleza de la información que se almacena en el CNJ, por la confidencialidad mismo y por el simple hecho de que se podrían realizar actividades que no están acorde al tratamiento de la justicia en el país.

Autoridad

- Norma ISO/IEC 27002:2013, Control 7.2.3

Propósito

El propósito que conlleva la realización y ejecución de la presente política, es la aplicación dentro de todos los involucrados en el proceso del negocio, un ambiente común y solidario de empoderamiento de todos los involucrados en el proceso de la Seguridad de la Información interna, y si quienes forman parte del presente proceso no se empoderan de lo que se debe realizar, el proceso no tendría el éxito que se está buscando.

Alcance

La presente política, es de aplicación a todos los elementos del Talento Humano, es decir, todo el personal de la empresa debe aplicar la política, creando un ambiente propicio para su ejecución y puesta en marcha.

Roles y Responsabilidades

Quienes tienen la responsabilidad principal para que la política sea bien aplicada dentro de la empresa es el departamento de Talento Humano, ellos son los responsables del recurso más importante que forma parte de la empresa.

Además, debe complementar el cumplimiento de la política, la Subgerencia de Desarrollo, en vista de que es ahí en donde directamente se mantiene el personal dedicado para esta finalidad, expandiéndose hacia el resto del personal existente en la empresa.

Definiciones

DNTIC'S. Dirección Nacional de Tecnologías de la Información y de la Comunicación.

Historial de Revisiones

Las revisiones deberán hacerse en forma periódica, sin dejar que pase demasiado tiempo, dejando sentada la fecha en la que se han realizado los cambios por quien y cuáles fueron los aspectos más importantes que se han realizado.

- **Política No. 2: Se debe iniciar en la fase de requerimentación:**

DESCRIPCIÓN

Luego de haber dado el primer paso en la cultura de SI (Seguridad de la Información), para el desarrollo de una aplicación, se deberá partir, con la recopilación de los requerimientos que se tiene para el desarrollo de ésta, ahí será cuando se determinen todas las necesidades de seguridad a tomar en consideración, así como las necesidades de la aplicación a desarrollar.

Autoridad

- Norma ISO/IEC 27002:2013, Control 14.1.1
- Norma ISO/IEC 27002:2013, Control 14.1.2
- Norma ISO/IEC 27002:2013, Control 14.1.3

Propósito

Partir desde la etapa de la requerimentación, permitirá al desarrollador, no dejar de lado ningún aspecto que pueda llegar a convertirse en una puerta para que se exploten los riesgos potenciales que pueda dejar una aplicación de software, la misma que, si no se ha corregido desde el inicio, resulta más difícil encontrar el lugar en el que se genera la ventana de vulnerabilidad que hacerlo desde el principio, y llevarla con seguridad hasta la conclusión de la aplicación.

Alcance

Aplicar la presente política está bajo la responsabilidad de quienes recopilen la información de requerimientos, sugiriendo de ser necesario, a quien es dueño de la aplicación, la necesidad de contar con los respectivos niveles de seguridad, que, a la larga, beneficiarán a la protección de los activos informáticos que se necesitan proteger.

Roles y Responsabilidades

La responsabilidad principal estará bajo la Subdirección de Desarrollo, y será aplicada por los desarrolladores, tomando en consideración que, son ellos quienes plasman en la aplicación los requerimientos que se han recolectado de los dueños del proceso.

Definiciones

Requerimentación: Acción de recolectar por diferentes medios, los requisitos necesarios para la realización de un proyecto.

Historial de Revisiones

Es muy importante llevar un control con las fechas y vulnerabilidades que se han encontrado y reducido, en vista de la necesidad de llevar un control para ser utilizado en una nueva aplicación.

- **Política No. 3: Se debe trabajar con un servidor de aplicaciones que permita configurar seguridades.**

DESCRIPCIÓN

El servidor de aplicaciones (web), debe permitir la posibilidad de que el administrador de la aplicación pueda configurar los niveles de seguridad, los mismos que deberán ser establecidos desde la requerimentación, pues, si no se establece al inicio existirán muchos retrasos cuando se quiera implementar sobre la marcha.

Hay que tomar en consideración que el servidor por sí solo no podrá repeler los ataques, hay que buscar la instalación de un servidor que bloquee ataques, o que no permita que se vulneren fácilmente las seguridades, o que sea considerado un primer filtro, que no permita el ingreso a los intrusos.

Autoridad

- Norma ISO/IEC 27002:2013, Control 9.4.1
- Norma ISO/IEC 27002:2013, Control 9.4.2
- Norma ISO/IEC 27002:2013, Control 9.4.3

Propósito

Seleccionar de una manera exhaustiva, el servidor en donde será alojada la aplicación, tomando en consideración diferentes aspectos, que permitirán mantener un mínimo de seguridades, seguridades que serán tomadas en beneficio del desarrollo de aplicaciones de Software, objetivo principal del presente trabajo de investigación.

Si el servidor proporciona la confianza necesaria para poder acoger una aplicación o su base de datos, el desarrollo de una aplicación de Software tomará menos esfuerzo de preocuparse demasiado por configurar la seguridad en el servidor, por lo que una buena selección del servidor podrá brindar un mejor apoyo en este cometido.

Alcance

Principalmente se puede determinar que, quienes deben tener la responsabilidad de una buena selección, sería el área de infraestructura, en combinación con la Subgerencia de Desarrollo,

debido a que el trabajo en equipo puede representar que se realice la toma de la mejor decisión, sin afectar los intereses, ni de la empresa, ni tampoco del área que desarrolla la solución de Software para determinada área de la institución.

Roles y Responsabilidades

La responsabilidad principal estará bajo la Subdirección de Desarrollo, y será aplicada por los desarrolladores, tomando en consideración que, son ellos quienes plasman en la aplicación los requerimientos que se han recolectado de los dueños del proceso.

Definiciones

Servidor: Equipo en el que se ponen en funcionamiento los servicios y aplicaciones que serán utilizadas para la institución.

Historial de Revisiones

La revisión y su historial de realizaciones, se debe tomar en consideración puesto que, es el equipo que debe permanecer encendido siempre, aquí se tendrá la aplicación que se presentará a quienes hacen uso de ella.

- **Política No. 4: Se debe proteger de ataques internos.**

DESCRIPCIÓN

La primera protección que debe existir es la protección contra los ataques internos, esto significa que, aunque se mantenga un nivel de seguridad muy elevado para quienes realizan sus ataques desde fuera de la institución, estaremos dejando abierta la puerta para que el atacante externo tome control de algún usuario al interior de la institución, dando pie para que, escalando los permisos de usuario pueda llegar en algún momento a tomar posesión del servidor, logrando su cometido.

Autoridad

- Norma ISO/IEC 27002:2013, Control 9.2.3
- Norma ISO/IEC 27002:2013, Control 12.4.1

- Norma ISO/IEC 27002:2013, Control 12.4.2
- Norma ISO/IEC 27002:2013, Control 12.4.3

Propósito

Se necesita el uso de esta política, porque es necesario evitar el acceso indebido hacia el servidor y sus aplicaciones, para poder evitar que se comprometa información delicada que pueda estar siendo comprometida si alguna persona que no tenga la debida autorización y que pueda significar un riesgo para la integridad de los activos informáticos sensibles de la institución.

Dicho esto, las personas que hacen los primeros intentos por tratar de vulnerar y acceder a este tipo de activos, son los funcionarios de la misma entidad, por desconocimiento, por curiosidad, por tratar de hacer alguna variación dentro de sus horarios, o si ya tienen un poco más de conocimientos, será para tratar de extraer la información y, lograr realizar alguna acción en su beneficio o por el simple hecho de perjudicar de alguna manera a alguien en específico.

Alcance

El departamento que mantiene esta responsabilidad y que es muy delicada, es primeramente la Unidad de Talento Humano, ellos son los encargados de determinar, que acciones puede o no realizar el funcionario que ingresa a laborar en la institución, determinando los roles que debe tener cada uno de los funcionarios de acuerdo a los reglamentos internos de la empresa.

Roles y Responsabilidades

Para la política en curso, los roles y responsabilidades deben llegar por parte de la Unidad de Talento Humano, y de acuerdo a lo establecido en los reglamentos internos y manuales funcionales.

Adicional a lo anterior, se necesita que los accesos a los servidores de aplicaciones no lo haga cualquier persona, por lo sensible de la información que se puede manejar en una entidad, sea pública o privada, por lo tanto, deberán existir, los certificados que puedan ser una camisa de fuerza que no permita la fuga de información, a su vez, que puedan existir las debidas seguridades para que los atacantes internos no vayan a vulnerarlas y realicen ataques desde adentro.

Definiciones

Información Sensible: Es información que no puede ser revelada a cualquier persona o empresa sin la debida autorización de autoridad judicial o de la persona o personas implicadas.

Historial de Revisiones

La revisión y su historial, se debe realizar con espacio de tiempo no muy separado, en vista de que, la información, hay que mantenerla controlada permanentemente, porque los riesgos de vulnerar las seguridades están latentes, y, se debe controlar quien ha realizado las diferentes acciones que puedan ejecutarse para realizar este tipo de acciones.

- **Política No. 5: Hay que prestar atención a los caracteres que se permitan ingresar.**

DESCRIPCIÓN

Cuando el funcionario ingresa sus credenciales de autenticación, las políticas de la institución, o, del servidor que presta estos servicios, podrán pedir el ingreso de caracteres especiales para el nombre del usuario, el Consejo de la Judicatura, utiliza un servidor Active Directory, en el mismo, se han especificado los usuarios para que puedan ingresar un punto en su nombre de usuario.

Si en el momento de programar, no se establece cuáles son y cuando se puede ingresar los caracteres especiales, el atacante podrá tomar esta posibilidad para poder utilizar una vulnerabilidad, puesto que, al no tomar en consideración que, el ingreso de otros datos que no corresponden a los registrados traería consecuencias desagradables en cuanto a la seguridad de la información, las mismas que podrían dejar desprotegidos los datos ingresados.

Autoridad

- Norma ISO/IEC 27002:2013, Control 12.4.2
- Norma ISO/IEC 27002:2013, Control 14.2.5

Propósito

Es necesario advertir que, cuando se desarrolla una aplicación de software, siempre se necesita tener una sección de login, en esta sección, se tiene un espacio en el cual se pide ingresar un usuario y una contraseña, es en ese momento en el que se generan diversas maneras de burlar las seguridades creadas para el ingreso.

Es en ese momento que, las personas que desarrollan Software, deben establecer cómo se puede evitar el mal uso de estos espacios, los que deben detallar y controlar de una manera exhaustiva, que caracteres son los permitidos para ingresar, debido a que, si se permite cualquier tipo de caracter, puede forzar al uso indebido de un usuario como administrador, y es justamente esa situación la llamada a evitarse.

Alcance

El uso de la presente política, reducirá en gran manera, los riesgos de ataques de SQLInjection principalmente, defendiendo así, la intrusión de atacantes hacia los servicios que se está brindando, previniendo el robo de información por parte de entes internos o externos

Porque, no es explícitamente alguien externo que va a querer extraer o ingresar información de manera fraudulenta, y que pueda desencadenar en responsabilidades de manera legal en contra de la empresa o quienes administran sus servicios.

Roles y Responsabilidades

La responsabilidad directa en esta política, va con el grupo de desarrollo, ellos son quienes deben tomar en consideración este tipo de situaciones, y, establecer de una manera responsable que es lo que cada persona que tiene acceso puede digitar, acorde con las políticas de seguridad de la empresa, para que, si existe alguien que sabe de ataques cibernéticos, no pueda explotarlo muy fácilmente.

Definiciones

Dominio: Red de computadores que se encuentran bajo una misma administración, siendo aplicadas diferentes reglas para el acceso o uso del equipo.

Active Directory: O Directorio Activo, es un servidor de control de accesos de los equipos, que permite la administración del dominio.

SQLInjection: Inserción de código malicioso a una base de datos, a través de sentencias SQL, las mismas que se utilizarán para realizar cualquier actividad inapropiada o fraudulenta en la base de datos.

Historial de Revisiones

La revisión y su historial, se debe realizar con espacio de tiempo no muy separado, en vista de que, la información, hay que mantenerla controlada permanentemente, porque los riesgos de vulnerar las seguridades están latentes, y, se debe controlar quien ha realizado las diferentes acciones que puedan ejecutarse para efectivizar este tipo de acciones.

- **Política No. 6: Presentar una página de error personalizada.**

DESCRIPCIÓN

Cuando un usuario no ha podido realizar la conexión, es desviado a una página de error, la misma que, nos muestra información que podría ser utilizada por un atacante servidor web utilizado, herramienta de programación, esto podría ser utilizado para sus propósitos de vulnerar la seguridad, si al momento de que esto ocurra se reenvía la petición, hacia una página que presente información que no comprometa la seguridad de la misma dentro del Consejo de la Judicatura, es decir mostrar lo que la institución quiere mostrar, y ocultar lo que no quiere presentar a quien utiliza la aplicación.

Autoridad

- Norma ISO/IEC 27002:2013, Control 12.4.1
- Norma ISO/IEC 27002:2013, Control 12.4.2
- Norma ISO/IEC 27002:2013, Control 12.4.3
- Norma ISO/IEC 27002:2013, Control 12.4.4

Propósito

El propósito principal de la aplicación de la política, se da porque, cuando a una página se la pone en mantenimiento, y el servidor aún se encuentra levantado, la respuesta que recibe la

persona que está haciendo uso de la aplicación, es información del servidor, plataforma en la que se está trabajando versiones, y así otra información, que para los casos de vulnerabilidades, se puede utilizar de mejores maneras (Para los atacantes), y pueden dejar en la indefensión a los servidores, evitar presentar esta información, aunque parezca que no tiene mucha importancia, la tiene y puede reducir en un alto porcentaje el riesgo de ataques.

Alcance

El alcance se da para, poder reducir en un alto porcentaje el proveer de información muy valiosa para que, el atacante pueda hacer uso de ella y, logre encontrar otras vulnerabilidades que no son precisamente en la aplicación, sino, en los servidores en donde ella se encuentra alojada, mitigando de gran manera un riesgo muy latente en las aplicaciones de Software.

Roles y Responsabilidades

Son responsables de que la política se lleve a efecto, quienes realizan directamente la programación de las aplicaciones, y deben verificarse a través de los módulos de prueba y de quienes realizan el control de calidad, porque ellos serán los responsables de verificar que, la aplicación esté optimizada para su puesta en producción.

Definiciones

Control de Calidad: Luego de realizarse las pruebas en el área de desarrollo, debe pasar al área de control de calidad, en donde se determinará si la aplicación cumple con todo lo necesario para ser puesta en producción, de no ser así, deberán regresar la aplicación para que realice los cambios necesarios para que pueda cumplir lo requerido y pueda ser aplicada para su uso tanto interno como externo.

Historial de Revisiones

Es muy importante que, se lleve un registro minucioso de todo lo requerido y lo realizado para corregirlo, con un detalle de fechas y la cantidad de revisiones, para poder saber si lo que se ha enviado a producción, ha cumplido con lo requerido desde el principio y con lo solicitado por el área de control de calidad.

- **Política No. 7: No presentar información delicada en la barra de dirección.**

DESCRIPCIÓN

Muchas de las veces, cuando un usuario de una aplicación realiza el ingreso, al momento de haber accedido, los datos ingresados son mostrados en la barra de dirección del navegador web, esta vulnerabilidad podría ser explotada por un atacante si estuviera presente, o en caso de que haya tomado posesión del equipo del funcionario.

Siempre será mejor ocultar esta información para que no se tenga acceso únicamente con estar junto a la persona que está ingresando, es decir no se deberá presentar la información ni siquiera del USER ID, puesto que a través de esta información se pueden realizar diferentes ataques que derivarían en la vulneración de los perímetros de seguridad de la información.

Autoridad

- Norma ISO/IEC 27002:2013, Control 13.1.1
- Norma ISO/IEC 27002:2013, Control 13.1.2

Propósito

En todo proyecto de Software, debe estar dentro de sus requisitos, un aspecto de seguridad que, ayude con la confidencialidad de la información almacenada, así como de la persona o personas que hacen uso de la aplicación, en la mayoría de casos, los datos de usuarios que tienen garantizado el acceso, se muestran en la barra de direcciones del navegador.

Convirtiéndose en un riesgo de seguridad, tanto para el usuario que ingresa, como para la empresa que mantiene la aplicación en sus servidores, por esto, se debe procurar en lo posible, que esta información, por ser tan sensible para todos los involucrados, no sea presentada.

Alcance

Los proyectos de software, cada vez deben tomar en consideración más aspectos de seguridad, la proliferación de personas en busca de puertas abiertas para poder ingresar y hacer de las suyas, hace indispensable que se tome en consideración estos detalles, al no permitir tener acceso a esta información, se estaría bloqueando de diferentes ataques que pudieran suceder

con la búsqueda de información con los datos presentados, es muy importante tomar en consideración para poder mitigar los riesgos.

Roles y Responsabilidades

La responsabilidad la llevaría directamente el área de desarrollo, puesto que en la construcción de la aplicación de Software es en donde se deben dejar sentados todos los requerimientos recopilados al iniciar el proyecto.

Definiciones

Puerta Abierta: Llámese a los puertos, o vulnerabilidades localizadas en un servidor o en una aplicación, que permita a través de ellas, el acceso para obtener el control y realizar actividades ajenas para las que fueron desarrolladas.

Historial de Revisiones

El historial de revisiones se lo debe llevar minuciosamente, en vista de que se debe verificar en que instante es el que se pueda presentar, de esta manera lograr corregirla antes de ponerla en producción lo que sería óptimo, o a su vez si ya está ejecutándose, pero se debe corregir este grave riesgo de vulnerabilidad.

- **Política No. 8: Cifrar la información.**

DESCRIPCIÓN

La información que se mantiene en las bases de datos, se encuentra tal como se la ingresa en los formularios o ventanas que tienen los diferentes aplicativos en el Consejo de la Judicatura, por lo tanto, si se efectúa la vulneración de los perímetros de seguridad, quien obtenga dicha información se encontrará con la facilidad que, simplemente con acceder a la base de datos, tendrá a su alcance todo lo que necesite.

Solamente realizando la explotación de seguridad que, no se encuentra cifrada, por eso es recomendable trabajar con un algoritmo de cifrado, lo cual permitirá que, quien logre vulnerar los cercos de seguridad por lo menos tenga un poco de trabajo para poder visualizar lo que ha obtenido.

Autoridad

- Norma ISO/IEC 27002:2013, Control 10.1.1
- Norma ISO/IEC 27002:2013, Control 10.1.2

Propósito

Cifrar la información es muy importante, al realizar un cifrado de la información, se logra mejorar significativamente la seguridad, tanto de la aplicación como de los servidores en donde se encuentran alojadas, el cifrado de información, permite que, si bien es cierto en algún momento la información puede ser alcanzada por personal que logre vulnerar las seguridades, no sea tan fácil de identificar la información que se está enviando a su verificación.

Alcance

Es necesario plantearse los objetivos como para guardar de una u otra manera, la información que puede circular a través de las redes de comunicaciones, y como se sabe, éstas no presentan una fidelidad del cien por ciento, entonces al cifrar la información emitida en estos canales de comunicación, nos brindarán un mejoramiento sustancial en la dificultad que se implementará para cubrir ciertas vulnerabilidades en los servidores y sus aplicaciones.

Roles y Responsabilidades

El área de desarrollo tendrá como responsabilidad el generar, un sistema de cifrado de la información, o a su vez el aplicar un sistema existente, el que permitirá reducir o mitigar el riesgo de que sean explotadas las vulnerabilidades existentes, y que pueda ser utilizada de manera fraudulenta la información ingresada.

Definiciones

Cifrado: Cifrar la información no es más que realizar un cambio a la información original, capaz que, si es intervenida, no pueda ser de fácil legibilidad para quien logró intervenirla.

Historial de Revisiones

Se llevará un registro exhaustivo, con fechas y que cosas fueron realizadas, de manera que se pueda determinar cuándo y como fue vulnerado el servicio, y poder tomar las correcciones necesarias para que el riesgo logre reducirse.

- **Política No. 9: Mantener el Software Actualizado.**

DESCRIPCIÓN

Para nadie es desconocido que, todo Sistema Operativo, Software de Utilidad, Ofimática y demás, sea del tipo que sea, con licencia o libre, en el momento de su lanzamiento siempre encontrará detractores, los mismos que se encargarán a futuro de buscar, encontrar, y lo que es más importante, explotar las vulnerabilidades que puedan encontrar.

Pero también, no es menos sabido que, las mismas empresas tratan en lo posible de tapar las vulnerabilidades encontradas, lanzando actualizaciones que contendrán estos parches para que el Software que, está siendo utilizado por cualquier usuario, pueda ser utilizado con la mayor seguridad posible.

Es por esto que una de las políticas y muy importante sería, mantener todo el Software utilizado dentro de la institución, con las últimas actualizaciones, esto con la finalidad de que, se instalen los parches a medida que sean publicados por parte del fabricante del producto.

Sin que exista la necesidad de que el Software sea licenciado, o sea Software Libre, puesto que no hay sistema cien por ciento seguro, y conforme siguen presentándose las vulnerabilidades se van presentando sus parches.

Autoridad

- Norma ISO/IEC 27002:2013, Control 12.5.1

Propósito

El propósito de aplicar esta política es, mantener el software de gestión, con las actualizaciones importantes, instaladas en los equipos, pues un Software desactualizado es

una puerta muy amplia para permitir el ingreso de atacantes, y por ende, es más fácil para ellos, interceptar la información que se debe proteger.

Alcance

Es muy importante tomar en consideración la política de actualización, porque, el mantener actualizado el software hace que se obtengan los últimos parches de seguridad, necesarios para que el Software instalado en el equipo no sea blanco de atacantes sean internos o externos.

Roles y Responsabilidades

El área de infraestructura, en coordinación con el área de desarrollo, serán los responsables por permitir en los diferentes sistemas que se utilizan, la normativa, de permitir que el Software se actualice periódicamente, conforme las empresas continúen lanzando nuevas actualizaciones, es decir deberán permitir su descarga e instalación.

Definiciones

Software de Gestión: Programas instalados en los equipos, que se utilizan como base para la realización de actividades dentro de ellos.

Historial de Revisiones

Se deberá llevar un registro con fecha y hora, así como la revisión periódica, con el propósito de tener el conocimiento de, cuando fue la última vez que se actualizó, y que actualizaciones fueron instaladas, y poder verificar si hace falta alguna y en caso de faltar, realizar la instalación.

- **Política No. 10: No permitir la opción de copiar y pegar**

DESCRIPCIÓN

Los funcionarios normalmente buscamos la mayor facilidad para poder ingresar nuestros datos sin mucho esfuerzo, y es por esto que, la opción de copiar y pegar, se hace una

“herramienta” muy útil al momento de poder ingresar las credenciales para que luego sean validadas para poder seguir utilizando los aplicativos.

Al no permitirle al funcionario el uso de las opciones de copiar y pegar, se reduce también el riesgo de sufrir ataques cuando se utilizan credenciales personales para los aplicativos indiferentemente que éstos sean internos o externos.

Autoridad

- Norma ISO/IEC 27002:2013, Control 13.1.2

Propósito

Los funcionarios que no forman parte del área de TIC’s, y no solamente ellos, también gente involucrada en el área, buscan la manera de cómo ahorrar tiempo, sin tener que escribir ni el nombre ni su contraseña, y es por ello que, guardan esos datos en un archivo de texto, el cual abren cuando quieren utilizar sus credenciales a las que únicamente hacen copiar y pegar en el cuadro de texto destinado para cada una y no tienen la necesidad de digitar.

De esta manera se “ahorran tiempo” o simplemente se “evitan la fatiga”, para evitar que esto suceda, se debe procurar una socialización con responsabilidades para que concienticen y empiecen a empoderarse ellos también en la seguridad de la información.

Alcance

Esta política se la debe socializar y concientizar en todos los funcionarios de la entidad, así se logrará reducir el riesgo de que, alguien pueda apoderarse de las credenciales de algún funcionario y poder tomar control para realizar actividades ilícitas dentro de los servidores de la empresa y poder llegar a hacer daño.

Roles y Responsabilidades

El área de infraestructura, en coordinación con el área de desarrollo, y coordinando con Talento Humano y Comunicación, se podrán determinar los medios necesarios para difundir, a las personas que laboran desde antes de aplicar las políticas de seguridad y para que quienes ingresen por primera vez las conozcan y las practiquen desde el principio.

Definiciones

Ilícito: Actividad que no se encuentra enmarcada en los parámetros legales o permitidos para su realización.

Historial de Revisiones

Se debe tomar en consideración llevar un control con fecha de quienes no lo están aplicando y poder ingerir de mejor manera en ellos, para que, se vaya reduciendo cada vez más, el personal que insiste en llevar a cabo estas actividades.

- **Política No. 11: No permitir guardar contraseñas**

DESCRIPCIÓN

Cuando el usuario de un aplicativo, requiere ingresar credenciales solicitadas, al momento de enviar el formulario, el navegador le realiza un cuestionamiento, que si desea recordar la contraseña para ser utilizada en posteriores ingresos al aplicativo, la comodidad de ser recordado y no tener que estar digitando en cada ingreso las credenciales de autenticación, nos hace guardar la contraseña, la misma que se encontraría a la mano de un atacante si llegara a tomar el control del equipo y así tratar de escalar hasta lograr llegar al servidor

Autoridad

- Norma ISO/IEC 27002:2013, Control 13.1.2

Propósito

Al igual que la política anterior, esto se debe inducir al funcionario, para que, no utilice el guardar las contraseñas, hoy en día y desde siempre, la política de los navegadores de internet, ha sido y seguirá siendo, facilitar su uso a quién lo haga, es por eso que se debe tratar de mantener desactivada esta opción, lo que se puede lograr en las configuraciones del navegador.

Alcance

El no permitir, o no mantener las contraseñas guardadas, tanto en el navegador, como en algún archivo, si bien es cierto no elimina el riesgo, pero si limita un poco a quienes tratan de utilizar esta vulnerabilidad para realizar su explotación.

Roles y Responsabilidades

El área de infraestructura, en coordinación con el área de desarrollo, y coordinando con Talento Humano y Comunicación, se podrán determinar los medios necesarios para difundir a las personas que laboran desde antes de aplicar las políticas de seguridad y para que quienes ingresen por primera vez las conozcan y las practiquen desde el principio.

Definiciones

Explotación: "Uso indebido" de una vulnerabilidad que tiene una aplicación de Software, la misma que se realiza a través de varios medios.

Historial de Revisiones

Se debe tomar en consideración que, esta configuración se la debe realizar in situ, es decir se debe desactivar la opción en cada uno de los equipos que se utilizan para acceder a la red.

- **Política No. 12: Mantener respaldos actualizados periódicamente.**

DESCRIPCIÓN

Como complemento de la ejecución de todas las políticas que se están desarrollando dentro del presente trabajo, se deberá mantener respaldos actualizados de todos los aplicativos que se encuentren en proceso.

Esto, se lo debe realizar en vista de que, si ocurriese algún tipo de desastre de cualquier índole que pueda presentarse, siempre es necesario continuar con lo que se venía realizando, y si no se ha respaldado lo que se ha avanzado, se debería empezar desde cero, un lujo que ningún desarrollador se puede dar.

Para presentar las aplicaciones siempre se imponen plazos que se deben cumplir, estos mismos plazos no se llegarían a concretar si no se van obteniendo respaldos periódicos, de tal forma que, cuando se retome el aplicativo para concluir con su ejecución de la mejor manera.

Hay que tomar en consideración que no estamos libres de cualquier tipo de desastre, y por esta razón debemos estar prevenidos, a parte de todas las prevenciones que deben hacerse para poder sobrellevar algún fenómeno que se pudiera presentar.

Autoridad

- Norma ISO/IEC 27002:2013, Control 12.3.1

Propósito

Todo esfuerzo que se realice para mantener la información segura, en caso de que se diera un desastre, no será suficiente, puesto que los respaldos no se los realiza de manera simultánea como van ingresando al servidor principal (Se lo debería hacer), respaldar la información con periodos de tiempo no muy alejados el uno del otro, es decir lo más rápido posible de un respaldo a otro.

En caso de información muy sensible, podría ser a diario, aunque sería recomendable mantener un servidor de almacenamiento que respalde las diferentes transacciones a la vez que se van realizando en el servidor principal.

Alcance

Realizar respaldos periódicos sin ser distantes los respaldos unos de otros, no asegura pero si permite que, la información se pueda restablecer muy rápido en caso de suceder alguna intrusión en los servidores, poder tener al alcance de la mano la información y restablecer los servicios lo más rápido que fuera posible, siendo esa la manera que debe actuar una empresa para no mantener sus servicios abajo por mucho tiempo.

Roles y Responsabilidades

La responsabilidad estará estrictamente bajo el área de infraestructura, quienes serán los responsables directos de mantener actualizados y asegurados los respaldos, los mismos que,

deberán estar disponibles en cualquier momento, para que, si llega a suceder, se pueda restaurar a la mayor brevedad posible, no existe empresa que esté libre de ser vulneradas sus seguridades, así que siempre hay que tomar todas las precauciones necesarias.

Definiciones

Respaldo: Acción de almacenar información sensible para ser utilizada en cualquier momento que se necesite.

Historial de Revisiones

Todas las actualizaciones deberán utilizar un formato único, y con su respectiva fecha, para saber qué es y si se ese segmento de información ha sido o no afectado como para necesitar ser restaurada.

- **Política No. 13: Concientizar al personal interno.**

Todo lo que se acaba de describir en las políticas no tendría validez de ninguna naturaleza, si al usuario interno no se le concientiza acerca de los riesgos que se corre tanto el funcionario como la institución.

Por ello, es necesario concientizar desde adentro, es decir, a todos nuestros usuarios internos, se los debe mantener concientizados acerca de la importancia de la cultura de seguridad, caso contrario, serán una puerta abierta hacia la pérdida de uno de los activos más grandes que tienen las empresas, su información.

Una de las principales causas para que se puedan explotar las vulnerabilidades, se da porque el usuario interno, no le dedica el cuidado necesario para asegurar los activos de los posibles riesgos que se pudieran presentar, además, por la falta de implementación de las políticas necesarias, que se deberían seguir precisamente para que, desde el usuario interno exista la plena conciencia de SEGURIDAD DE LA INFORMACIÓN, y así sumarse a los diferentes departamentos que se están preocupando para prevenir ataques constantemente.

Algo que no se debe olvidar, es la "***SOCIALIZACION***" de las políticas, cuando se habla de políticas, no se puede decir "*tengo las políticas pero las tengo guardadas*", expresiones que por cualquier razón, motivo, o circunstancia no tiene ninguna validez si no se ha socializado con el

personal involucrado, es decir todos quienes forman parte de la organización, todos esos usuarios deben conocer las políticas, por un principio básico de tener las herramientas para poder utilizarlas.

Si quienes integran la institución, están completamente motivados, concientizados, y al mismo tiempo con todo el ánimo de participar activamente en la cultura de la Seguridad de la Información, pero no tienen conocimiento de las políticas, es como decir que a un barco le dejamos sin combustible para sus motores a la deriva en altamar.

4.2. Desarrollo de las pruebas

Antes de empezar a realizar las pruebas hay que tomar en consideración por lo menos la definición de lo que es un ataque, pues, eso es lo que se va a realizar para determinar si la aplicación presenta o no vulnerabilidades, y, eso es lo que realiza el software OWASP ZAP, definir qué es un ataque es muy sencillo:

Se establece que, un ataque, es el intento que se realiza de manera externa para vulnerar la falta de seguridad que presenta una aplicación, explotando de manera ilegal las debilidades o vulnerabilidades, permitiendo así que, una fuerza extraña o ajena a la empresa cumpla su objetivo de explotar dichas vulnerabilidades.

Generalmente cuando se desarrolla Software, no se toma en consideración ninguna política de seguridad para cumplir con este objetivo, el mismo que se plantea por parte de una empresa que requiere una solución para mantenerse junto con los avances y facilidades que brinda la informática en la actualidad.

Para poder establecer de mejor manera cuáles han sido los resultados obtenidos se han desarrollado dos prototipos, los mismos que mostrarán con que vulnerabilidades empieza la aplicación, que servirá para que, más adelante aplicar las políticas y verificar si se ha mitigado de buena manera las vulnerabilidades encontradas al programar.

Al desarrollar las pruebas se ha encontrado que, el servidor que se ha escogido, sin necesidad de tener levantado un firewall (que será necesario utilizar para mejorar el nivel de seguridad), no presenta demasiadas vulnerabilidades de acuerdo con el OWASP ZAP 2.5, presentamos la captura de los ataques que se desarrollan, recalcando que el servicio de firewall se encuentra desactivado.

Es muy importante destacar que, no se ha activado el firewall, porque a pesar de ser un aspecto de seguridad demasiado importante y, se lo debe tener configurado, es una opción que está fuera del alcance de un desarrollador, puesto que, quienes tienen esta obligación, son las personas encargadas de la configuración de los servidores.

Al realizar el desarrollo no es éste el departamento que realiza dichas configuraciones, pues, es allí en donde se realizará la configuración de quienes son las personas que pueden realizar o no ciertas tareas propias del servidor y no de desarrollo de software.

Para determinar si el servidor se encuentra en ejecución, utilizamos la URL: http://ipservidor:8080, la presente prueba se la está realizando con la dirección IP 10.18.33.32, es decir nuestra URL del servidor para las pruebas será http://10.18.33.32:8080, al realizar las primeras pruebas obtendremos los datos y pantallas que se muestran a continuación:

4.2.1. Pruebas realizadas hacia el servidor.

Para determinar que el servidor se encuentra desactivado van las siguientes imágenes:
Al ubicar la URL del servidor JBOSS que se utiliza en este prototipo, http://10.18.33.32:8080, en la figura, se mostrará la dirección IP que se está utilizando en el equipo servidor, el mismo contiene el servidor y en el se encuentra alojada nuestra aplicación de Software.

La figura que sigue presentará la configuración IP con la que se procederá a realizar las pruebas correspondientes

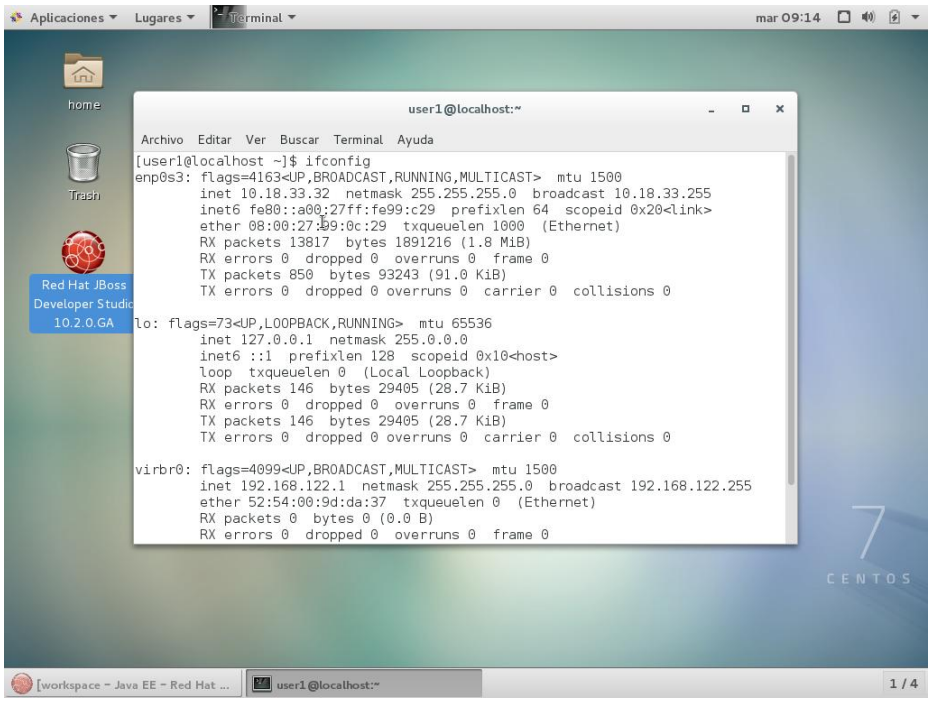

Figura 1-4: Dirección IP para pruebas
Realizado por: Renny Montalvo 2017

4.2.1.1. Pruebas al servidor que no ha sido levantado.

Continuando con las figuras que van a presentar las diferentes pruebas realizadas, en la próxima figura que se presenta, se puede evidenciar que el servidor no se encuentra levantado.

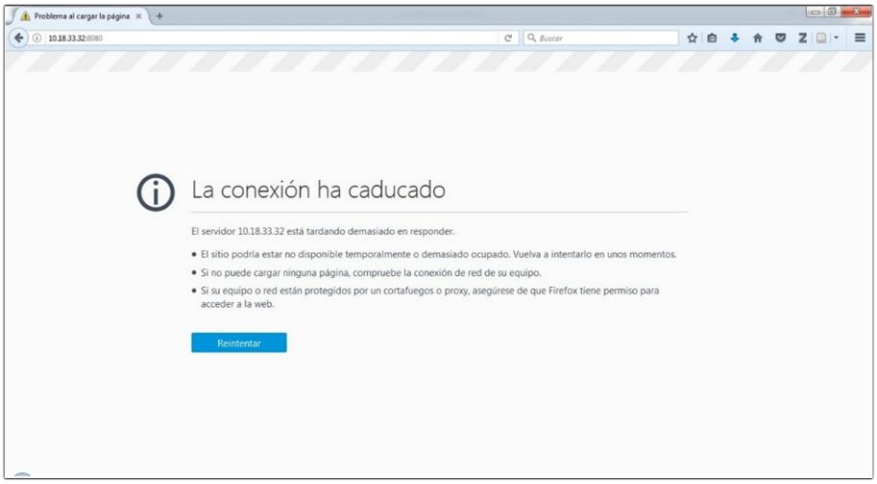

Figura 2-4: Servidor no levantado
Realizado por: Renny Montalvo 2017

La siguiente figura demostrará que el servidor se encuentra sin haberse iniciado.

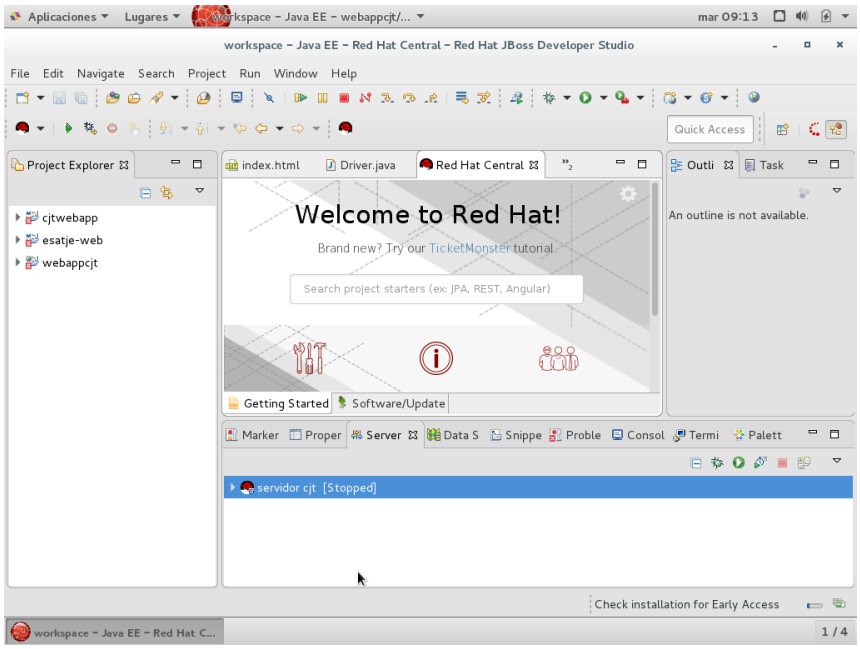

Figura 3-4: Servidor sin iniciar
Realizado por: Renny Montalvo 2017

Antes de empezar a realizar los ataques, la siguiente figura presentará el firewall inactivo en el equipo que hace de servidor (Máquina Virtual), lo que haría más sencillo el uso de cualquier herramienta para vulnerar las seguridades de una aplicación de Software.

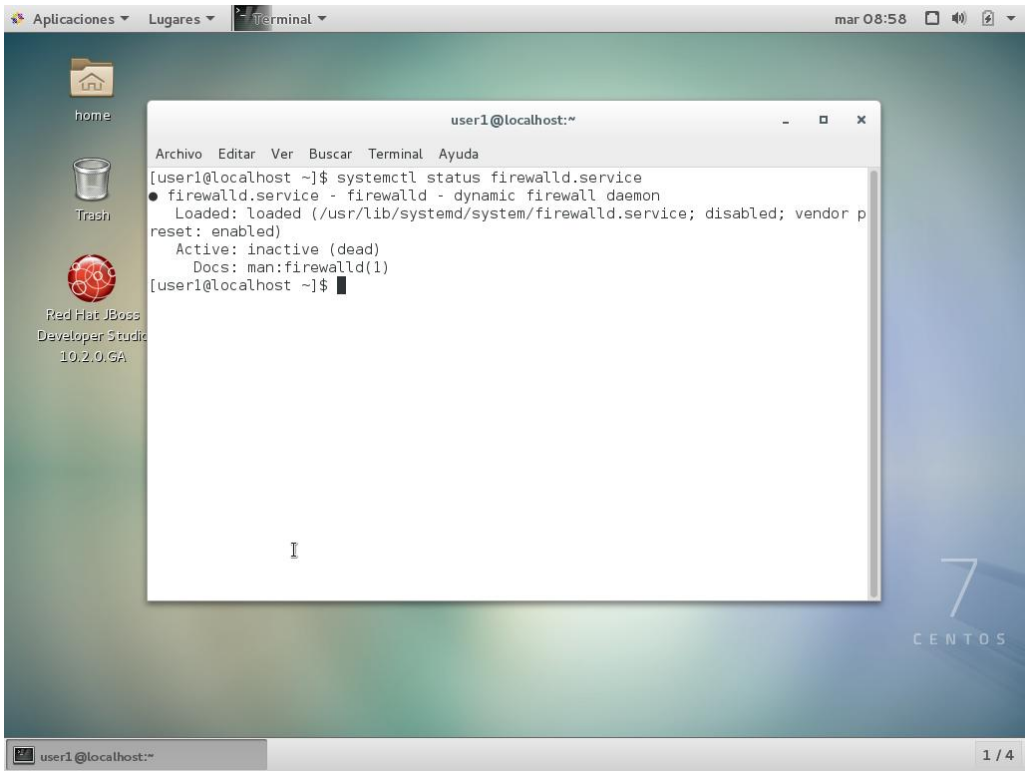

Figura 4-4: Firewall desactivado.
Realizado por: Renny Montalvo 2017

Ahora se empieza con la realización de ataques a través de la herramienta que habíamos mencionado anteriormente, para ello la siguiente figura presenta el ataque realizado al servidor mientras se encuentra en estado down, es decir aún no ha sido levantado.

Al verse la información que se encuentra en la figura, se verá la manera como no presenta ningún resultado, todo lo contrario, presenta un mensaje de que "el ataque a la URL ha fallado: Connection refused: connect".

Esto está dando la indicación de que el servidor no ha sido levantado, y se encuentra rechazando todas las conexiones entrantes, es decir, no se encuentra habilitado, más adelante se presentará la información de los servicios ya levantados.

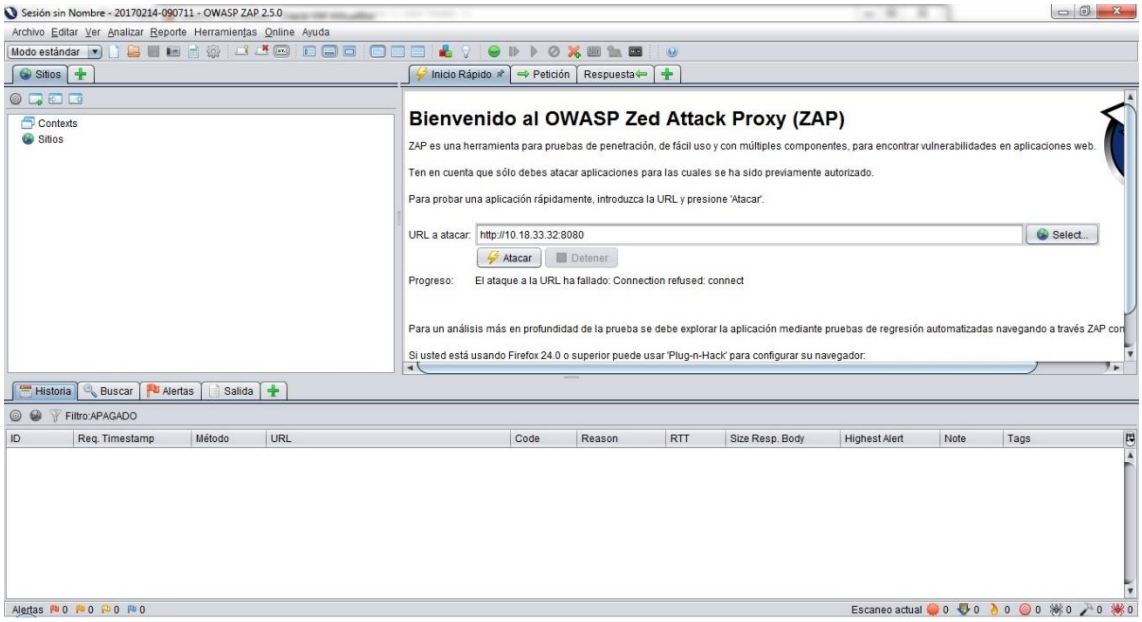

Figura 5-4: Ataque fallido.
Realizado por: Renny Montalvo 2017

Culminando con el ataque que se ha realizado al servidor sin haberse levantado, ahora se puede continuar con el ataque y la presentación del mismo, pero ahora si con el servidor levantado:

4.2.1.2. Pruebas al servidor en funcionamiento.

Esta figura presenta el servidor ya levantado.

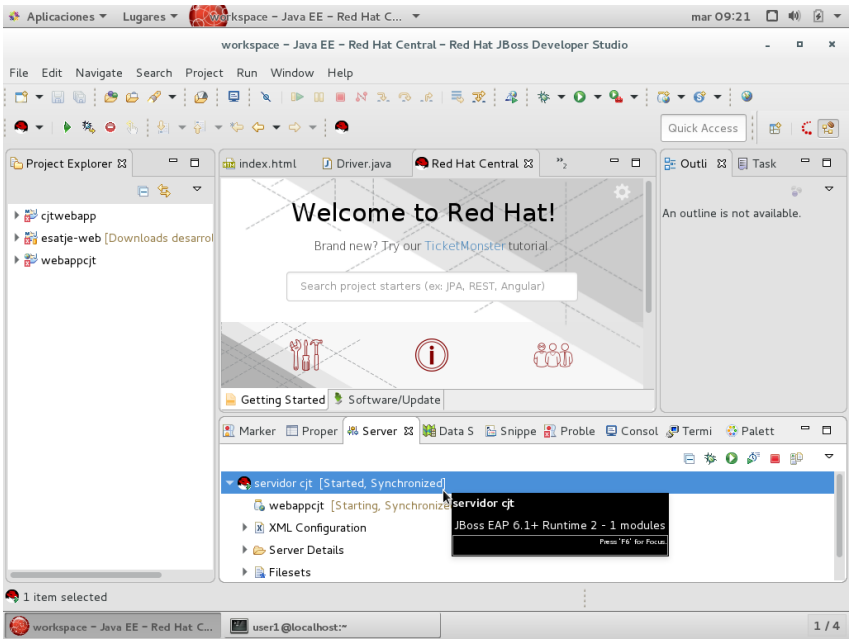

Figura 6-4: Servidor levantado
Realizado por: Renny Montalvo 2017

Al momento de verificar si el servidor se encuentra habilitado, presentará una página como se muestra en la figura.

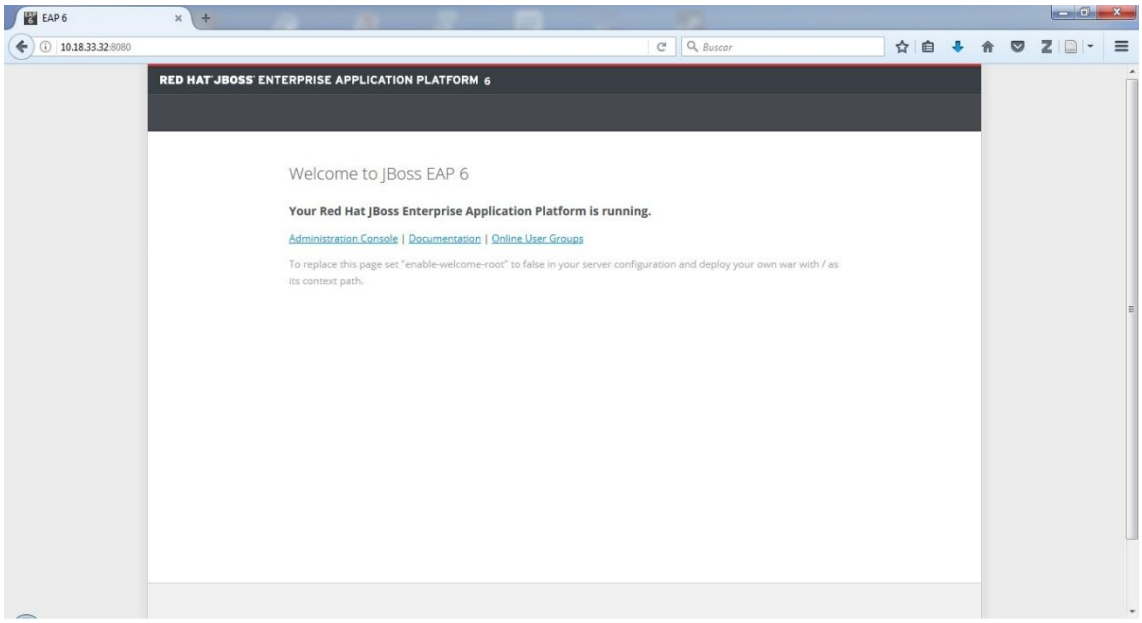

Figura 7-4: Página de Servidor levantado
Realizado por: Renny Montalvo 2017

Luego de verificar si el servidor se encuentra levantado, se procede a realizar el ataque por intermedio de la herramienta seleccionada para el efecto.

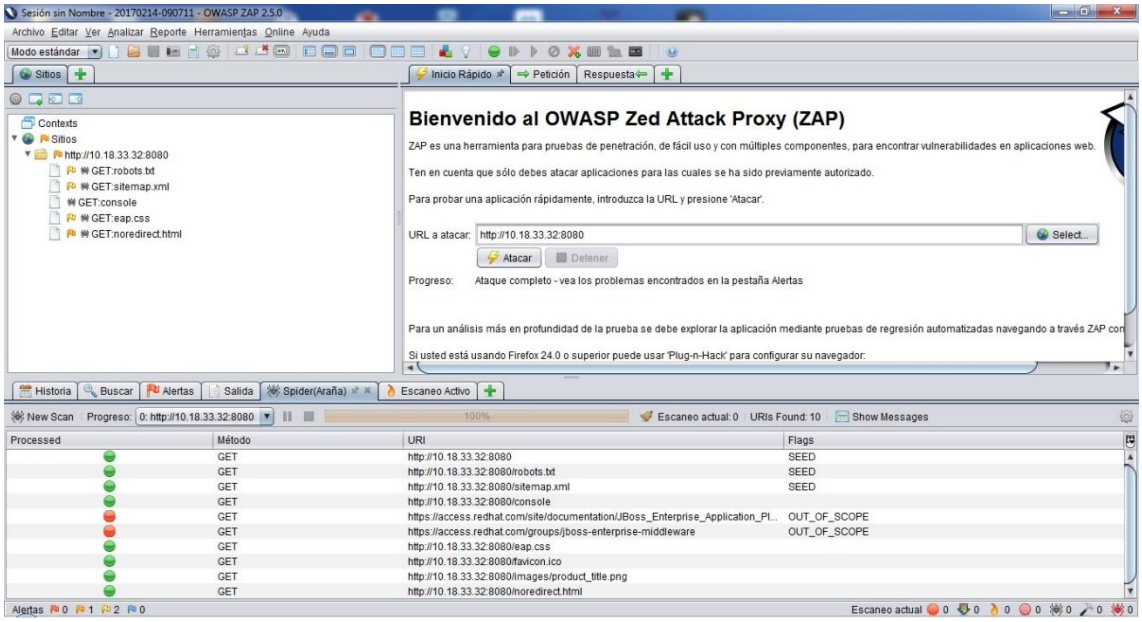

Figura 8-4: Ataque a Servidor levantado
Realizado por: Renny Montalvo 2017

Luego de haber culminado con el ataque la herramienta presenta sus resultados, así como en la siguiente figura.

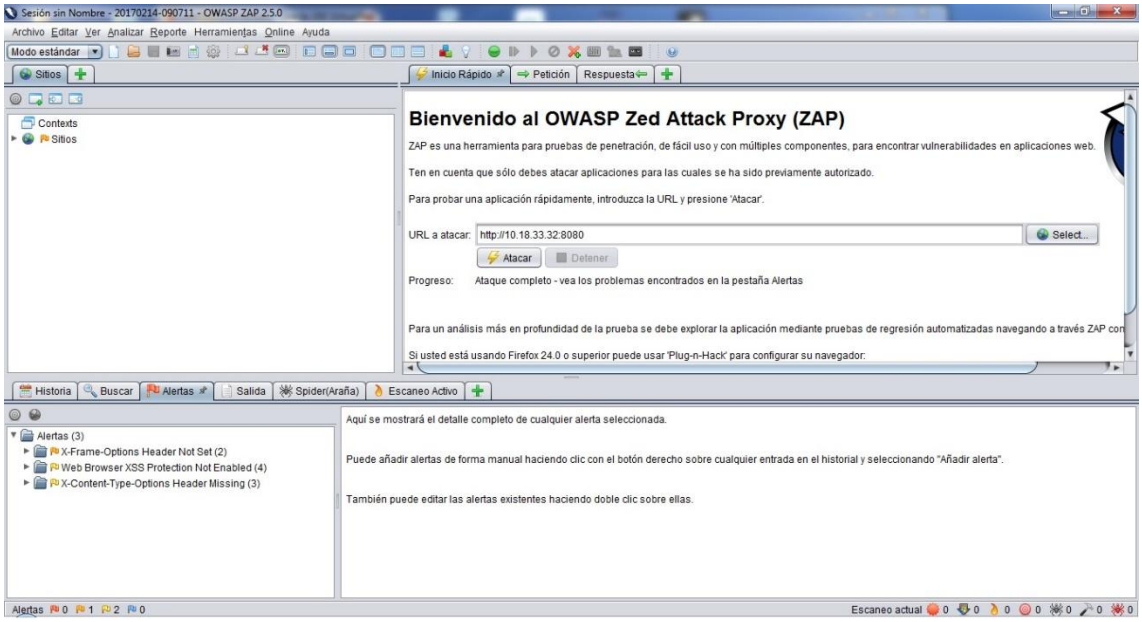

Figura 9-4: Resultado de ataque a Servidor levantado
Realizado por: Renny Montalvo 2017

Esta es la secuencia de lo realizado para atacar al servidor, que si bien es cierto, no es parte de la presente investigación, si influye en su realización, porque, las aplicaciones, deberían

obligatoriamente estar alojadas en un servidor, y por ser su punto de anclaje se debería también realizar estos análisis.

A continuación, se empieza con las pruebas realizadas para los prototipos de donde se tomarán los datos para tomar una decisión que conlleve a la aplicación o no de las nuevas políticas de seguridad en el Consejo de la Judicatura de Tungurahua.

4.2.1.3. Pruebas Prototipo 1

Para la realización de las pruebas en el Prototipo I, se volvieron a realizar las pruebas con el OWASP ZAP, al igual que al realizar las pruebas del servidor, en la aplicación que se ha desarrollado para el efecto, que no cuenta con las debidas medidas de seguridad, que impidan de una u otra manera la explotación de vulnerabilidades existentes en la aplicación.

Realizadas las pruebas, los resultados se muestran en la figura.

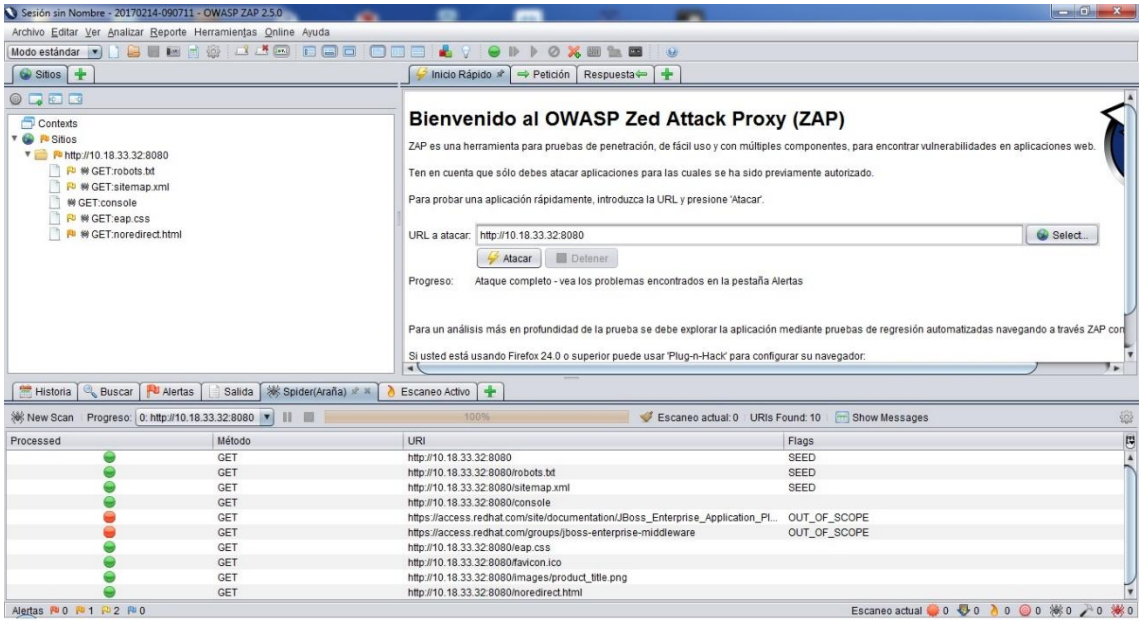

Figura 10-4: Ataque a Prototipo 1
Realizado por: Renny Montalvo 2017

4.2.1.4. Pruebas Prototipo 2

Luego de que se han aplicado las políticas generadas en el presente trabajo de investigación, se presentará que se redujeron las vulnerabilidades significativamente, permitiendo la aplicación de los diferentes estudios que, para la demostración de la hipótesis más adelante, será muy significativo, y, ayudará a comprobar si han sido bien escogidas o no éstas Políticas.

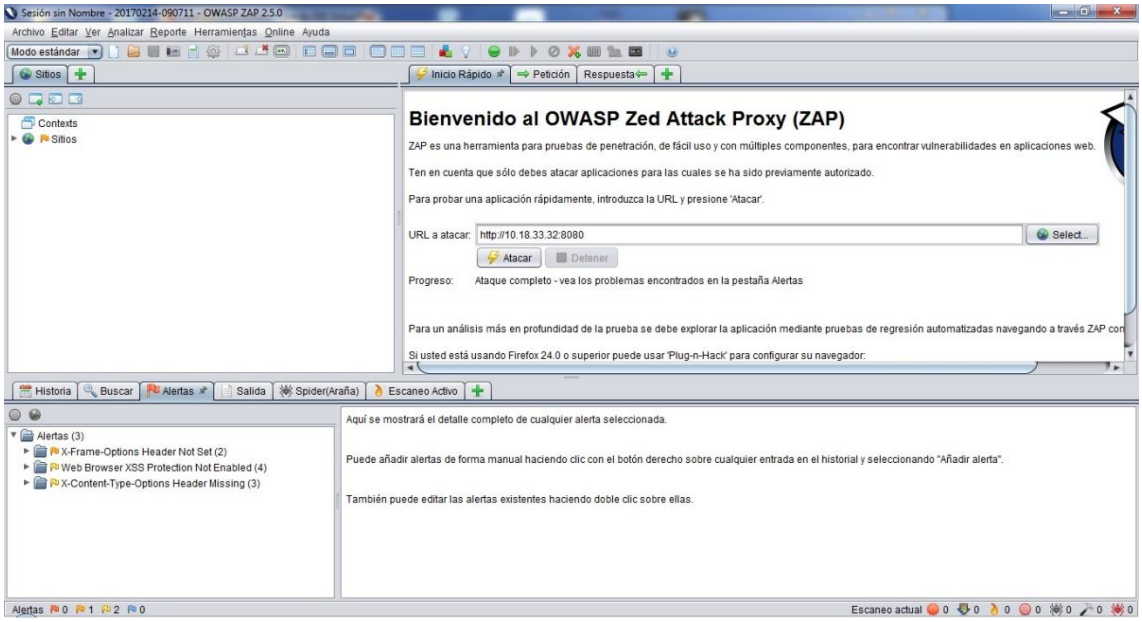

Figura 11-4: Ataque a Prototipo 2
Realizado por: Renny Montalvo 2017

4.3. Análisis y comparación de resultados

Habiendo determinado la ponderación de vulnerabilidades, se debe realizar el análisis de vulnerabilidades, para saber cuáles son las más relevantes y así poder realizar los correctivos necesarios y poder mitigar los riesgos que incidan más para la seguridad de los aplicativos.

4.3.1. Análisis de la situación actual.

Dentro de la encuesta se establece la probabilidad de ocurrencia de un Riesgo establecido en función del promedio de las respuestas obtenidas a las preguntas establecidas para la evaluación de cada riesgo; es así que el cálculo de la probabilidad de ocurrencia del riesgo evaluado es igual a:

$$Probabilidad = \frac{Promedio\ de\ Respuestas\ positivas}{Total\ de\ ataques\ realizados}$$

Obteniéndose los siguientes resultados:

Tabla 1-4: Datos de respuestas Probabilidad de ocurrencia de riesgos identificados

Vulnerabilidad	**D1**	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**	**D9**	**D10**	**D11**	**D12**
A1 – Inyección	0	0	0	0	0	0	0	0	0	0	0	0
A2 – Pérdida de Autenticación y Gestión de Sesiones	1	0	1	0	0	1	0	0	0	1	1	1

A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	1	1	1	1	1	1	1	1	1	1	1	1
A4 – Referencia Directa Insegura a Objetos	0	1	0	0	0	0	1	1	0	0	0	0
A5 – Configuración de Seguridad Incorrecta	0	1	1	1	1	0	0	0	0	0	0	1
A6 – Exposición de Datos Sensibles	1	1	0	0	0	1	1	1	1	1	1	1
A7 – Ausencia de Control de Acceso a las Funciones	0	0	0	0	0	0	0	0	0	0	0	0
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	0	0	0	0	0	0	0	0	0	0	0	0
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0	0	0	0	0	0	0	0	0	0	0	0
A10 – Redirecciones y reenvíos no validados	1	0	0	1	1	1	0	0	0	1	1	1

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d.)

Para poder tabular se dará un valor a los ceros y unos, se tendrán las siguientes equivalencias:

Tabla 2-4: Ponderación de ocurrencia de riesgos identificados

Se vulnera	**Valor**
Si	1
No	0

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d., p. 18)

De esta forma se puede obtener una ponderación de ocurrencia evaluando el impacto de que ocurra el riesgo evaluado, en función a la escala de impacto definida anteriormente, para lo cual se obtiene los siguientes datos:

Tabla 3-4: Ponderación de ocurrencia de riesgos identificados

Vulnerabilidad	**Probabilidad**	**Impacto**	**Ponderación**
A1 – Inyección	0,17	4	0,68
A2 – Pérdida de Autenticación y Gestión de Sesiones	0,50	2	1
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	1,00	4	4
A4 – Referencia Directa Insegura a Objetos	0,25	1	0,25
A5 – Configuración de Seguridad Incorrecta	0,42	1	0,42
A6 – Exposición de Datos Sensibles	0,75	3	2,25
A7 – Ausencia de Control de Acceso a las Funciones	0,00	2	0
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	0,25	1	0,25
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0,00	1	0
A10 – Redirecciones y reenvíos no validados	0,58	3	1,74

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d.)

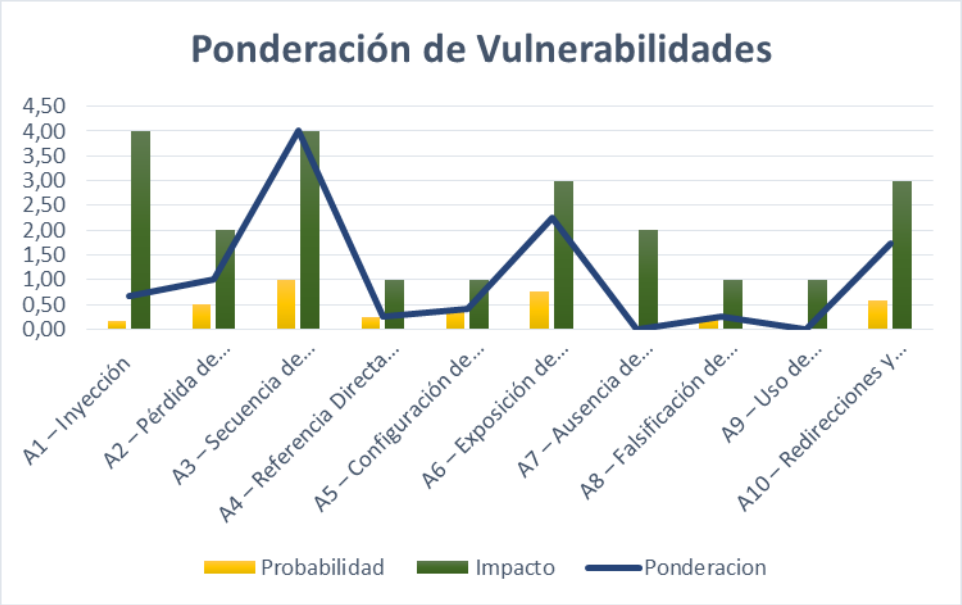

Gráfico1-4: Ponderación de riesgos.
Realizado por: Renny Montalvo 2017

Fuente: Personal

En base a este análisis se puede establecer que los riesgos de ponderación superior a los 2.5 puntos son los riesgos más críticos y a los que más atención se debe prestar, por lo que se debe implementar con mayor urgencia una solución para los siguientes riesgos ordenados de mayor a menor prevalencia en función a su ponderación:

Tabla 4-4: Riesgos de mayor prevalencia

Orden	Vulnerabilidad	Ponderacion
1	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	4
2	A6 – Exposición de Datos Sensibles	2,25
3	A10 – Redirecciones y reenvíos no validados	1,74
4	A2 – Pérdida de Autenticación y Gestión de Sesiones	1
5	A1 – Inyección	0,68

Realizado por: Renny Montalvo 2017

Fuente: Personal

De lo que se puede derivar que, la vulnerabilidad de Cross Site Scripting (XSS), por no utilizar las cabeceras que mitigan este tipo de vulnerabilidades, pues no se cuenta con una política que, ingiera en el uso de este tipo de soluciones.

La exposición de datos sensibles, es uno de los errores que más podría afectar a la organización, puesto que, si esta información se filtra, el atacante podría sin lugar a dudas, aprovechar la situación para ingresar al servidor y, de esta manera seguir escalando los privilegios, hasta tomar posesión de los activos ya mencionados, y luego estando con privilegios de administrador, poder realizar las acciones que haya tenido planificadas.

De acuerdo a lo mostrado en el análisis, se afecta gravemente la Confidencialidad, Privacidad, e Integridad de la información que si bien es cierto la gran mayoría de ella se encuentra visible para el público a través de Internet, también es cierto que, si existe información que no debe ser mostrada, y por lo tanto, se encuentra protegida y no puede ser divulgada.

4.3.2. Análisis de la situación Post-Implementación.

Habiéndose realizado la implementación de las políticas de seguridad, y al haberse aplicado en la aplicación prototipo, se han realizado nuevamente las pruebas de vulnerabilidades a través del OWASP ZAP, al igual que se hizo sin haberse aplicado las Políticas generadas, se han obtenido los siguientes resultados:

Tabla 5-4: Probabilidad de ocurrencia de riesgos identificados Post-Implementación

Vulnerabilidad	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12
A1 – Inyección	0	0	0	0	1	0	0	0	0	0	0	0
A2 – Pérdida de Autenticación y Gestión de Sesiones	0	0	0	0	0	0	1	0	1	0	0	0
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	0	1	0	0	0	1	0	0	1	0	0	0
A4 – Referencia Directa Insegura a Objetos	0	0	0	1	1	0	0	0	0	0	0	0
A5 – Configuración de Seguridad Incorrecta	0	0	0	0	0	0	0	0	0	0	0	1
A6 – Exposición de Datos Sensibles	0	0	0	0	1	1	0	1	0	0	0	0
A7 – Ausencia de Control de Acceso a las Funciones	0	0	0	0	0	0	0	0	0	0	0	0
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	0	0	0	0	0	0	0	0	1	0	0	0
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0	0	0	0	0	0	0	0	0	0	0	0
A10 – Redirecciones y reenvíos no validados	0	0	1	0	0	0	0	1	0	0	0	0

Realizado por: Renny Montalvo 2017

Fuente: Personal

Así mismo, al seguir la misma metodología, se pudo obtener la siguiente ponderación:

Tabla 6-4: Ponderación de ocurrencia de riesgos identificados Post-Implementación

Vulnerabilidad	Probabilidad	Impacto	Ponderación
A1 – Inyección	0,08	4	0,32
A2 – Pérdida de Autenticación y Gestión de Sesiones	0,17	2	0,34
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	0,25	4	1
A4 – Referencia Directa Insegura a Objetos	0,17	1	0,17
A5 – Configuración de Seguridad Incorrecta	0,08	1	0,08
A6 – Exposición de Datos Sensibles	0,25	3	0,75
A7 – Ausencia de Control de Acceso a las Funciones	0,00	2	0
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	0,08	1	0,08
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0,00	1	0
A10 – Redirecciones y reenvíos no validados	0,17	3	0,51

Realizado por: Renny Montalvo 2017

Fuente: Personal

La tabla y la ilustración muestran, la significativa mejora que existe al desarrollar, aplicaciones de Software aplicando las Políticas Generadas, contribuyendo de esta manera con la Seguridad de la Información en el Consejo de la Judicatura.

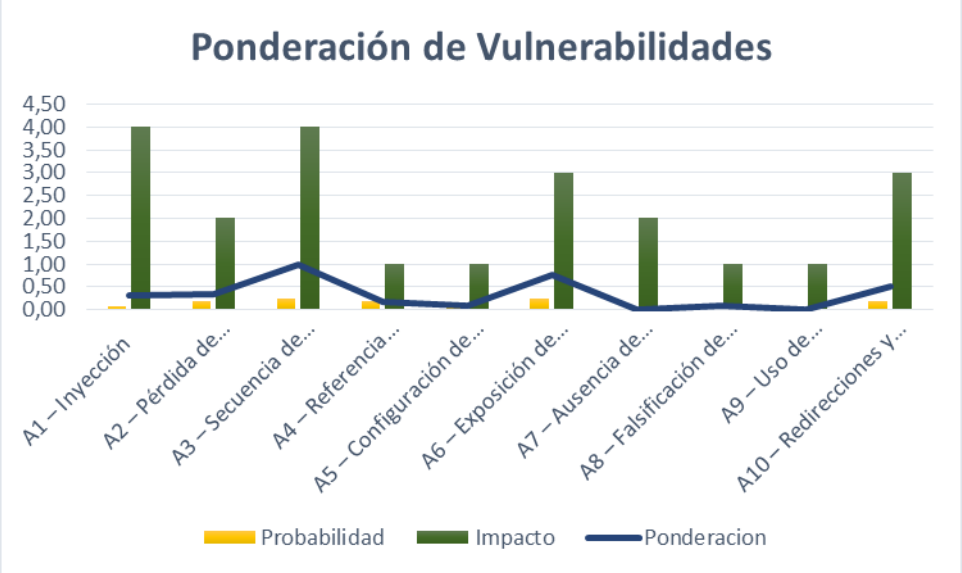

Gráfico 2-4: Ponderación de riesgos Post-Implementación.

Realizado por: Renny Montalvo 2017

Fuente: SPSS

La mejora sustancial presentada en el gráfico, puede decir que, las Políticas generadas, si muestran efectividad, y permite que se las pueda aplicar.

Tabla 7-4: Tabla cruzada

			SI				Total
			,00	1,00	2,00	3,00	
Vulnerabilidad	A1 – Inyección	Recuento	0	1	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A10 – Redirecciones y reenvíos no validados	Recuento	0	0	1	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A2 – Pérdida de Autenticación y Gestión de Sesiones	Recuento	0	0	1	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	Recuento	0	0	0	1	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A4 – Referencia Directa Insegura a Objetos	Recuento	0	0	1	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A5 – Configuración de Seguridad Incorrecta	Recuento	0	1	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A6 – Exposición de Datos Sensibles	Recuento	0	0	0	1	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A7 – Ausencia de Control de Acceso a las Funciones	Recuento	1	0	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A8 – Falsificación de Peticiones en Sitios Cruzados (CSR	Recuento	0	1	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A9 – Uso de Componentes con Vulnerabilidades Conocidas	Recuento	1	0	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
Total		Recuento	2	3	3	2	10
		Recuento esperado	2,0	3,0	3,0	2,0	10,0

Realizado por: Renny Montalvo 2017

Fuente: SPSS

4.4. Comprobación de Hipótesis.

Luego de haber realizado los diferentes análisis, y con los datos obtenidos, se procede a realizar el análisis con el método de la hipótesis nula de Chi-cuadrado (X^2), para lo cual definimos la hipótesis nula.

H_0= La generación de políticas para gestionar los riesgos de seguridad de la información, no permitirán mitigar las vulnerabilidades existentes en el desarrollo de software

H_1= La generación de políticas para gestionar los riesgos de seguridad de la información, permitirán mitigar las vulnerabilidades existentes en el desarrollo de software

Luego de establecer las Hipótesis, se procede a realizar el método con Chi-cuadrado, y se obtiene las siguientes tablas

Para generar la tabla de los resultados, se tomará en consideración los valores de vulneración antes y después, es decir, aquí se expondrá los valores de las vulnerabilidades que se han podido explotar, con políticas y, sin políticas.

Tabla 8-4: Probabilidades de vulnerabilidad

	ANTES		**DESPUÉS**	
Vulnerabilidad	**SI**	**Probabilidad**	**SI**	**Probabilidad**
A1 – Inyección	2	0,17	1	0,08
A2 – Pérdida de Autenticación y Gestión de Sesiones	6	0,50	2	0,17
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	12	1,00	3	0,25
A4 – Referencia Directa Insegura a Objetos	3	0,25	2	0,17
A5 – Configuración de Seguridad Incorrecta	5	0,42	1	0,08
A6 – Exposición de Datos Sensibles	9	0,75	3	0,25
A7 – Ausencia de Control de Acceso a las Funciones	0	0,00	0	0,00
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	3	0,25	1	0,08
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0	0,00	0	0,00
A10 – Redirecciones y reenvíos no validados	7	0,58	2	0,17

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d.)

Con estos valores, se procederá a realizar el cálculo.

Tabla 9-4: Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Vulnerabilidad * SI	10	90,9%	1	9,1%	11	100,0%

Vulnerabilidad * NO	10	90,9%	1	9,1%	11	100,0 %

Realizado por: Renny Montalvo 2017

Fuente: SPSS

Tabla 10-4: Tabla cruzada

			SI				
			,00	1,00	2,00	3,00	Total
Vulnerabilidad	A1 – Inyección	Recuento	0	1	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A10 – Redirecciones y reenvíos no validados	Recuento	0	0	1	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A2 – Pérdida de Autenticación y Gestión de Sesiones	Recuento	0	0	1	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	Recuento	0	0	0	1	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A4 – Referencia Directa Insegura a Objetos	Recuento	0	0	1	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A5 – Configuración de Seguridad Incorrecta	Recuento	0	1	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A6 – Exposición de Datos Sensibles	Recuento	0	0	0	1	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A7 – Ausencia de Control de Acceso a las Funciones	Recuento	1	0	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A8 – Falsificación de Peticiones en Sitios Cruzados (CSR	Recuento	0	1	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
	A9 – Uso de Componentes con Vulnerabilidades Conocidas	Recuento	1	0	0	0	1
		Recuento esperado	,2	,3	,3	,2	1,0
Total		Recuento	2	3	3	2	10
		Recuento esperado	2,0	3,0	3,0	2,0	10,0

Realizado por: Renny Montalvo 2017

Fuente: SPSS

Tabla 11-4: Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	30,000[a]	27	,314
Razón de verosimilitud	27,323	27	,446
N de casos válidos	10		

a. 40 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.

Realizado por: Renny Montalvo 2017

Fuente: SPSS

Al obtener los valores y trabajando con un Nivel de Significancia del 5%, se tiene lo siguiente:

Nivel de Significancia= 5% = 0,05

Grados de libertad= 27

p= 0,95

Chi-cuadrado crítico= 16,1514

Chi-cuadrado obtenido=30,000

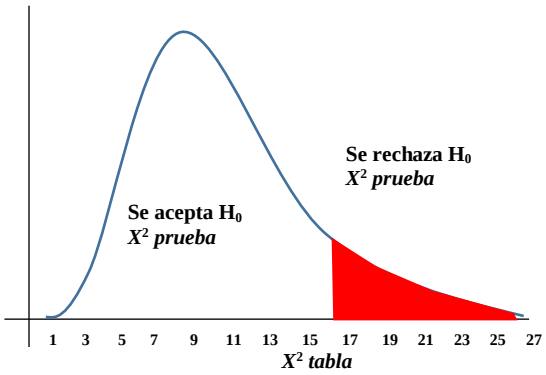

Gráfico 3-4: Curva de Chi Cuadrado

Realizado por: Renny Montalvo 2017

Fuente: SPSS

Como se puede observar en el gráfico, con valores de chi-cuadrado superiores a 16.1514, se rechaza la hipótesis nula.

El chi-cuadrado que se ha obtenido tiene un valor de 30, y como se presenta en el gráfico, está en el rango que se rechaza la hipótesis nula, por lo tanto, se demuestra la validez de la hipótesis planteada al inicio de la presente investigación, y se lo presenta en las siguientes tablas:

Resultados del análisis de riesgos al desarrollar Software sin aplicar las Políticas Generadas:

Tabla 12-4: Probabilidades de Riesgo antes de aplicar las políticas.

	ANTES		
Vulnerabilidad	**SI**	**NO**	**Probabilidad**
A1 – Inyección	2	10	0,17
A2 – Pérdida de Autenticación y Gestión de Sesiones	6	6	0,50
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	12	0	1,00
A4 – Referencia Directa Insegura a Objetos	3	9	0,25
A5 – Configuración de Seguridad Incorrecta	5	7	0,42
A6 – Exposición de Datos Sensibles	9	3	0,75
A7 – Ausencia de Control de Acceso a las Funciones	0	12	0,00
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	3	9	0,25
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0	12	0,00
A10 – Redirecciones y reenvíos no validados	7	5	0,58

Realizado por: Renny Montalvo 2017

Fuente: (Alvaro Machaca, n.d.)

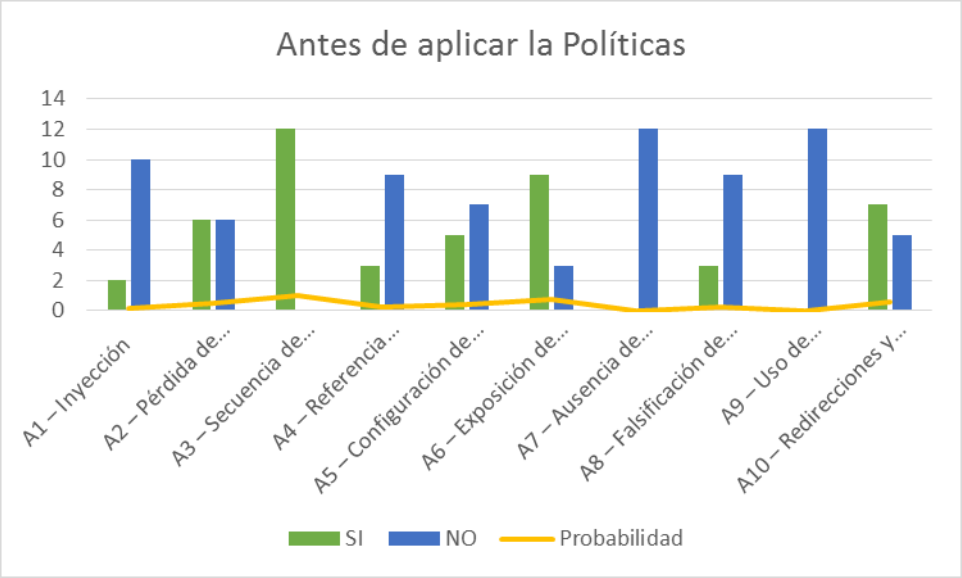

Gráfico 4-4: Probabilidad de riesgo antes de aplicar las políticas.
Realizado por: Renny Montalvo 2017

Fuente: Personal

Los resultados obtenidos luego de aplicar las Políticas Generadas se presentan a continuación:

Tabla 13-4: Probabilidades de Riesgo después de aplicar las políticas.

	DESPUES		
Vulnerabilidad	**SI**	**NO**	**Probabilidad**
A1 – Inyección	1	11	0,08
A2 – Pérdida de Autenticación y Gestión de Sesiones	2	10	0,17
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	3	9	0,25
A4 – Referencia Directa Insegura a Objetos	2	10	0,17
A5 – Configuración de Seguridad Incorrecta	1	11	0,08
A6 – Exposición de Datos Sensibles	3	9	0,25
A7 – Ausencia de Control de Acceso a las Funciones	0	12	0,00
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	1	11	0,08
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0	12	0,00
A10 – Redirecciones y reenvíos no validados	2	10	0,17

Realizado por: Renny Montalvo 2017

Fuente: Personal

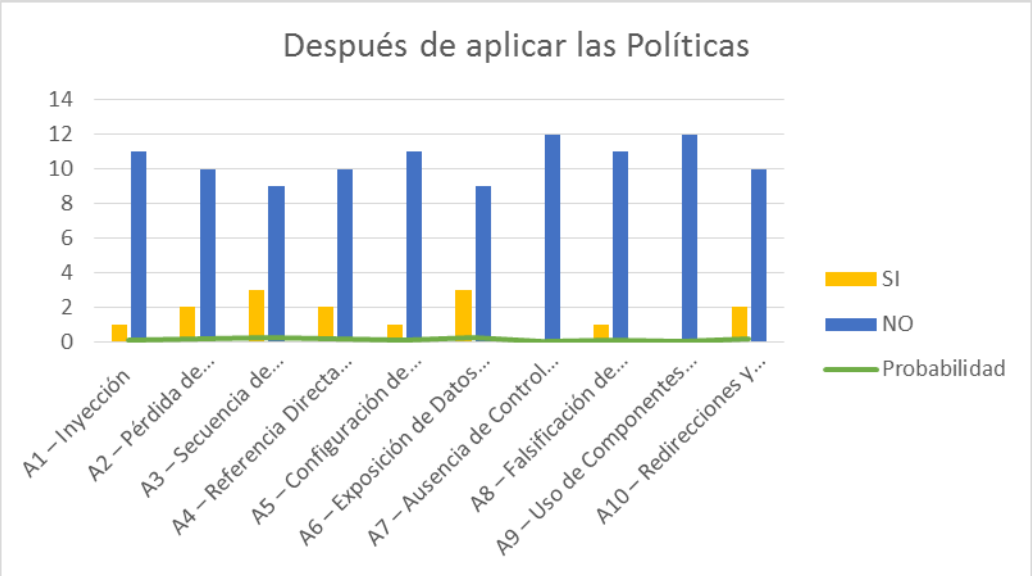

Gráfico 5-4: Probabilidad de riesgo después de aplicar las políticas.
Realizado por: Renny Montalvo 2017

Fuente: Personal

En la siguiente tabla, con su respectivo gráfico, se podrá observar la diferencia que existe de la probabilidad de que un riesgo pueda llegar a ocurrir, antes y después de haber aplicado las políticas generadas.

Tabla 14-4: Cuadro comparativo de la probabilidad de ocurrencia del riesgo.

Vulnerabilidad	ANTES	DESPUES
A1 – Inyección	0,17	0,08

A2 – Pérdida de Autenticación y Gestión de Sesiones	0,5	0,17
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	1	0,25
A4 – Referencia Directa Insegura a Objetos	0,25	0,17
A5 – Configuración de Seguridad Incorrecta	0,42	0,08
A6 – Exposición de Datos Sensibles	0,75	0,25
A7 – Ausencia de Control de Acceso a las Funciones	0	0
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	0,25	0,08
A9 – Uso de Componentes con Vulnerabilidades Conocidas	0	0
A10 – Redirecciones y reenvíos no validados	0,58	0,17

Realizado por: Renny Montalvo 2017

Fuente: Personal

Gráfico 6-4: Cuadro comparativo de la probabilidad de ocurrencia del riesgo.
Realizado por: Renny Montalvo 2017

Fuente: Personal

4.5. Recomendaciones de Políticas de Seguridad

Al realizar el desarrollo de Software, como se ha manifestado en el transcurso de la presente investigación, no se toma en consideración ninguna política de seguridad, y por esta razón, en su mayoría las aplicaciones de Software que se generan, incrementan el riesgo de permitir el ataque a una o varias vulnerabilidades, por lo tanto, como se ha demostrado en el capítulo anterior, es necesario seguir o cumplir con ciertas normas técnicas que permitan construir un Software seguro.

4.6. Recomendaciones de formación

La formación, es un aspecto demasiado importante dentro del desarrollo de aplicaciones de Software, puesto que, actualmente, se siguen descubriendo plataformas, herramientas, y Software que ayudan para generar estas aplicaciones, el estar formándose, enterándose, y capacitándose en

las nuevas tecnologías, permitirán que la competitividad del desarrollador siga en aumento, por ende, se revalorizará su capacidad y tendrá mejores réditos de lo que se esté proponiendo.

4.7. Recomendaciones para Desarrollar Software.

Siempre en las aulas de clase, se dice a quienes se encuentran en la etapa de formación y en búsqueda de conocimientos para lograr un mejor futuro, que se deben respetar los ciclos de vida para el Desarrollo de Software, pero, quien recibe la formación, poco o nada hace caso de dichas recomendaciones.

Precisamente por ello, es necesario que, se siga el ciclo de vida del software de manera completa, para que, de esta manera, se pueda lograr mantener un software que cumpla con todas las especificaciones recomendadas al inicio, poniendo mucho énfasis en la requerimientación, hay que tomarse el tiempo necesario para tomar todos los requerimientos que tenga el dueño del producto o, quien lo vaya a utilizar.

No deje de lado ninguno de los pasos o fases, siempre documente todo, y siempre haga llegar al interesado sus requerimientos por escrito, y mantenga su aceptación de la misma manera, se estaría disciplinando tanto quien desarrolla como quien va a utilizar el producto, para evitar cambios de última hora que puedan retrasar el proyecto, e incluso, si se necesita realizar algún cambio o inclusión de última hora poderlo lograr sin salirse del presupuesto.

¿Por qué se menciona lo del presupuesto? será la primera pregunta que se traiga al tema, simplemente, porque ese es el principal obstáculo que se puede presentar al Desarrollar cualquier proyecto de Software.

4.8. Recomendaciones de contraseña

Cada entidad, tiene para sí, configuraciones de contraseñas que deben ser utilizadas obligatoriamente, caso contrario, si no las cumplen no permitirá que sean creadas y, esto causará una gran molestia en quienes van a utilizar las aplicaciones.

Es muy importante socializar a quienes deban utilizar los aplicativos de la institución, el correcto uso de las contraseñas, sin estarlas compartiendo, sin estarlas haciendo públicas, sin permitir, que otras personas realicen actividades con sus usuarios y contraseñas, debe entender y tener muy claro, las responsabilidades que podría acarrear el no hacer uso correcto de las contraseñas, para

esto se deberá mantener publicadas, políticas y reglamentos, que normen y sancionen en caso que se deba hacerlo para poder aplicar los correctivos necesarios.

4.9. Recomendaciones a la Institución.

Las Políticas de Seguridad para el Desarrollo de Software Seguro, son políticas que se han desarrollado para que, se puedan aplicar y pensando siempre en el futuro de los proyectos de Software que se vayan a generar más adelante, que se puedan aplicar a las actualizaciones que sigan realizando a los que ya están en producción y, que permitan sobre todo, facilitar el trabajo de mantenimiento que se pueda presentar en caso de que llegare a fallar alguna funcionalidad que tenga la aplicación.

Cabe recordar que, haciendo referencia a la frase escuchada frecuentemente, dentro del plan de estudios, "NO EXISTE SOFTWARE CIEN POR CIENTO SEGURO", pero si existen varias cosas que se pueden aplicar para mitigar la vulnerabilidad, entre ellas están las Políticas motivo del presente trabajo de investigación.

CONCLUSIONES

Al evaluar las políticas existentes para el desarrollo de software, se ha podido concluir que, las políticas existentes que se han publicado, y se puedan aplicar para poder realizar esta tarea, se encuentran elaboradas de una manera general para la Seguridad de la Información Empresarial, pero, dichas políticas no particularizan para el Desarrollo de Software, lo cual se debería tener para poder desarrollar Software seguro.

Las coincidencias entre las Normas ISO 27001, 27005, y OWASP, buscan mantener seguras a las empresas, dado que, siguen un estándar de calidad, así mismo, cada una utiliza parámetros para mantener seguros los activos de la empresa, finalmente la discrepancia que más resalta es, que únicamente la ISO 27001, es una Norma de Certificación, las demás Normas se utilizan para la ejecución de ella, y OWASP no es un estándar, es una metodología que, permite mantener el control de las vulnerabilidades existentes en la institución.

Se ha podido establecer que, la mejor herramienta para evaluar y administrar los riesgos ha sido la metodología OWASP, por su poca dificultad y además, por los aplicativos existentes para poder establecer y mejorar las seguridades dentro de la empresa a través del Desarrollo de Software.

Como resultado de la investigación, es posible concluir que, aplicar las políticas y utilizarlas durante la etapa de desarrollo de software, logra reducir del 39,2 % al 12,5 % en las pruebas realizadas, de manera que, se pueda seguir mejorando las vulnerabilidades existentes en las aplicaciones desarrolladas.

Al aplicar las políticas hacia un prototipo de prueba, antes de ser puesto en producción, se logra observar que, sin las políticas de seguridad, la aplicación es 39,2 % menos segura que cuando se logra aplicar las políticas que, la aplicación tiene el 12,5 % de riesgos, valores que se encuentran en la tabla 14-4 de la presente investigación.

RECOMENDACIONES

Al no existir de manera particular, un conjunto de políticas que se puedan aplicar para desarrollar aplicaciones de software, se recomienda el uso de las políticas generadas, para que, de esta manera tener al alcance de quienes realizan esta función dentro de la institución, una herramienta que guíe el Desarrollo de Aplicaciones y poder obtener un producto seguro.

Se recomienda el uso de las Normas creadas para mantener la seguridad de los activos informáticos de cualquier empresa, para desarrollar sus propias aplicaciones de software, se deben tomar en consideración las coincidencias y, dentro de las discrepancias, las que puedan coadyuvar para presentar una aplicación segura, no se las debe descartar, puesto que, no se puede limitar el uso de Normas cuando se trata de la seguridad.

Es recomendable que, para evaluar y administrar riesgos de seguridad, se tome en consideración la facilidad que brinde la herramienta a sus usuarios y, la información existente y si existen aplicativos que permitan mayor facilidad y mayor rapidez para determinar las vulnerabilidades que se pudieran encontrar, obteniéndose de esta manera, resultados que aporten para corregir y mitigar vulnerabilidades.

Se recomienda al Consejo de la Judicatura que, siendo una institución del estado que administra justicia, y, por ende, mantiene almacenada información sensible, aplicar, a través de la Subgerencia de Desarrollo, las Políticas Generadas para gestionar y mejorar la seguridad de sus activos informáticos sensibles, logrando mejorar y mitigar las vulnerabilidades existentes en sus aplicativos.

Siempre será recomendable, desarrollar prototipos para realizar las diferentes pruebas de ataques que puedan determinar las vulnerabilidades existentes, para poder corregir antes y no sufrir ataques fácilmente al ser puestas en producción.

BIBLIOGRAFÍA

BSI - BS ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:2005 Information Technology. Security Techniques. Code Of Practice For Information Security Management. (2015, July 16).

CASTRO, A. R., & BAYONA, Z. O. (2011). Gestión De Riesgos Tecnológicos Basada En Iso 31000 E Iso 27005 Y Su Aporte A La Continuidad De Negocios. *Ingeniería*, *16*(2), 56–66.

CHOO, K.-K. R. (2014). A Cloud Security Risk-Management Strategy. *Ieee Cloud Computing*, *1*(2), 52–56.

CLUSIF. (2010). MEHARI-2010-Introduccion - Mehari-2010-Introduccion.

COMITÉ TÉCNICO CONJUNTO ISO/IEC Jtc 1 Tecnología De La Información, & Subcomité Sc 27 Técnicas De Seguridad Ti. (N.D.). Norma Iso/Iec 27001:2005.

ETEROVIC J. E., **& PAGLIARI, G. A**. (N.D.). Metodología De Análisis De Riesgos Informáticos.

FERNÁNDEZ C. M. Coordinador De Tic, & De Aenor. (N.D.). La Norma Iso 27001 Del Sistema De Gestión De La Seguridad De Información.2012.

HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2010a). *Metodología De La Investigación* (5a Ed). México, D.F: Mcgraw-Hill.

HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2010b). *Metodología De La Investigación* (5a Ed). México, D.F: Mcgraw-Hill.

ISO27000.- El Portal De Iso 27001 En Español. Gestión De Seguridad De La Información. (N.D.).

MACHACA A. (N.D.). Analisis_De_Riesgo_Usando_La_Metodologia_Owasp.

MÉNDEZ P. (2015). *Nuevo Algoritmo Criptográfico Con La Incorporación De La Esteganografía En Imágenes*.

MERA D., VILLAMARÍN C., ARTEAGA L., & SOSA R. (N.D.). *Metodologia_De_La_Seguridad_Ing.*

MORENO F. (N.D.). Norma Iso-27005-Espanol.

MOSQUERA, D. F. P., NARVAÉZ, J. A. J., DONADO, S. A., FLOR, E. U. M., ALBARRACÍN, C. A. A., GARCÉS, S. D., & OTHERS. (2015). Control Inteligente Para El Servicio Crítico De Un Sistema De Información En Línea Enmarcado En Un Dominio De La Iso/Iec 27002.

PAINTSIL E. (2013). Evaluation Of Privacy And Security Risks Analysis Construct For Identity Management Systems. *Systems Journal, Ieee*, *7*(2), 189–198.

Seguridad Informatica - MAGERIT. (N.D.).

SYALIM, A., HORI, Y., & SAKURAI, K. (2009). Comparison Of Risk Analysis Methods: Mehari, Magerit, Nist800-30 And Microsoft's Security Management Guide (Pp. 726–731). Presented At The Availability, Reliability And Security, 2009. Ares '09. International Conference On, Ieee.

THE OWASP FOUNDATION. (2013). Owasp Top 10 - 2013 - Español.

UNIVERSIDAD DE COLOMBIA. (2003). Guia_Para_Elaborar_Politicas_V1_0.

YAQUB, S. C. (2007). Relating CORAS Diagrams And Markov Chains.

YIFENG, W., HUA, Z., ZHIHAO, L., LONGSHENG, H., JUFANG, L., & PING, X. (2012). Distribution Asset Risk Dynamic Warning And Coordination Management. In *2012 China International Conference On Electricity Distribution (Ciced)* (Pp. 1–6).

ANEXOS