INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACÁN

TESINA

Seminario de Titulación
"Auditoría de las Tecnologías de la Información y Comunicaciones"
DES/ESIME-CUL-2009/38/02/12

Análisis de Vulnerabilidades del Sistema Web SISER de Grupo Iusacell, Basado en la Metodología de Ec-Council.

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

Presentan:

BLANCAS MIRANDA YADIRA
CASTILLO TORRES ADRIAN
EUGENIO REYES ERNESTO
REYES MARTÍNEZ ARTURO ULISES
RUIZ BERNAL ERICK OCTAVIO

Asesores:

M. EN C. RAYMUNDO SANTANA ALQUICIRA
ING. MIGUEL ANGEL MIRANDA HERNÁNDEZ

México D., F. Junio 2012

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE: INGENIERO EN COMPUTACION

NOMBRE DEL SEMINARIO: AUDITORIA DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

VIGENCIA: DES/ESIME-CUL-2009/38/02/12

DEBERA DESARROLLAR: BLANCAS MIRANDA YADIRA
CASTILLO TORRES ADRIAN
EUGENIO REYES ERNESTO
REYES MARTÍNEZ ARTURO ULISES
RUIZ BERNAL ERICK OCTAVIO

NOMBRE DEL TEMA

"ANALISIS DE VULNERABILIDADES DEL SISTEMA WEB SISER DE GRUPO IUSACELL, BASADO EN LA METODOLOGIA DE EC-COUNCIL"

INTRODUCCION

Actualmente, el área de Aseguramiento de Ingresos y Prevención de Fraudes (AIyPF) de Grupo Iusacell cuenta con una aplicación web de uso interno denominada Sistema Integral de Servicios de AIyPF (SISER de AIyPF)
El sistema al no contar con un examen de seguridad previo a su liberación en producción, carece de una fuente confiable que evalué el nivel de seguridad del portal, por lo que puede ser susceptible a brechas de seguridad, que ponga en peligro la integridad, confidencialidad y disponibilidad de la información contenida.
Por lo anterior el objetivo de este trabajo es evidenciar las áreas de mejora en cuanto a la seguridad del Aplicativo Web para su posterior actualización, se realizará un análisis de vulnerabilidades sobre el servidor que soporta la aplicación web y específicamente para el puerto donde está montado el sistema, excluyendo el servidor de Bases de Datos.

CAPITULADO

I. INTRODUCCIÓN A LA AUDITORÍA DE LAS TECNOLOGÍAS Y LAS COMUNICACIONES.
II. APLICACIONES WEB.
III. METODOLOGÍA Y MÉTRICAS SOBRE SERVICIOS WEB.
IV. APLICACIÓN DE AUDITORÍA AL SERVICIO WEB SISER AIyPF.

Fecha: México D.F. a 11 de junio de 2012.

FIRMA DE ASESORES

M. EN C. RAYMUNDO SANTANA ALQUICIRA
Coordinador del Seminario

ING. MIGUEL ANGEL MIRANDA HERNÁNDEZ
Instructor del Seminario

DR. JOSÉ VELÁZQUEZ LÓPEZ
Jefe de la carrera de I.C.

AGRADECIMIENTOS

Agradezco a mis padres Felicitas y Francisco, que siempre me han apoyado desde que era una pequeña que daba sus primeros pasos, hasta el día de hoy, que termino mi carrera como profesionista y cierro este ciclo en mi vida; A mi esposo José A., que siempre me ha motivado a seguir mis sueños y conseguir mis metas y A mi hermano Saúl, que invariablemente ha sido mi ejemplo para prevalecer integra en mis ideales y lograr el éxito en todos los aspectos de mi vida.
Gracias y los quiero mucho.

Yadira Blancas Miranda.

Quiero agradecer a Dios ante todo, por darme la oportunidad de vivir y llegar hasta este momento, a mi FAMILIA por apoyarme SIEMPRE, a mis padres por no dejar que claudique en mis ideales; mamá: siempre a mi lado y al pendiente, papá: consejos que me son útiles, hermana: un motivo por el cual querer ser un ejemplo a seguir. También me gustaría agradecer a todos los profesores que tienen la vocación de ayudar sin recibir nada a cambio. Dedico esta tesina a todos ellos y demás personas que comparten instantes de vida conmigo

Ruiz Bernal Erick Octavio

Al concluir este ciclo profesional, agradezco a Dios por estar conmigo a cada instante de mi vida, a mis padres, hermanos y sobrinas por su amor, valores, ternura y sencillez, por ser mi fuente de inspiración y la razón más importante de tratar de ser una mejor persona, por haberme enseñado a no rendirme ni perder la esperanza aun en los momentos más difíciles, por las alegrías y tristezas, por todos los recuerdos hermosos.
Gracias a todos ellos, los amo.

Eugenio Reyes Ernesto

Agradezco el apoyo incondicional que me han brindado mis padres, por enseñarme el valor de las cosas y encaminarme siempre por el buen camino, a mis maestros por enseñarme a aprender y comprender los libros, a mis jefes por brindarme su apoyo para realizar esta tesis y a las personas que siempre han estado cerca de mí para enseñarme siempre algo nuevo y dejarme aprender de ellos. A todos ellos les agradezco por formar parte de mi vida.

Arturo Ulises Reyes Martínez

RESUMEN

Actualmente, el área de Aseguramiento de Ingresos y Prevención de Fraudes (AIyPF) de Grupo Iusacell cuenta con una aplicación web de uso interno denominada Sistema Integral de Servicios de AIyPF (SISER de AIyPF), donde se realiza la validación, facturación y se calculan las objeciones de grupos terceros como Telcel, Telmex y Telefónica el cual es de suma importancia para el área de contabilidad y finanzas porque facilita la manipulación de la información de manera más cómoda, rápida y sencilla y que además permite que los directivos aprueben o no las facturas allí suministradas para su posterior pago.

Debido a esto, se requiere que este portal sea seguro, confiable y que garantice la seguridad de la información ya que la pérdida de ésta puede generar riesgos económicos y de fraudes para la empresa.

ABSTRACT

Actually, the area of Revenue Assurance and Fraud Prevention (AIyPF) of Group Iusacell has an internal Web application called the Integrated Services System of AIyPF (SISER of AIyPF), which performs validation, billing and calculating the third group objections as Telcel, Telmex and Telephonic which is of utmost importance to the areas of accounting and finance because it facilitates the handling of information more convenient, fast and easy and also allows managers approve or not invoices provided there for later payment.

Because of this requires that this web site is safe, reliable, and guarantee the security of information as the loss of it can generate economic risks and fraud for the company.

TABLA DE CONTENIDO

INTRODUCCIÓN.

En la actualidad las aplicaciones web son indispensables para la comunicación interna y externa de las organizaciones para facilitar la administración, control y seguridad de la información, debido a que el gran volumen de información es humanamente imposible de manipular y además tiende a crecer con el tiempo por la demanda de los servicios que se demandan constantemente.

Las aplicaciones web son populares debido a lo práctico del navegador web como cliente ligero, a la independencia del sistema operativo, así como a la facilidad para actualizar y mantener aplicaciones web sin distribuir e instalar ***software*** a miles de usuarios potenciales. Existen aplicaciones como los ***webmails, wikis, weblogs***, ***webstores*** y la propia ***Wikipedia*** que son ejemplos bien conocidos de aplicaciones web.

Es importante mencionar que una página Web puede contener elementos que permiten una comunicación activa entre el usuario y la información. Esto permite que el usuario acceda a los datos de modo interactivo, gracias a que la página responderá a cada una de sus acciones, como por ejemplo rellenar y enviar formularios, participar en juegos diversos y acceder a gestores de base de datos de todo tipo.

Es por eso que la seguridad no es un punto importante, sino una obligación con la que debe contar los sistemas web para garantizar la protección de los datos de las empresas en consecuencia de que es de carácter confidencial y de gran importancia para el éxito de la organización ya que depende de esta para incrementar sus ingresos y dar mejores servicios.

Existen diferentes métodos de intrusión y de captura de paquetes en la red por lo que se debe contar con diferentes métodos y candados para evitar el riesgo de que la información quede a disposición de cualquier persona no autorizada por medio de estos accesos indebidos.

I. PROBLEMÁTICA.

El sistema al no contar con un examen de seguridad previo a su liberación en producción, carece de una fuente confiable que evalué el nivel de seguridad del portal, por lo que puede ser susceptible a brechas de seguridad, que ponga en peligro la integridad, confidencialidad y disponibilidad de la información contenida.

II. OBJETIVO.

Evidenciar las áreas de mejora en cuanto a la seguridad del Aplicativo Web SISER de grupo **Iusacell** para su posterior actualización.

III. JUSTIFICACIÓN

La aplicación web SISER maneja información sensible para **Iusacell**, referente a su contabilidad y protección contra fraudes por lo que es de gran importancia validar la seguridad de dicha aplicación para garantizar la integridad de la información. Por lo que al carecer de un análisis de seguridad que determine el nivel de seguridad de dicha aplicación, se requiere realizar un análisis de vulnerabilidades de la misma.

IV. ALCANCE.

Se realizará un análisis de vulnerabilidades sobre el servidor que soporta la aplicación web SISER y específicamente para el puerto donde está montado el sistema: **DOMINIO: http://172.19.235.122:8084/SISER**

DESCRIPCION: Sistema Integral de Servicio de Aseguramiento de Ingresos y Prevención de Fraudes **SISER AIyPF**, administra la facturación de Grupo Iusacell.

CAPÍTULO I

Introducción a la Auditoría de las Tecnologías y las Comunicaciones

1.1 Concepto de Tecnologías de la Información y las Comunicaciones.

Las denominadas ***Tecnologías de la Información y las Comunicaciones (TIC)*** ocupan un lugar central en la sociedad y en la economía del fin de siglo, con una importancia creciente. El concepto de TIC surge como convergencia tecnológica de la electrónica, el software y las infraestructuras de telecomunicaciones. La asociación de estas tres tecnologías da lugar a una concepción del proceso de la información, en el que las comunicaciones abren nuevos horizontes y paradigmas.

Se realiza una descripción de los objetivos de cada una de estas tecnologías, sentando las bases para los temas futuros de esta tesina. Se explican sus conceptos fundamentales y se repasa el estado del arte de la electrónica, el ***software*** y las infraestructuras de telecomunicaciones.

1.1.1 Concepto e Importancia de las TIC.

Las TIC son el conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Las TIC incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.

Las TIC tienen sus orígenes en las llamadas ***Tecnologías de la Información (Information Technologies o IT)***, concepto aparecido en los años 70, el cual se refiere a las tecnologías para el procesamiento de la información: la electrónica y el *software*. Este procesamiento se realizaba casi exclusivamente en entornos locales, por lo que la comunicación era una función poco valorada. Por otra parte, la estrategia centralista de las corporaciones, hacía compatible la existencia de un departamento de sistemas de información centralizado en una única máquina.

Las nuevas formas de trabajo y la globalización de la economía imponen la necesidad del acceso instantáneo a la información y por tanto, de interconectar las distintas redes que se han ido creando, diseñándose nuevas arquitecturas de sistemas, en las que la función de comunicación es de igual importancia o superior por lo estratégico de la disponibilidad instantánea de la información. A esto se añade, la existencia de unas infraestructuras de comunicación muy extendidas y fiables y un abaratamiento de los costes de comunicación lo que estimuló la aparición de nuevos servicios adecuados a las estrategias de las corporaciones.

La comunicación instantánea es vital para la competitividad de una empresa, en un mundo en que la información se convierte en un input más del sistema de producción.

El uso y el acceso a la información es el objetivo principal de las TIC. El manejo de la información es cada vez más dependiente de la tecnología, ya que los crecientes volúmenes de la misma que se manejan y su carácter claramente multimedia obligan a un tratamiento con medios cada vez más sofisticados. El acceso a redes como Internet mediante ordenadores personales o la complejidad de los sistemas bancarios y de reservas aéreas totalmente informatizadas son pruebas evidentes de que sin la tecnología el uso de la información sería imposible en la actualidad.

En conclusión, la causa de la aparición de las TIC, fusión del tratamiento y de la comunicación de la información, es que se produce un proceso de convergencia tecnológica de distintas áreas de conocimiento y aplicación, la electrónica, la informática y las telecomunicaciones que, si bien hasta comienzos de la década de los setenta se desarrollaban independientemente, hoy día están estrechamente relacionadas entre sí. Sin embargo, desde el punto de vista técnico se trata de un amplio espectro de disciplinas interrelacionadas.

1.1.2 Componentes Base de las TIC.

La ***microelectrónica***, frecuentemente denominada ***hardware***, está residente en todas las funcionalidades del proceso de información. Resuelve los problemas relacionados con la interacción con el entorno como la adquisición y la presentación de la información, mediante dispositivos como transductores, tarjetas de sonido, tarjetas gráficas, etc. No obstante, su mayor potencialidad está en la función de tratamiento de la información. La unidad fundamental de tratamiento de la información es el microprocesador, que es el órgano que interpreta las órdenes del *software*, las procesa y genera una respuesta.

El ***software*** traslada las órdenes que un usuario da a una computadora al lenguaje de ejecución de órdenes que entiende la máquina. Está presente en todas las funcionalidades del proceso de la información, pero especialmente en el tratamiento de la información.

El ***hardware*** sólo entiende un lenguaje que es el de las señales eléctricas en forma de tensiones eléctricas, por lo que es necesario abstraer de esta complejidad al hombre y poner a su disposición elementos más cercanos a sus modos de expresión y razonamiento.

Las inf***raestructuras de comunicaciones*** constituyen otro elemento base del proceso de información, desde el momento en que alguna de las funcionalidades resida en un lugar físicamente separado de las otras. Para acceder a esta función hay que utilizar redes de comunicación por las que viaja la información, debiéndose asegurar una seguridad, calidad, inexistencia de errores, rapidez, etc.

En la *figura 1.1* vemos cómo se combinan estos tres elementos soporte de las TIC para proporcionar al usuario servicios a través de las aplicaciones. La capa de aplicaciones es una integración adecuada de tecnologías dispuestas de forma que el acceso y uso de los servicios sea intuitivo y sencillo para el usuario, de manera que le abstraiga de la complejidad tecnológica residente en el servicio.

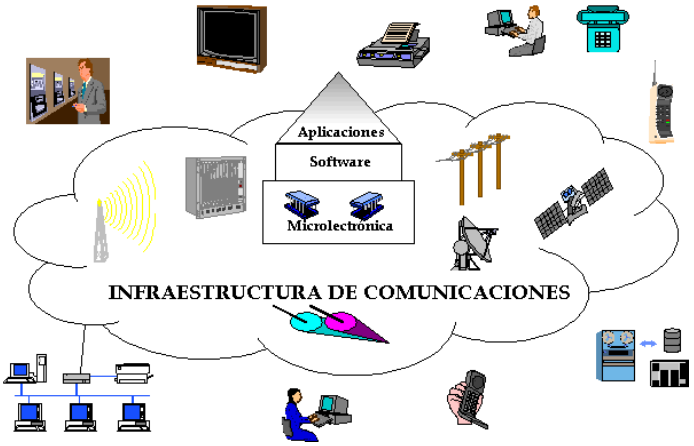


Figura 1.1. Los componentes base de las TIC

La Microelectrónica

La tecnología microelectrónica estudia cómo dotar a un circuito o asociación de circuitos agrupados (encapsulados) en una única unidad física, de una mayor velocidad de proceso ocupando el mínimo volumen y un coste aceptable, con ciertos compromisos de consumo energético.

Los avances en microelectrónica han permitido la integración a gran escala de circuitos en un solo chip, proporcionando componentes *hardware* cada vez más potentes y de menor coste. El chip es la unidad mínima físicamente inseparable de procesamiento de información, estando internamente constituido por millones de componentes elementales como transistores, resistencias, condensadores, etc., cuya asociación y configuración mediante conexiones en un modo apropiado

proporciona la funcionalidad específica del circuito. Por tanto, los criterios que orientan la microelectrónica son:

La combinación de estos componentes y el concurso de otras tecnologías, en particular las magnéticas, para almacenamiento y recuperación de información, y las ópticas, con amplias aplicaciones, permite construir el *hardware* de los equipos y sistemas electrónicos que se dirigen a distintos segmentos de mercado, de los que destacan cuatro:

Hardware **Informático**

El ***hardware*** diseñado para la informática es un amplio conjunto de componentes, subsistemas y sistemas que se integran en los equipos informáticos.

El *Software*

El ***software*** o soporte lógico es el conjunto de instrucciones escritas en lenguajes de programación y traducidas posteriormente a dígitos binarios para que sean entendidas por el hardware. Está presente en todas las funcionalidades del proceso de la información, pero especialmente en el tratamiento de la información. El hardware sólo entiende un lenguaje que es el de las señales eléctricas en forma de tensiones eléctricas, por lo que es necesario abstraer de esta complejidad al hombre y poner a su disposición elementos más cercanos a sus formas de expresión y razonamiento.

La tecnología ***software*** está presente en todos los procesos de información, ya que dichas funciones son realizadas cada vez con mayor intensidad por ordenadores. Los distintos componentes bases del *software* son:

Sistemas Operativos: Para el control de las complejas arquitecturas que pueden construirse con los componentes microelectrónicos y facilitar interfaces amigables con el usuario.

Middleware: Es la parte de la arquitectura encargada de abstraer a las aplicaciones de los detalles de las plataformas de explotación, mediante las ***Application Programs Interfaces*** (**APIs**).

Cliente/Servidor: La arquitectura cliente/servidor reparte la carga de trabajo entre la estación de usuario y la estación central.

Bases de Datos: Para el manejo, manipulación y administración de información.

Programas de Aplicación: *Software* para la realización de tareas variadas como puedan ser hojas de cálculo, proceso de textos, aplicaciones de gestión comercial, científicas, de diseño, etc.

Lenguajes de Programación y Herramientas para la Ingeniería *Software*: Conjunto de lenguajes y herramientas de ayuda al desarrollo de la realización de aplicaciones específicas.

Las Infraestructuras de Telecomunicaciones

Las ***infraestructuras de telecomunicaciones*** transportan la información desde un punto a otro, mediante un conjunto de equipos y medios de acceso, transmisión y conmutación. Proporcionan la capacidad necesaria para mantener una comunicación, ya sea ésta en forma de voz, datos o imágenes. Esta definición incluye todas las necesidades que impone una comunicación, como son tener acceso a la red de comunicación, transportar la información y poner en comunicación al emisor y al receptor. Todo ello dentro de un marco de operación de distintos servicios que se basan en iguales o distintas redes y requiere su interconexión.

Los conceptos fundamentales en telecomunicaciones *figura 1.2* son:

- El acceso a las redes mediante la red de acceso.
- La señalización entre el terminal y la red para conocer su estado, tarificar y encaminar la llamada.
- Seleccionar entre los múltiples caminos aquél que comunica al emisor con el receptor mediante la conmutación.
- Transportar eficientemente la información mediante la transmisión.

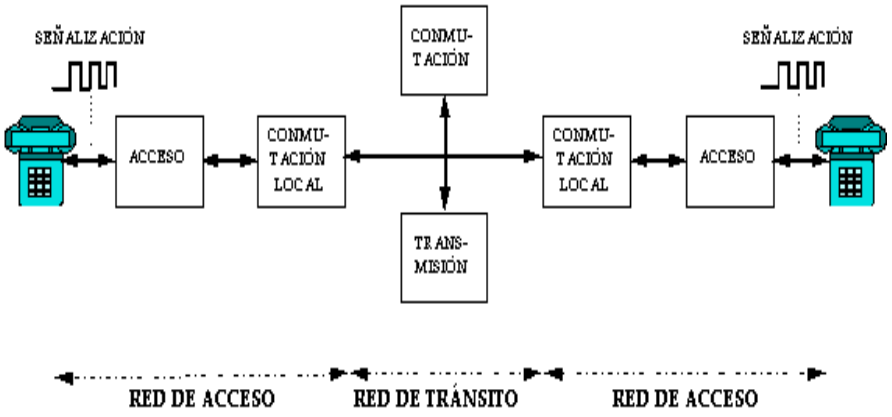


Figura 1.2. Conceptos de Telecomunicaciones.

El Sector Multimedia

El desarrollo tecnológico y las posibilidades de los nuevos productos a que da lugar, apuntan actualmente hacia una convergencia entre los sectores de las telecomunicaciones, la informática y el audiovisual. Esta convergencia permite definir un nuevo sector que agrupa todas estas líneas de actividad orientadas en su conjunto al manejo de información en cualquiera de sus formas.

Este nuevo sector, el sector multimedia, se caracteriza por la posibilidad de acceder y usar información digitalizada de todo tipo (voz, datos e imágenes) en cualquier momento y en cualquier lugar. Como se desprende de esta definición, no formal, el multimedia representa una nueva generación de servicios, e implica tecnologías hasta ahora diferentes.

Cada uno de los sectores que convergen en el sector multimedia ha evolucionado rápidamente en los últimos años, teniendo esta evolución en común para los tres sectores, el hecho de estar basadas en la digitalización de sus tecnologías. No obstante, es preciso que alcancen su fase de maduración mediante la mejora de sus prestaciones y la reducción de costes, de forma que sea económicamente viable para su implantación generalizada.

La convergencia de sectores y sus tecnologías en un nuevo mercado de aplicaciones y servicios ha dado origen al nuevo sector multimedia. Las distintas empresas de cada uno de los sectores, que inicialmente actuaban en sus respectivos sectores, están buscando alianzas con empresas de los otros sectores para adquirir sus tecnologías y experiencia e integrarlas para la creación de nuevos negocios.

Por tanto, los tres factores motores del desarrollo de los servicios multimedia son ver *figura 1.3:*

- La digitalización
- La convergencia de tecnologías y mercados
- El desarrollo de la plataforma de usuario

Los agentes del sector multimedia están formados por empresas de los tres sectores y por otras pertenecientes al sector multimedia, surgidas como nuevas empresas o como alianzas o fusiones. La estructura del mercado es la siguiente:

- Informática: proveedores de ***software*** y hardware informático.
- Telecomunicaciones: proveedores de redes y servicios de comunicaciones.
- Audiovisual: difusores de televisión, radiodifusores y proveedores de contenidos.
- Multimedia: plataforma de usuario y proveedores de servicios avanzados multimedia, como televisión interactiva, vídeo bajo demanda, teleeducación, etc. Los cuales requieren la integración de las distintas tecnologías.

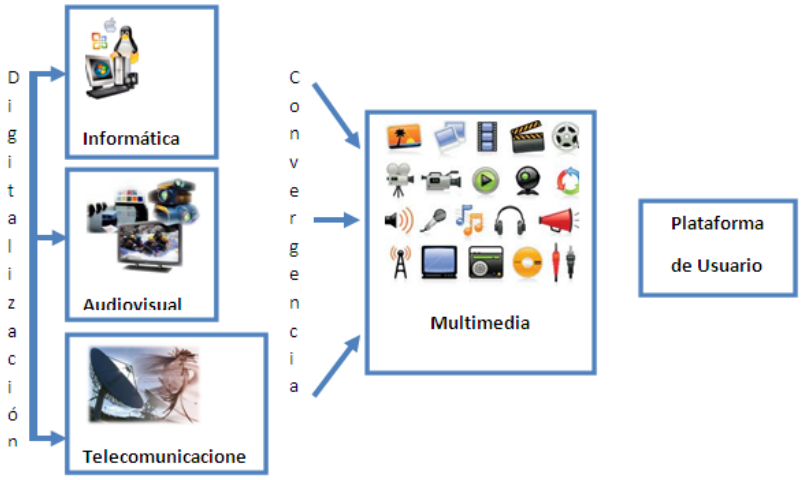


Figura 1.3. La Convergencia Sectorial en el Multimedia

1.2 Auditoría de las TIC.

Desde el procesamiento electrónico de datos que comenzó en la década de 1950 para llevar las cuentas y el registro de actividades en las organizaciones. Se inició con el interés por auditar los sistemas de información, los procesos de negocios apoyados por estos, los datos financiero-contables, la infraestructura tecnológica y la seguridad informática.

Se someten a examen las actividades apoyadas por las TIC para revisar los controles, el cumplimiento con políticas y regulaciones, así como el grado en el cual estas apoyan la eficiencia, eficacia y rentabilidad económica.

Estas auditorías ayudan a las organizaciones a evaluar la manera en que hacen sus negocios o proveen sus servicios apoyados por TIC, buscando proteger los intereses de socios, empleados y clientes. Esto permite validar la seguridad, confiabilidad, integridad y privacidad de los sistemas de información.

Los auditores informáticos pueden recomendar cambios en los procesos de negocios para lograr los objetivos económicos o sociales de la organización. También es posible que las investigaciones revelen fraudes, desperdicios o abusos. Los auditores informáticos modernos proceden de manera sistemática en sus estudios, planificando sus acciones y enfocándose en las áreas de mayor riesgo.

1.2.1 Concepto de Auditoría.

El es proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso.

Por otra parte la Auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización.

1.2.2 Tipos de Auditoría.

Cuando se generalizó el uso de las nuevas tecnologías, surgió también la necesidad de realizar auditorías sobre los sistemas de tratamiento de información. En este sentido se podría decir que la auditoria informática es un proceso, de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización, y utiliza eficientemente los recursos, alineándose con determinados estándares relacionados con el buen uso (***best practices***) de los sistemas. Este proceso metodológico en la actualidad está siendo utilizado para valorar y evaluar la confianza que se puede depositar en TI.

Los distintos tipos de auditorías que se pueden realizar se clasifican en:

- Financieras
- Verificativas
- Informáticas
- Operativas o de Gestión
- Técnicas.

Dentro de la auditoría informática destacan los siguientes tipos:

Auditoría de la gestión: Referido a la contratación de bienes y servicios, documentación de los programas, etc.

Auditoria legal del reglamento de protección de datos: Cumplimiento legal de las medidas de seguridad exigidas por el reglamento de desarrollo de la ley orgánica de protección de datos.

Auditoría de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

Auditoría de las bases de datos: Control de acceso, de actualización, de integridad y calidad de los datos.

Auditoría de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Auditoria de la seguridad Física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo

La auditoría puede ser ejercida por dos órganos uno referente a la auditoría Interna y otro a la auditoría Externa, misma que serán explicadas a continuación.

La Auditoría Interna.

Constituye una función de evaluación independiente. Sin embargo, existe en el seno de una entidad y bajo la autorización de la dirección con el ánimo de examinar y evaluar las actividades de la entidad. La función principal del auditor interno es ayudar a la dirección en la realización de sus funciones.

Auditor Interno

Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.

Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes. Revisar y juzgar el nivel de eficacia, utilidad; fiabilidad y seguridad de los equipos e información.

Características de la Auditoría Interna

Una unidad con atribuciones y facultades para auditar todas las operaciones de las organizaciones, situada en el organigrama en dependencia directa de la alta dirección. Con la finalidad de asegurar el control interno influyendo en la gestión de las mismas independiente para la formulación de sus opiniones y recomendaciones, trabajando con arreglo a la previa y autorizada planificación anual de sus informes y actividades, revisar los medios de salvaguarda de los activos y, si procede, verificar su existencia, valorar la economía y eficacia con que son utilizados los recursos, revisar las operaciones o programas para verificar si los resultados están de acuerdo con los objetivos y metas establecidas y si las operaciones o programas se llevan a cabo en la forma prevista. La independencia permite a los auditores internos emitir juicios imparciales y sin prejuicios, lo que es

esencial para la adecuada ejecución de las auditorias. Esto se consigue mediante un adecuado nivel en la organización y con objetividad.

La Auditoría Externa.

Constituye una función de evaluación independiente y externa a la entidad que se examina. En la mayoría de las empresas, se contrata anualmente la realización de una auditoría de los estados financieros por parte de un contador público independiente, bien voluntariamente o bien por obligación legal.

Objetivo de la auditoría externa

El objetivo principal de una auditoría externa es la expresión de una opinión respecto de la calidad de los estados financieros de la entidad, por lo que el auditor externo se ocupa principalmente de la fiabilidad de la información financiera.

1.2.3 Conceptos de Políticas de Seguridad Informática y Controles.

Políticas, planes y procedimientos

Las Políticas definen qué se debe proteger en el sistema, mientras que los Procedimientos de Seguridad describen cómo se debe conseguir dicha protección. Una Política es un conjunto de orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Política de Seguridad

Conjunto de directrices que permiten resguardar los activos de información. Características de una política de seguridad

- Definir la postura del Director y de la gerencia con respecto a la necesidad de proteger la información corporativa.
- Definir la base para la estructura de seguridad de la organización.
- Ser un documento de apoyo a la gestión de seguridad informática.
- Tener larga vigencia, manteniéndose sin grandes cambios en el tiempo.
- Ser general, sin comprometerse con tecnologías específicas.

- Debe abarcar toda la organización
- Debe ser clara y evitar confusiones
- No debe generar nuevos problemas
- Debe permitir clasificar la información en confidencial, uso interno o pública.
- Debe identificar claramente funciones específicas de los empleados como: responsables, custodio o usuario, que permitan proteger la información

Componentes de una política de seguridad de la información

- Políticas específicas
- Procedimientos
- Estándares o prácticas
- Estructura organizacional

Políticas Específicas

Definen en detalle aspectos específicos que regulan el uso de los recursos de información y están más afectas a cambios en el tiempo que la política general.

Procedimiento

Los procedimientos de auditoría, son el conjunto de técnicas de investigación aplicables a una partida o a un grupo de hechos y circunstancias relativas a los estados financieros sujetos a examen, mediante los cuales, el contador público obtiene las bases para fundamentar su opinión.

Debido a que generalmente el auditor no puede obtener el conocimiento que necesita para sustentar su opinión en una sola prueba, es necesario examinar cada partida o conjunto de hechos, mediante varias técnicas de aplicación simultánea o sucesiva.

Extensión o alcance de los procedimientos de auditoría

Dado que las operaciones de las empresas son repetitivas y forman cantidades numerosas de operaciones individuales, generalmente no es posible realizar un examen detallado de todas las transacciones individuales que forman una partida global. Por esa razón, cuando se llenan los requisitos de multiplicidad de partidas y similitud entre ellas, se recurre al procedimiento de examinar una muestra representativa de las transacciones individuales, para derivar del resultado del

examen de tal muestra una opinión general sobre la partida global. Este procedimiento, no es exclusivo de la auditoría, sino que tiene aplicación en muchas otras disciplinas. En el campo de la auditoría se le conoce con el nombre e pruebas selectivas.

Políticas de seguridad y Controles

Los controles son mecanismos que ayudan a cumplir con lo definido en las políticas, si no se tienen políticas claras, no se sabrá qué controlar, orientación de los controles:

- PREVENIR la ocurrencia de una amenaza
- DETECTAR la ocurrencia de una amenaza
- RECUPERAR las condiciones ideales de funcionamiento una vez que se ha producido un evento indeseado.

1.2.4 Seguridad de la Información.

Es necesario hablar de la Seguridad de la Información porque el negocio se sustenta a partir de la información que maneja, no sólo es un tema Tecnológico y porque la institución no cuenta con Políticas de Seguridad de la Información formalmente aceptadas y conocidas por todos, así mismo es necesario reconocer los activos de información importantes para la institución.

- Información propiamente tal: bases de datos, archivos, conocimiento de las personas
- Documentos: contratos, manuales, facturas, pagarés, solicitudes de créditos.
- ***Software***: aplicaciones, sistemas operativos, utilitarios.
- Físicos: equipos, edificios, redes
- Recursos humanos: empleados internos y externos
- Servicios: electricidad, soporte, mantención.

Es de suma importancia reconocer las Amenazas a que están expuestos.

Amenaza: Evento con el potencial de afectar negativamente la Confidencialidad, Integridad o Disponibilidad de los Activos de Información.

Vulnerabilidad: Una debilidad que facilita la materialización de una amenaza

Riesgo: La posibilidad de que una amenaza en particular explote una vulnerabilidad y afecte un activo.

Acceso Físico Ilegal: Una persona logra un acceso físico no autorizado a instalaciones del computador. Como resultado, pueden causar daño físico al hardware o hacer copias no autorizadas de programas y datos.

Abuso de Privilegios: Una persona usa privilegios, que le han sido asignados, para propósitos no autorizados. Como consecuencias de Abusos, tenemos

1) Destrucción de activos
2) Sustracción de activos
3) Modificación de activos
4) Violación de privacidad
5) Interrupción de operaciones
6) Uso no autorizado de activos
7) Daño físico a personas y/o activos

1.3 Modelos de Auditoría.

1.3.1 COSO.

Desde la década de los 80 se comenzaron a ejecutar una serie de acciones en diversos países desarrollados con el fin de dar respuesta a un conjunto de inquietudes sobre la diversidad de conceptos, definiciones e interpretaciones que sobre el Control Interno existían en el ámbito internacional, ajustados obviamente al entorno empresarial característico de los países capitalistas.

El Informe ***COSO*** (siglas que representan los organismos miembros), siendo el título formal del mismo "Control Interno - Sistema Integrado", surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, funciones e interpretaciones existentes en torno a la temática referida. La definición de control que propone, como la estructura de control que describe, impulsa una nueva cultura administrativa en todo tipo de organizaciones, y ha servido de plataforma para diversas definiciones y modelos de control a escala internacional. En esencia, todos los informes hasta ahora conocidos, persiguen los mismos

propósitos y las diferentes definiciones, aunque no son idénticas, muestran mucha similitud.

Se trataba entonces de materializar un objetivo fundamental: definir un nuevo marco conceptual de Control Interno, capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre este tema, logrando así que, al nivel de las organizaciones públicas o privadas, de la auditoría interna o externa, y de los niveles académicos o legislativos, se cuente con un marco conceptual común, una visión integradora que satisfaga las demandas generalizadas de todos los sectores involucrados.

En este informe se plasman los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la ***Treadway*** comisión y la ***National Commission on Fraudulent Financial Reporting***. El grupo estaba constituido por representantes de organizaciones de Estados Unidos:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executive Institute (FEI)
- Institute of Internal Auditors (IIA)
- Institute of Management Accountants (IMA)

En junio de 1994 la Oficina General de Contabilidad del Congreso de los Estados Unidos expresó su apoyo al Informe COSO. Fue a partir de entonces cuando se convirtió en norma de hecho para los controles internos.

Es oportuno exponer dentro de los nuevos conceptos del Control Interno, la definición que sobre el mismo se elaboró en el Informe COSO:

El Control Interno es un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.
- Integridad de la información.

El Control Interno se define como un proceso, y por lo tanto el mismo podrá ser evaluado en cualquier punto de su desarrollo. Al ser considerado como un proceso, el mismo es un medio para alcanzar un fin, y no un fin en sí mismo.

El Control Interno debe estar integrado a los procesos operativos de la entidad, y no ser un "agregado" a los mismos. Todos los integrantes de la organización son responsables por el Control Interno, ya que lo llevan a cabo las personas que actúan en todos los niveles, no tratándose solamente de manuales de organización y procedimientos que indican lo que se debe hacer. La responsabilidad del Control Interno no es exclusiva de ningún evaluador externo al proceso operativo de la entidad, como tradicionalmente se ha supuesto.

El Control Interno sólo puede proporcionar un grado de seguridad razonable con relación al logro de los objetivos fijados. La seguridad total o absoluta no existe en este sentido, ya que pueden tomarse decisiones erróneas o producirse acuerdos entre varias personas que vulneren el Sistema de Control Interno por más fuerte que el mismo sea.

Para el debido entendimiento del Informe ***COSO***, es necesario tener claridad sobre los elementos que contiene la definición que anteriormente se reprodujo, lo más importante radica en el señalamiento de que el control es un proceso efectuado por el personal y diseñado para garantizar razonablemente el cumplimiento de los objetivos.

El señalamiento de propósito del control en cuanto a asegurar razonablemente el cumplimiento de objetivos de tipo operacional, financiero y normativo, se comprende mejor cuando se analizan los cinco componentes del Informe COSO y sus 17 factores, que en conjunto forman una estructura integrada de control, ya que existe una relación directa entre los objetivos que la organización persigue y los citados componentes, puesto que estos representan lo necesario para la consecución de tales objetivos.

A continuación se presentan los 5 componentes y los 17 factores del Informe ***COSO*** *(Tabla 1.4)*.

COMPONENTES Y FACTORES COSO	
Ambiente de Control:	Integridad y Valores Éticos. Métodos y Estilos de Dirección. Estructura Organizativa. Política de Recursos Humanos. Manuales, Procedimientos y Disposiciones Legales y Reglamentarias.
Evaluación de Riesgo:	Objetivos de la Entidad. Identificación y Evaluación de Riesgos. Seguimiento y Control de Riesgos.
Actividades de Control:	Coordinación entre las áreas y Documentación. Niveles definidos de autorización y Separación de Tareas. Rotación del personal en las tareas claves. Indicadores del Desempeño. Control de las Tecnologías de la Información. Acceso restringido a los recursos, Activos y Registros.
Información y Comunicación:	Información. Comunicación.
Supervisión y Monitoreo:	Supervisión y Monitoreo:

1.4. Tabla de Componentes y Factores COSO

Los componentes y factores se presentan en mayor o menor grado en cualquier área, proceso o división de toda organización y se reconoce que los componentes con mayor influencia e importancia son los dos primeros: el Ambiente de Control y la Evaluación de Riesgos.

1.3.2 COCO.

El Informe ***COCO*** es producto de una profunda revisión del Comité de Criterios de Control de Canadá sobre el reporte ***COSO*** y cuyo propósito fue hacer el planteamiento de un informe más sencillo y comprensible, ante las dificultades que en la aplicación del ***COSO*** enfrentaron inicialmente algunas organizaciones. El resultado es un informe conciso y dinámico encaminado a mejorar el control, el cual describe y define al control en forma casi idéntica a como lo hace el Informe ***COSO***.

El modelo ***COCO*** fue emitido en 1995 por el Consejo denominado "***The Criteria of Control Board"*** y dado a conocer por el Instituto Canadiense de Contadores Certificados (CICA) a través de un Consejo encargado de diseñar y emitir criterios o lineamientos generales sobre control interno.

La mayoría de las definiciones dadas por los diferentes autores estudiados coinciden en catalogar el control interno como un conjunto de medidas, métodos o procedimientos (en el Informe COSO y en la Resolución 297 se analiza como un

proceso) que permiten lograr una mejor protección de los recursos, mayor confiabilidad en la información, asegurar el cumplimiento de todas las leyes o reglamentos establecidos por la dirección y la eficiencia y eficacia de las operaciones. El llamado ciclo de entendimiento básico del control, como se representa en el informe, consta de cuatro etapas que contienen los 20 criterios generales, conformando un ciclo lógico de acciones a ejecutar para asegurar el cumplimiento de los objetivos de la organización.

A continuación mostramos los criterios del modelo **COCO** en 4 apartados *(Tabla 1.5)*.

CRITERIOS DE MODELO COCO	
Propósito:	Los objetivos deben ser comunicados. Se deben identificar los riesgos internos y externos que afecten el logro de objetivos. Las políticas para apoyar el logro de objetivos deben ser comunicadas y practicadas, para que el personal identifique el alcance de su libertad de actuación. Se deben establecer planes para guiar los esfuerzos. Los objetivos y planes deben incluir metas, parámetros e indicadores de medición del desempeño.
Compromiso:	Se deben establecer y comunicar los valores éticos de la organización. Las políticas y prácticas sobre recursos humanos deben ser consistentes con los valores éticos de la organización y con el logro de sus objetivos. La autoridad y responsabilidad deben ser claramente definidas y consistentes con los objetivos de la organización, para que las decisiones se tomen por el personal apropiado. Se debe fomentar una atmósfera de confianza para apoyar el flujo de la información.
Aptitud:	El personal debe tener los conocimientos, habilidades y herramientas necesarios para el logro de objetivos. El proceso de comunicación debe apoyar los valores de la organización. Se debe identificar y comunicar información suficiente y relevante para el logro de objetivos. Las decisiones y acciones de las diferentes partes de una organización deben ser coordinadas. Las actividades de control deben ser diseñadas como una parte integral de la organización.
Evaluación y Aprendizaje:	Se debe monitorear el ambiente interno y externo para identificar información que oriente hacia la reevaluación de objetivos. El desempeño debe ser evaluado contra metas e indicadores. Las premisas |consideradas para el logro de objetivos deben ser revisadas periódicamente. Los sistemas de información deben ser evaluados nuevamente en la medida en que cambien los objetivos y se precisen deficiencias en la información. Debe comprobarse el cumplimiento de los procedimientos modificados. Se debe evaluar periódicamente el sistema de control e informar de los resultados.

Tabla 1.5. Tabla de Criterios de modelo COCO.

Un Auditor acostumbrado a la tradicional evaluación del Control Interno, enfrenta un gran desafío al tener que realizar de acuerdo a dichos informes, un trabajo más complejo y de mayor alcance a través de la evaluación de los cinco componentes o los 20 criterios.

Esto debido a que diversos factores o criterios según el caso, corresponden a aspectos intangibles o informales desde el punto de vista de su documentación, percepción o funcionamiento, tales como integridad y valores éticos, filosofía de la organización, estilo de mando, medición de los riesgos, etc.; así como el tener que evaluar las tres categorías de objetivos (y no solamente el financiero) para opinar sobre la suficiencia y efectividad del Sistema de Control.

El Informe COSO ha sido adoptado en todo el territorio de los EE.UU., por el Banco Mundial y otros organismos financieros a través del mundo. Sin embargo, el Informe COCO de Canadá, publicado tres años más tarde que el COSO, simplifica los conceptos y el lenguaje, para hacer posible una discusión del alcance total del control, con la misma facilidad en cualquier nivel de la organización empleando un lenguaje accesible para todos los trabajadores.

Las semejanzas más importantes en cuanto a los dos informes, es que ambos abordan al Control Interno como un proceso, además de establecer como premisa que todo el personal dentro del ámbito de una organización tienen participación y responsabilidad en el proceso de control.

Diferencias fundamentales entre los informes:

Independientemente al énfasis e interés desarrollado en los últimos años en varios países, acerca de la gran diversidad de conceptos y puntos de vista relacionados con el Control Interno, sus normas, evaluación, informes, etc., continua siendo una temática tan amplia como los propios objetivos y perspectivas en que el mismo puede ser contemplado, y que se encuentran materializados en leyes, decretos leyes, proyectos de leyes, resoluciones, reglamentos, normas, directivas, informes y bibliografía especializada.

Por consiguiente, el alcance de dichos documentos es tan amplio como los posibles objetivos del Control Interno y las diversas perspectivas desde las que puede ser visto. Contienen diferentes definiciones, diferentes opiniones acerca de la función del Control Interno, cómo debe establecerse, cómo debe evaluarse, sin olvidar que en su mayoría se redactarán en defensa de los intereses de la clase dominante en la sociedad que se trate.

Entre las diversas definiciones que pueden ser encontradas, se considera actualizada la siguiente:

CONTROLAR es verificar que todo se desarrolle de acuerdo con las reglas establecidas, observando que las metas, planes y objetivos se cumplan, detectando en su momento las desviaciones para corregirlas.

En la Resolución Económica del V Congreso del Partido Comunista de Cuba el 9 de octubre de 1997 se señala:

En las nuevas condiciones en que opera la economía, con un mayor grado de descentralización y más vinculados a las exigencias de la competencia internacional, el control oportuno y eficaz de la actividad económica es esencial para la dirección a cualquier nivel, y más adelante se señala: Condición indispensable en todo este proceso de transformaciones del sistema empresarial será la implantación de fuertes restricciones financieras que hagan que el control del uso eficiente de los recursos sea interno al mecanismo de gestión y no dependa únicamente de comprobaciones externas.

Lo anterior demuestra que en Cuba, al igual que en el resto del mundo, y adecuado a nuestras características y condiciones ha sido necesario definir, -en la Política Económica que se precisa en dicho documento- líneas de acción e investigación vinculadas con la necesidad del control y del papel que deben desempeñar los cuadros de dirección y los trabajadores en todas las instancias, en la custodia de los bienes y recursos que el Estado ha puesto en sus manos, para todo lo cual resulta imprescindible disponer del Control Interno eficiente.

Como elemento primordial para volver a insertar en la economía internacional a las entidades estatales y que estas logren un nivel adecuado de competitividad, se hace imprescindible la aplicación y desarrollo de la contabilidad y del Control Interno como pilares de nuestra economía, siendo necesario que todos los dirigentes y trabajadores de nuestro país entiendan que la lucha por la aplicación del Control Interno es imprescindible para lograr la eficiencia y eficacia en la gestión de las entidades y que es una responsabilidad de todos dentro de la organización y no sólo del personal del área económico-contable.

La relevancia que está adquiriendo el Control Interno en los últimos tiempos, a causa de numerosos problemas producidos por su ineficiencia, ha hecho necesario que los miembros de los consejos de dirección asumieran de forma efectiva, responsabilidades que hasta ahora se habían dejado en manos de las áreas económico-contable de las entidades. Por eso es necesario que la

administración tenga claro en qué consiste el Control Interno para que pueda actuar al momento de su implementación.

Un Sistema de Control Interno es importante por cuanto no se limita únicamente a la confiabilidad en la manifestación de las cifras que son reflejadas en los Estados Financieros, sino también evalúa el nivel de eficiencia operacional en los procesos contables y administrativos.

Por todo ello, nuestro país requiere cada vez más, disponer de mayor información sobre lo que acontece a nivel internacional al respecto, con el objetivo de no sólo brindar información actualizada en el ejercicio de la docencia, sino de estar en condiciones de poder proponer criterios.

Otra de las reestructuraciones está en que, de acuerdo con la nueva concepción, el Ministerio de Finanzas y Precios gestiona todo lo relacionado con el Control Interno, apoyado en el Ministerio de Auditoría y Control, otras organizaciones y la Asociación Nacional de Economistas y Contadores (ANEC).

A las novedades también se suman la Comprobación al Grado de Implementación de la 297/03 en sustitución de la Comprobación Nacional, que otorgaba el aval de con control o sin él. En tal sentido el mes de noviembre fue revelador para conocer las entidades que, según las nuevas categorías, ostentan la condición de Adelantada, Normal o Atrasada, pues se desarrollaron las primeras verificaciones sobre el tema. Con la "297" la suerte está en manos de todos. Ahora el autoexamen dependerá de la constancia en la preparación, del buen flujo de las informaciones, de una precisa evaluación de los riesgos que pueda correr la entidad y, sobre todo, del conocimiento que cada miembro posea sobre sus responsabilidades en el desempeño dentro de ella.

Es el proceso integrado a las operaciones efectuado por la dirección y el resto del personal de una entidad para proporcionar una seguridad razonable al logro de los objetivos siguientes:

- Confiabilidad de la información.
- Eficiencia y eficacia de las operaciones.
- Cumplimiento de las leyes, reglamentos y políticas, establecidas.
- Control de los recursos, de todo tipo, a disposición de la entidad.

1.3.3 Control Interno.

Características generales del Control Interno:

Es un proceso, es decir, un medio para lograr un fin y no un fin en sí mismo. Lo llevan a cabo las personas que actúan en todos los niveles y no se trata solamente de manuales de organización y procedimientos.

En cada área de la organización, la persona encargada de dirigirla es responsable por el Control Interno ante su jefe inmediato de acuerdo con los niveles de autoridad establecidos, en su cumplimiento participan todos los trabajadores de la entidad independientemente de la categoría ocupacional que tengan.

Debe facilitar la consecución de objetivos en una o más de las áreas u operaciones en la empresa.

Aporta un grado de seguridad razonable, aunque no total, en relación con el logro de los objetivos fijados.

Debe propender al logro del autocontrol, liderazgo y fortalecimiento de la autoridad y responsabilidad de los colectivos laborales.

Es de capital importancia destacar, que el Control Interno, no importa que tan bien haya sido diseñado y operado, solamente puede dar una seguridad razonable a la alta dirección sobre el logro de sus objetivos. La probabilidad de logro y eficacia del sistema, se ve afectada en muchas ocasiones, por limitaciones inherentes al Sistema de Control Interno.

Limitaciones del Control Interno

El concepto SEGURIDAD RAZONABLE está relacionado con el reconocimiento explícito de la existencia de limitaciones inherentes del Control Interno. En el desempeño de los controles pueden cometerse errores como resultado de interpretaciones erróneas de instrucciones, errores de juicio, descuido, distracción y fatiga. Las actividades de control dependientes de la separación de funciones, pueden ser burladas por colusión entre trabajadores, es decir, ponerse de acuerdo para dañar a terceros.

La extensión de los controles adoptados en una organización también está limitada por consideraciones de costo, por lo tanto, no es factible establecer controles que proporcionan protección absoluta del fraude y del desperdicio, sino establecer los controles que garanticen una seguridad razonable desde el punto de vista de los costos.

La función del Control Interno es aplicable a todas las áreas de operación de las entidades y organismos estatales, de su efectividad depende que la administración obtenga la información necesaria para seleccionar de las alternativas, las que mejor convengan a los intereses de la entidad. El Control Interno debe establecerse previo estudio de las necesidades y condiciones de cada entidad.

Componentes del Control Interno.

Los componentes o divisiones en que se agrupan las acciones que deben contribuir a conformar un adecuado Sistema de Control Interno, son:

- Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Supervisión y Monitoreo

Como puede observarse la división presentada por la 297 es idéntica a la planteada en el Informe COSO, lo cual nos demuestra que la Resolución 297 tiene un basamento teórico incuestionable en el Informe COSO. Cada uno de estos componentes, están integrados por normas, mientras que en el Informe COSO se habla de factores.

Ambiente de Control:

El ambiente o entorno de control constituye el andamiaje para el desarrollo de las acciones y refleja la actitud asumida por la alta dirección en relación con la importancia del Control Interno y su incidencia sobre las actividades de la entidad. El ambiente de control fija el tono de la organización al influir en la conciencia del personal. Este puede considerarse como la base de los demás componentes del Control Interno, por lo que debe tener presente todas las disposiciones, políticas y regulaciones que se consideren necesarias para su implementación y desarrollo exitoso.

Evaluación de Riesgos:

El Control Interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las entidades. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza, se evalúa la vulnerabilidad del sistema. Para ello debe adquirirse un conocimiento práctico de la entidad y sus componentes como manera de identificar los puntos débiles, enfocando los riesgos tanto de la entidad (internos y externos) como de la actividad. Cabe recordar que los objetivos de control deben ser específicos, así como adecuados, completos, razonables e integrados a los globales de la entidad.

Actividades de Control:

Las actividades de control son procedimientos que ayudan a asegurarse que las políticas de la dirección se llevan a cabo, y deben estar relacionadas con los riesgos que ha determinado y asume la dirección. Estas se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgo, conociendo los riesgos, se disponen los controles destinados a evitarlos o a minimizarlos.

Se manifiesta la necesidad de establecer con claridad los procedimientos necesarios para llevar a cabo las políticas empresariales, un procedimiento no sería útil si se realiza de forma mecánica, sin la existencia de un enfoque continuo de atención hacia el objetivo final.

Información y Comunicación:

La información debe permitir a los funcionarios y trabajadores cumplir sus obligaciones y responsabilidades. Los datos pertinentes deben ser identificados, captados, registrados, estructurados en información y comunicados en tiempo y forma. Una entidad debe disponer de una corriente fluida de arriba hacia abajo y viceversa, así como a todo lo largo de la organización y procurar la exactitud, suficiencia y adecuación de la información relativa a los acontecimientos internos y externos comprobando que esta sea comunicada en tiempo oportuno al personal adecuado.

Supervisión o monitoreo:

Es el proceso que evalúa la calidad del Control Interno en el tiempo. Es importante monitorear el Control Interno para determinar si este está operando en la forma esperada y si es necesario hacer modificaciones. Las actividades de monitoreo permanente incluyen actividades de supervisión realizadas de forma periódica, directamente por las distintas estructuras de dirección, para de esta manera establecer mecanismos para reportar deficiencias y desarrollar acciones correctoras apropiadas y oportunas.

1.3.4 Modelo de Madurez.

El Modelo de Madurez de Capacidades o ***CMM*** (***Capability Maturity Model***), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de ***software*** por la Universidad Carnegie-Mellon para el ***SEI*** (***Software Engineering Institute***).

El SEI es un centro de investigación y desarrollo patrocinado por el Departamento de Defensa de los Estados Unidos de América y gestionado por la Universidad Carnegie-Mellon. "CMM" es una marca registrada del SEI.

A partir de noviembre de 1986 el SEI, a requerimiento del Gobierno Federal de los Estados Unidos de América (en particular del Departamento de Defensa, **DoD**), desarrolló una primera definición de un modelo de madurez de procesos en el desarrollo de ***software***, que se publicó en septiembre de 1987. Este trabajo evolucionó al modelo CMM o SW-CMM (***CMM for Software***), cuya última versión (v1.1) se publicó en febrero de 1993.

Este modelo establece un conjunto de prácticas o procesos clave agrupados en Áreas Clave de Proceso (***KPA - Key Process Area***). Para cada área de proceso define un conjunto de buenas prácticas que habrán de ser:

- Definidas en un procedimiento documentado.
- Provistas (la organización) de los medios y formación necesarios.
- Ejecutadas de un modo sistemático, universal y uniforme (institucionalizadas).
- Medidas.
- Verificadas.

A su vez estas Áreas de Proceso se agrupan en cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez.

Los niveles son:

1 - Inicial. Las organizaciones en este nivel no disponen de un ambiente estable para el desarrollo y mantenimiento de ***software***. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado de los proyectos es impredecible.

2 -Repetible. En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión de proyectos, existen unas métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente.

3 - Definido. Además de una buena gestión de proyectos, a este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos, formación del personal, técnicas de ingeniería más detallada y un nivel más avanzado de métricas en los procesos. Se implementan técnicas de revisión por pares (***peer reviews***).

4 - Gestionado. Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El ***software*** resultante es de alta calidad.

5 - Optimizado. La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Así es como el modelo CMM establece una medida del progreso, conforme al avance en niveles de madurez. Cada nivel a su vez cuenta con un número de áreas de proceso que deben lograrse. El alcanzar estas áreas o estadios se detecta mediante la satisfacción o insatisfacción de varias metas claras y cuantificables. Con la excepción del primer nivel, cada uno de los restantes Niveles de Madurez está compuesto por un cierto número de Áreas Claves de

Proceso, conocidas a través de la documentación del CMM por su sigla inglesa: **KPA**.

Cada KPA identifica un conjunto de actividades y prácticas interrelacionadas, las cuales cuando son realizadas en forma colectiva permiten alcanzar las metas fundamentales del proceso. Las KPAs pueden clasificarse en 3 tipos de proceso: Gestión, Organizacional e Ingeniería.

Las prácticas que deben ser realizadas por cada Área Clave de Proceso están organizadas en 5 Características Comunes, las cuales constituyen propiedades que indican si la implementación y la institucionalización de un proceso clave es efectivo, repetible y duradero.

Estas 5 características son: Compromiso de la realización, la capacidad de realización, las actividades realizadas, las mediciones y el análisis, la verificación de la implementación.

Las organizaciones que utilizan CMM para mejorar sus procesos disponen de una guía útil para orientar sus esfuerzos. Además, el SEI proporciona formación a evaluadores certificados (***Lead Assesors***) capacitados para evaluar y certificar el nivel CMM en el que se encuentra una organización. Esta certificación es requerida por el Departamento de Defensa de los Estados Unidos, pero también es utilizada por multitud de organizaciones de todo el mundo para valorar a sus subcontratistas de ***software***.

Se considera típico que una organización dedique unos 18 meses para progresar un nivel, aunque algunas consiguen mejorarlo. En cualquier caso requiere un amplio esfuerzo y un compromiso intenso de la dirección.

Como consecuencia, muchas organizaciones que realizan funciones de factoría de ***software*** o, en general, ***outsourcing*** de procesos de ***software***, adoptan el modelo CMM y se certifican en alguno de sus niveles

A partir de 2001, en que se presentó el modelo CMMI, el SEI ha dejado de desarrollar el SW-CMM, cesando la formación de los evaluadores en diciembre de 2003, quienes dispondrán hasta fin de 2005 para reciclarse al CMMI. Las organizaciones que sigan el modelo SW-CMM podrán continuar haciéndolo, pero ya no podrán ser certificadas a partir de fin de 2005.

SE-CMM

El Modelo de Madurez de Capacidades en la Ingeniería de Sistemas fue publicado por el SEI en noviembre de 1995. Está dedicado a las actividades de ingeniería de sistemas.

Define 18 áreas de proceso divididas en tres grupos:

- Ingeniería (7)
- Proyectos (5)
- Organizativas (6)

No utiliza niveles de madurez generales sino que en cada área de proceso una organización puede alcanzar un determinado nivel de madurez.

Al igual que el SW-CMM, ha sido integrado en el CMMI.

El Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas es un modelo derivado del CMM y que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas.

Ha sido desarrollado por la "***International Systems Security Engineering Association (ISSEA)***", organización sin ánimo de lucro patrocinada por un buen número de compañías dedicadas a la seguridad de sistemas.

Nació a partir de 1993 bajo los auspicios de la Agencia Nacional de Seguridad (NSA) de los E.U.A., con la participación de numerosas compañías de los sectores de tecnologías de la información, seguridad y defensa. La primera versión data de 1997 y la actual (v3.0) fue publicada en junio de 2003.

Pretende servir como:

Herramienta para que las organizaciones evalúen las prácticas de ingeniería de seguridad y definan mejoras a las mismas.

Mecanismo estándar para que los clientes puedan evaluar la capacidad de los proveedores de ingeniería de seguridad. Base para la organización de un mecanismo de evaluación y certificación. A diferencia del CMM original, las áreas de proceso no están agrupadas en función de los niveles de madurez, sino que define 22 áreas para cada una de las cuales se puede alcanzar un nivel en función del cumplimiento de unas "características comunes".

1.3.5 ITIL

ITIL (***IT Infrastructure Library***, biblioteca de infraestructura de TI) igual a Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

Como marco de referencia, ITIL se creó como un modelo para la administración de servicios de TI e incluye información sobre las metas, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar a las áreas de TI.

Desde sus inicios ITIL fue puesta a disposición del público en forma de un conjunto de libros, de ahí su nombre, para que las organizaciones de todo el mundo pudieran adoptarlo. La primera versión consistía de 10 libros principales que cubrían dos grandes temas: “Soporte al servicio” y “Entrega del servicio”, amén de una serie de libros complementarios que cubrían temas tan disímbolos como la administración de la continuidad o cuestiones relacionadas con cableado. Posteriormente, en 2001 se hizo una reestructura importante que reunió los 19 libros principales en sólo 2, mientras que otros temas siguieron en libros separados, dando así un total de 7 libros para la segunda versión de ITIL:

1. Soporte al servicio.
2. Entrega del servicio.
3. Administración de la seguridad.
4. Administración de la infraestructura ICT.
5. Administración de las aplicaciones.
6. La perspectiva del negocio.
7. Planeación para implantar la administración de servicios.

Precisamente con la versión 2, a mediados de los años 90, ITIL fue reconocido como un “estándar de facto” para la administración de servicios de TI, el cual, como siempre, tuvo que seguir evolucionando para considerar las nuevas

escuelas de pensamiento y alinearse mejor a otros estándares, metodologías y mejores prácticas, lo que llevó en 2007 a la liberación de la versión 3 de ITIL.

ITIL V3 sólo consta de cinco libros, que están estructurados en torno al ciclo de vida del servicio:

1. Estrategia de servicios.
2. Diseño de servicios
3. Transición de servicios.
4. Operación de servicios.
5. Mejora continua de servicios.

Esta nueva estructura organiza los procesos de ITIL V2 con contenido y procesos adicionales encaminados a una mejor administración del periodo de vida de los servicios de TI. Partiendo de esta observación, podemos afirmar que la V3 refuerza el foco en los servicios de TI, sin dejar de lado los procesos, pero haciendo patente que aunque los procesos son importantes son secundarios y sólo existen para planificar, entregar y dar soporte a los servicios.

Las mejores prácticas no tienen un fundamento matemático o analítico puro, simplemente son obtenidas del mundo real y representan lo que “parece ser lo mejor” hasta el momento. Como tales, las mejores prácticas pueden cambiar con el transcurso del tiempo y, lo que también es muy importante, ser muy cuidadoso al establecerlas para no llegar a conclusiones erradas o ilógicas que lleven a unas “mejores prácticas” absurdas. Dado que ITIL no es un estándar, es importante comprender que una empresa no puede certificarse en ITIL. Lo más que puede obtenerse es una especie de diagnóstico en el que alguna empresa de consultoría puede opinar que, desde su punto de vista, cierta organización “está alineada” con ITIL. Las únicas certificaciones disponibles actualmente son para personas, que de esta manera reciben un aval sobre sus conocimientos de parte de los organismos que desarrollan ITIL.

ITIL es un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos. Por lo que los libros de ITIL listan una serie de procesos y funciones que se recomienda implantar para una mejor entrega de los servicios que las áreas de TI proporcionan a sus usuarios. La idea es que toda organización de TI opere con un enfoque de procesos para la administración de servicios de TI, empleando ITIL como una guía sobre qué procesos implantar y cuáles son las características principales de dichos procesos.

En ITIL V2 (*Figura 1.6*) se definió un modelo de procesos cuyo núcleo lo constituyen los libros de “Soporte de servicios” y “Entrega de servicios”, y juntos forman la “Administración de servicios”.

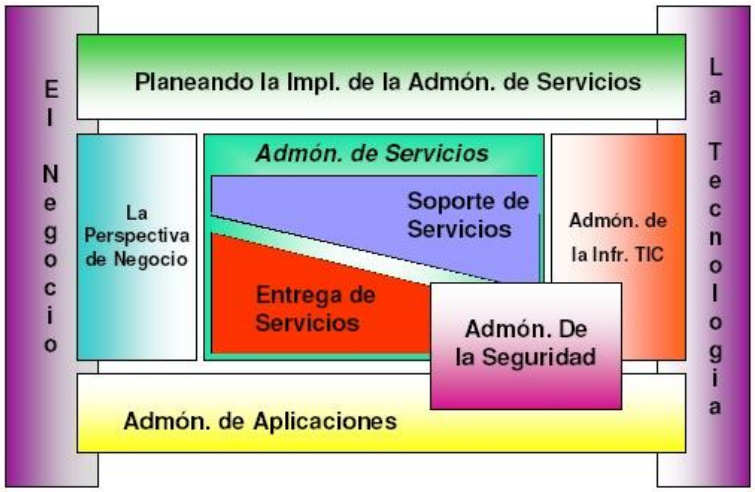


Figura 1.6. Modelo de Procesos de ITIL V2

Soporte de servicios

Administración de la configuración: Proceso cuyo objetivo es lograr el “control de la infraestructura”. La idea es tener claridad en los componentes de la infraestructura involucrados en la prestación de los servicios, la documentación (configuración) de los mismos y las relaciones entre ellos.

Administración de incidentes. Enfocado a lograr, lo antes posible, la restauración de los servicios cuando éstos quedan inoperables o degradados a causa de un incidente.

Administración de problemas. Proceso responsable de identificar la causa raíz de los incidentes para evitar su repetición y minimizar el impacto sobre las operaciones del negocio.

Administración de cambios. Garantiza el uso de métodos estandarizados para la realización de cambios en la infraestructura, minimizando así el impacto de los incidentes relacionados con dichos cambios.

Administración de liberaciones. Permite una visión integral de los cambios para asegurar que en su implantación se hagan las pruebas necesarias y se consideren tanto los aspectos técnicos como los no técnicos de la liberación.

Mesa de ayuda. Función en el organigrama con actividades de gran importancia en la interrelación de TI con sus usuarios: es parte fundamental del proceso de incidentes al ser el punto único de contacto para aconsejar, guiar, y restaurar rápidamente los servicios normales de los clientes y usuarios.

Entrega de servicios

Administración de niveles de servicio. Proceso encargado de mantener y mejorar la calidad de los servicios de TI mediante la definición, monitoreo y reporte de los niveles de servicio.

Administración financiera de TI. Provee guías para la utilización eficiente, en cuanto a costos, de los recursos de TI.

Administración de la capacidad. Proceso que asegura que la capacidad de los recursos de TI sea suficiente para cumplir las necesidades presentes y futuras del negocio, siempre a un costo adecuado.

Administración de la disponibilidad. Permite ofrecer un nivel de disponibilidad sostenido en los servicios de TI, con un costo adecuado para que el negocio pueda alcanzar sus objetivos.

Administración de la continuidad. Proceso que permite la continuidad de los servicios de TI para que, en caso de un desastre, se recuperen dentro de los tiempos y costos acordados.

ITIL V3 (*Figura 1.7*), al igual que la versión anterior, define un modelo de procesos basado en la administración de servicios, sólo que ahora dichos procesos están supeditados al ciclo de vida de las aplicaciones y los servicios de TI

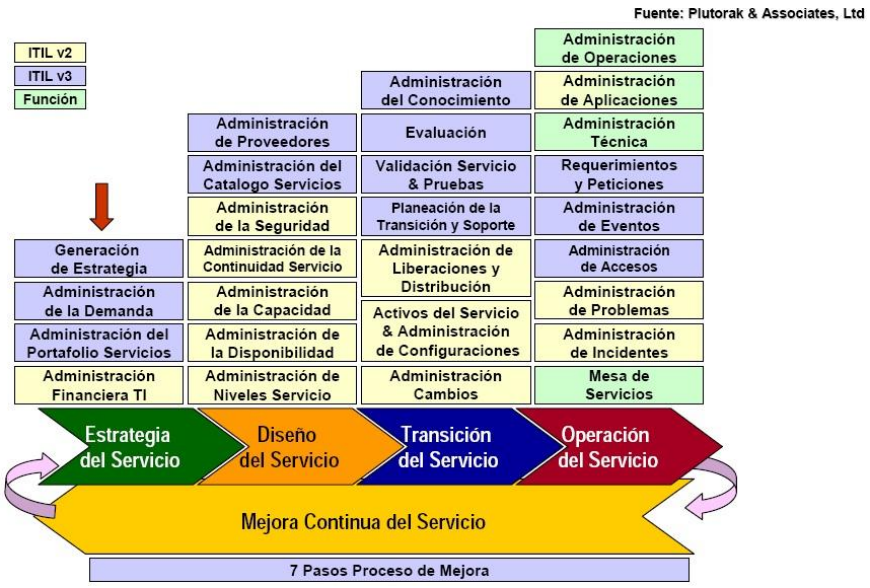


Figura 1.7. Funciones y Procesos Considerados en ITIL V3

1.3.6 COBIT e ISACA

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

La creciente dependencia en información y en los sistemas que proporcionan dicha información

La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información (***information warfare***). La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información;

El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y Las prácticas de negocio, crear nuevas oportunidades y reducir costos para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa.

Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI. Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos Mainframe. Por lo tanto, la administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega) al tiempo que demanda que esto se realice a un costo más bajo. Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados. ***COBIT*** ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona "prácticas sanas" a través de un Marco Referencial de dominios y procesos y presenta actividades en una estructura manejable y lógica. Las prácticas sanas de ***COBIT*** representan el consenso de los expertos (le ayudarán a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo usted será juzgado si las cosas salen mal.

Las organizaciones deben cumplir con requerimientos de calidad, de reportes fiduciarios y de seguridad, tanto para su información, como para sus activos. La administración deberá obtener un balance adecuado en el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la administración deberá establecer un sistema adecuado de control interno. Por lo tanto, este sistema o marco referencial deberá existir para proporcionar soporte a los procesos de negocio y debe ser preciso en la forma en la que cada actividad individual de control satisface los requerimientos de información y puede impactar a los recursos de TI. El impacto en los recursos de TI es enfatizado en el Marco Referencial de ***COBIT*** conjuntamente a los requerimientos de información del negocio que deben ser alcanzados: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

La administración, mediante este gobierno corporativo, debe asegurar que la debida diligencia sea ejercitada por todos los individuos involucrados en la administración, empleo, diseño, desarrollo, mantenimiento u operación de sistemas de información.

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI.

La orientación a negocios es el tema principal de ***COBIT***. Está diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación ***(Checklist)*** detallada para los propietarios de los procesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y otorgamiento de autoridad (***Empowerment***) de los dueños de procesos para que estos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados. El Marco Referencial de ***COBIT*** proporciona herramientas al propietario de procesos de negocio que facilitan el cumplimiento de esta responsabilidad. El Marco Referencial comienza con una premisa simple y práctica:

Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos de TI agrupados en forma natural.

Continúa con un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios: planeación & organización, adquisición & implementación, entrega (de servicio) y monitoreo. Esta estructura cubre todos los aspectos de información y de la tecnología que la soporta. Dirigiendo estos 34 Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información. Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría o de aseguramiento que permite la revisión de los procesos de TI contra los 302 objetivos detallados de control recomendados por ***COBIT*** para proporcionar a la Gerencia la certeza de su cumplimiento y/o una recomendación para su mejora. ***COBIT*** contiene un conjunto de herramientas de implementación que proporciona lecciones aprendidas por empresas que rápida y exitosamente aplicaron ***COBIT*** en sus ambientes de trabajo. Incluye un Resumen Ejecutivo para el entendimiento y la sensibilización de la alta gerencia sobre los principios y conceptos fundamentales de ***COBIT.*** La guía de implementación cuenta con dos útiles herramientas (Diagnóstico de Sensibilización Gerencial – ***Management Awareness Diagnostic***– y Diagnóstico de Control en TI – ***IT Control Diagnostic*** –) para proporcionar asistencia en el análisis del ambiente de control en una organización.

El Marco Referencial ***COBIT*** otorga especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el Marco Referencial proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con Tecnología de Información.

La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en TI para medir en forma comparativa ***(Benchmark***) tanto su ambiente de TI existente, como su ambiente planeado. ***COBIT*** es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio. Así mismo ***COBIT*** habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de organizaciones, a nivel mundial. El objetivo de ***COBIT*** es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

1.4 Gestión de Riesgos en TIC.

“Según el diccionario de la Real Academia Española el riesgo es la proximidad de un daño y viene de Del italiano risico o rischio, y este del árabe clásico Rizq, que quiere decir “lo que depara la providencia”.

La palabra riesgo proviene del Latín Riscara que significa atreverse o transitar por un sendero peligroso. En realidad tiene un significado negativo, relacionado con peligro, daño siniestro o pérdida. Sin embargo, el Riesgo es parte inevitable de los procesos de toma de decisiones en general. En este sentido, el riesgo es una opción en lugar de un destino de las acciones que nos atrevemos a tomar, depende la toma de decisiones, son lo que la historia de riesgos es para todos nosotros y que la historia ayuda a definir lo que significa ser un ser humano, el riesgo está presente en las organizaciones en todos los niveles de operación, desde el nivel estratégico al nivel operativo al nivel táctico, pero normalmente se describe como un negocio o el riesgo operativo

Desde el comienzo de la década de 1990, ha habido un cambio significativo en el nivel de y el tipo de riesgo que todos los sectores de gobierno y la industria han estado expuestos a la política de AR debe ser alto nivel basada en los objetivos del negocio, los objetivos de la seguridad, un enfoque bien definido, responsabilidades, alcances y desventajas; todos estos aspectos, de formas

claras y acordados. De igual manera, estas políticas deberán ser bien comunicadas a todo el personal involucrado

1.4.1 Elementos Relacionados

Identificar los recursos

Realizar una lista de los recursos que se necesitan para proteger, se necesita un amplio conocimiento de las instalaciones, contratos con proveedores, garantías, leyes, etc. Los recursos a proteger incluyen tangibles e intangibles, incluir todo lo que se considere de valor y para esto, considerar la pérdida o daño de un recurso en términos de pérdida de tiempo, costo, reparación, utilidad o reemplazo.

Análisis de amenazas

Esta área incluye la identificación de amenazas que puedan impactar el ambiente o infraestructura evaluada. Las amenazas pueden ser ambientales, como fuego, terremotos, explosiones e inundaciones. Deben de incluir eventos raros, pero posibles, como fallas en la estructura del edificio.

Amenazas, tales como: Perdida de servicios elementales (luz, agua, teléfono, electricidad) por un periodo de tiempo largo; Inundación; Robo de discos o cintas.; Robo de laptops; Robo de computadoras; Virus; Proveedores en quiebra; “Bugs” en el ***software***; Contratistas; Terrorismos políticos; Mal uso de los recursos, profanando a la empresa.

Identificación de recursos y valoración

Esta tarea incluye las identificaciones de los recursos valiosos del ambiente, tanto tangibles como intangibles. Se tiene que cuantificar los costos de reposición, aso como la valoración del recurso de la información en cuanto a su disponibilidad, integridad y confidencialidad. Esta tarea es análoga a un BIA en cuanto que identifica los recursos, los riesgos que sufren y su valor.

Realizar una lista de los recursos que se necesitan para proteger.

- Se necesita un amplio conocimiento de las instalaciones, contratos con proveedores, garantías, leyes, etc.

- Los recursos a proteger incluyen tangibles e intangibles, incluir todo lo que se considere de valor.
- Y para esto, considerar la pérdida o daño de un recurso en términos de pérdida de tiempo, costo, reparación, utilidad o reemplazo.

Algunos recursos pueden incluir son:

Tangibles: computadoras, información propietaria, respaldos y archivos, manuales, guías y libros, cd's o disquetes (de ***software***), registros personales, registros de auditoría,

Intangibles: seguridad y salud del personal, privacidad de los usuarios, contraseñas personales, imagen pública y reputación, beneficio del cliente, disponibilidad de procesamiento, información de configuración

El hecho de no contar con un plan de contingencias para responder a un desastre, tendrá como consecuencia el hecho de actuar sin previa planeación ni coordinación.

De ahí que el costo de tratar de salvar o arreglar los daños no están cuantificados y no se puede saber si va a salir más caro solucionar un problema o mejor dejarlo y arreglarlo de alguna otra manera.

Análisis costo-beneficio

Esta tarea incluye la valoración del grado de una reducción de riesgo, la cual se espera alcanzar mediante la implantación de las salvaguardas de reducción de riesgos seleccionadas. El beneficio bruto menos el costo anual de las salvaguardas seleccionadas para alcanzar la reducción del nivel de riesgo, nos lleva al beneficio neto. Herramientas para calcular el retorno de la inversión o el valor presente, siempre son utilizadas para realizar un análisis más detallado de la actividad de los costos de las salvaguardas.

1.4.2.Tipos de Riesgo

Cuantitativo: La característica principal es la de minimizar la subjetividad en la toma de decisiones. El uso de métricas objetivas, asignándoles valor para tener una visión más clara.

Cualitativo: El uso de métricas subjetivas, como priorización utilizando claves como bajo, medio y alto

Elementos de Métricas de Riesgo

- Valor del recurso
- Frecuencia de la amenaza
- Factor de exposición de la amenaza
- Efectividad de la salvaguarda
- Costo de la salvaguarda
- Incertidumbre

Análisis de Riesgo

- Valor de perdida unitaria (SLE)
- Frecuencia anual de ocurrencia (ARO)
- Valor de pérdida anual (ALE)
- Factor de exposición (EF)
- Probabilidad
- Riesgo
- Análisis de Riesgo (Risk Analysis)
- Valoración del Riesgo (Risk Assessment)
- Administración del Riesgo (Risk Management)

1.4.3. ISO 27001

El estándar para la seguridad de la información ISO/IEC-27001 (***Information technology – Security techniques – Information security management systems – Requirements)*** fue aprobado y publicado en 2005 por la International ***Organization for Standardization*** y por la ***International Electrotechnical Commission***, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) *Figura 1.8.*

BS17799 -ISO 27001.

Contiene 133 controles aplicables, que ayudarán a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información, su origen está en la norma de BSI (British Standards Institution) BS7799-Parte1, que fue publicada por primera vez en 1995. No es certificable.

ISO 27001 contiene un anexo A, que considera los controles de la norma ISO 17799 para su posible aplicación en el SGSI que implante cada organización (justificando, en el documento denominado “Declaración de Aplicabilidad”, los motivos de exclusión de aquellos que finalmente no sean necesarios).

Historia de ISO 27001 e ISO 17799

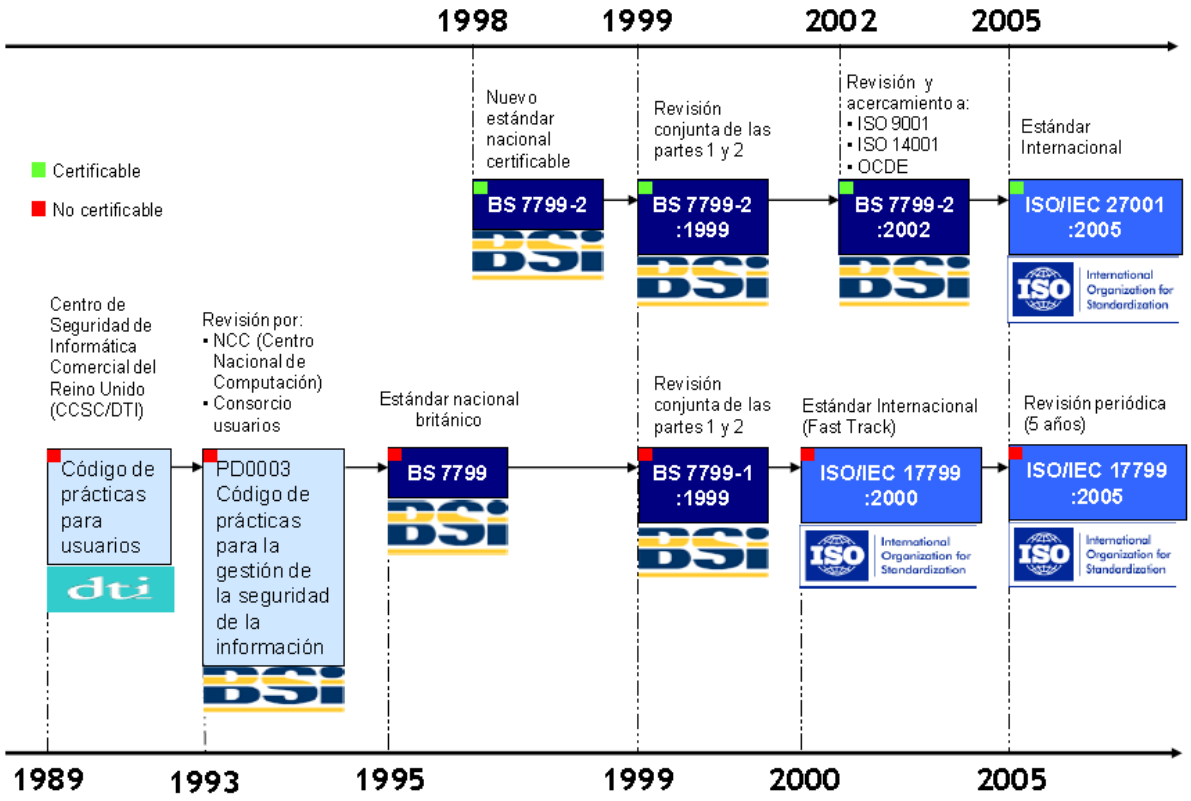


Figura 1.8. Historia de ISO 27001 e ISO 17799

Importancia del Sistema de Gestión de la Seguridad de la Información (SGSI).

1. Proporciona el mejor reconocimiento oficialmente reconocido para el SGSI.

2. Para proteger las ventajas de la información.

3. Incrementa el Compromiso interno dado que el sistema permite garantizar la eficacia de los esfuerzos desarrollados en materia de Gestión de Seguridad de la Información en todos los niveles de la Organización.

4. Para salvaguardar ventajas competitivas sobre técnicas avanzadas en gestión, mejora de procesos, nuevos desarrollos de ***software***.

5. Incrementar la confianza y la reputación corporativa de la Organización hacia los Clientes, Empleados, Accionistas, y Proveedores.

6. Para obtener posibles reducciones en las primas de su seguro, vinculadas a una posible disminución de los incidentes en materia de Seguridad de la Información.

7. Para evitar pérdidas, robos, descuidos, etc., con los activos de información en las organizaciones.

8. Para garantizar la Conformidad y el cumplimiento a las autoridades competentes de los aspectos referentes a la reglamentación y leyes aplicables, pudiendo evidenciarlo mediante registros.

9. Proporciona una mejora en la Gestión del Riesgo Financiero de la Organización evitando posibles sanciones, pérdida de valor en bolsa, reducción facturación.

Norma ISO del 27001:2005

La norma establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información (*Figura 1.9)*:

1. Política de seguridad.

2. Aspectos organizativos para la seguridad.

3. Clasificación y control de activos.

4. Seguridad ligada al personal.

5. Seguridad física y del entorno.

6. Gestión de comunicación es y operaciones.

7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.

9. Gestión de continuidad del negocio.

10. Conformidad con la legislación.

Se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

Figura 1.9 División de Norma ISO 27001:2005.

Aspectos organizativos para la seguridad.

Gestionar la seguridad de la información dentro de la organización. Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por tercero. Mantener la seguridad de la información cuando la responsabilidad de su tratamientos e ha externalizado a otra organización.

Seguridad ligada al personal.

Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

CAPÍTULO II

Aplicaciones Web

2.1. Sistemas Operativos.

2.1.1. Windows Server.

Windows Server es una plataforma de fácil administración, para el desarrollo y alojamiento fiable de aplicaciones y servicios web que se entregan del servidor o a través de la Web. Las características incluye la administración simplificada. Cuenta con una configuración rápida de aplicaciones y servicios web, y de una plataforma web personalizada.

2.1.2. Unix.

Unix (registrado oficialmente como ***UNIX***®) es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy.1 2

Hasta 2009, el propietario de la marca ***UNIX***® fue ***The Open Group,*** un consorcio de normalización industrial. A partir de marzo de 2010 y tras una larga batalla legal, esta ha pasado nuevamente a ser propiedad de Novell, Inc. Sólo los sistemas totalmente compatibles y que se encuentran certificados por la especificación pueden ser denominados "***UNIX***®" (otros reciben la denominación "similar a un sistema ***Unix***" o "similar a ***Unix***"). En ocasiones, suele usarse el término "***Unix*** tradicional" para referirse a Unix o a un sistema operativo que cuenta con las características de ***UNIX Versión 7*** o ***UNIX System V***.

2.1.3. Linux.

Es un sistema informático de tipo Unix operativo montado en el marco del modelo de desarrollo de *software* de código libre y abierto. El componente de la definición de Linux es el ***kernel*** de Linux, un núcleo del sistema operativo lanzado por primera vez 05 de octubre 1991 por Linus Torvalds.

Linux fue desarrollado originalmente como un sistema operativo libre para Intel x86 basados en computadoras personales. Desde entonces, ha sido portado a más plataformas de hardware que cualquier otro sistema operativo. Se trata de un sistema operativo líder en servidores y otros sistemas de hierro grandes, tales como computadoras centrales y supercomputadoras: más del 90% de los mejores de hoy en día 500 supercomputadoras ejecutar alguna variante de Linux,

incluyendo el más rápido 10. Linux también se ejecuta en sistemas embebidos (dispositivos en los que se suele ser el sistema operativo integrado en el firmware y altamente adaptada al sistema), tales como teléfonos móviles, ***Tablet*** PC, ***routers***, televisores y consolas de videojuegos, el sistema ***Android*** de amplio uso en los dispositivos móviles se basa en el ***kernel*** de ***Linux***.

El desarrollo de Linux es uno de los ejemplos más destacados de la colaboración de ***software*** de código libre y abierto: el código fuente subyacente puede ser utilizado, modificado y distribuido-comercial o no comercial, por cualquier persona bajo licencias como la Licencia Pública General de GNU. Normalmente, Linux está empaquetado en un formato conocido como una distribución de Linux para uso de escritorio y servidor. Algunos populares principales distribuciones de Linux incluyen de ***Debian*** (y sus derivados como ***Ubuntu***), ***Fedora*** y ***openSUSE***. Distribuciones de Linux incluyen el ***kernel*** de Linux, servicios de apoyo y de las bibliotecas y por lo general una gran cantidad de *software* de aplicación para cumplir con el uso previsto de la distribución.

Una distribución orientada hacia el uso de escritorio suelen incluir el sistema X ***Window*** y un entorno de escritorio de acompañamiento tales como ***GNOME*** o ***KDE Plasma***. Algunas distribuciones pueden incluir un escritorio menos intensivo de recursos, tales como ***LXDE o Xfce*** para su uso en ordenadores más antiguos o menos poderosos. Una distribución destinada para funcionar como un servidor puede omitir todos los entornos gráficos de la instalación estándar y en lugar de incluir otros programas como el Servidor Apache HTTP y un servidor SSH como ***OpenSSH***. Debido a que Linux es de libre distribución, cualquier persona puede crear una distribución para cualquier uso. Aplicaciones de escritorio de uso común con los sistemas Linux incluyen el navegador web ***Mozilla Firefox***, la suite de oficina ***LibreOffice*** aplicación, y el editor de imágenes GIMP.

2.2 Plataformas.

2.2.1. Apache.

El ***servidor HTTP*** Apache es un ***servidor web HTTP*** de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.12 y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que Behelendorf quería que tuviese la connotación de algo que es firme y enérgico pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de EEUU, y en esos momentos la preocupación de su

grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de internet. Además Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. En inglés, ***apatchy server*** (un servidor "parcheado") suena igual que Apache Server.

El servidor Apache se desarrolla dentro del proyecto ***HTTP Server (httpd)*** de la ***Apache Software Foundation***. Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años. (Estadísticas históricas y de uso diario proporcionadas por ***Netcraft3***).

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

2.2.2. IIS.

Internet Information Services o IIS1 es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Originalmente era parte del Option Pack para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS. Antiguamente se denominaba ***PWS*** (***Personal Web Server***), y actualmente forma parte de la distribución estándar de Windows, de modo que no se necesita una licencia extra para instalarlo. Este servicio convierte a una PC en un servidor web para Internet o una intranet, es decir que en las computadoras que tienen este servicio instalado se pueden publicar páginas web tanto local como remotamente.

Los servicios de ***Internet Information Services*** proporcionan las herramientas y funciones necesarias para administrar de forma sencilla un servidor web seguro. El servidor web se basa en varios módulos que le dan capacidad para procesar distintos tipos de páginas. Por ejemplo, Microsoft incluye los de ***Active Server***

Pages (ASP) y ASP.NET. También pueden ser incluidos los de otros fabricantes, como PHP o Perl.

IIS fue inicialmente lanzado como un conjunto de servicios basados en Internet para Windows NT 3.51. IIS 2.0 siguió agregando soporte para el sistema operativo Windows NT 4.0 y IIS 3.0 introdujo las ***Active Server Pages***, una tecnología de scripting dinámico. IIS 4.0 eliminó el soporte para el protocolo ***Gopher*** y fue puesto con Windows NT como un CD-ROM de "Paquete Opcional" separado.

La versión actual de IIS es la 7.5 para Windows Server 2008 y IIS 5.1 para Windows XP Professional. IIS 5.1 para Windows XP es una versión compacta del IIS que soporta sólo 10 conexiones simultáneas y sólo un sitio web. IIS 6.0 ha agregado soporte para IPv6. Windows Vista viene con IIS 7.0 preinstalado. No limitará el número de conexiones permitidas pero limitará el flujo de tareas basándose en las solicitudes activas concurrentes, mejorando el uso y el rendimiento en escenarios punto-a-punto (***peer-to-peer***).

2.2.3. JBoss.

JBoss es un servidor de aplicaciones J2EE de código abierto implementado en Java puro. Al estar basado en Java, ***JBoss*** puede ser utilizado en cualquier sistema operativo para el que esté disponible Java. Los principales desarrolladores trabajan para una empresa de servicios, ***JBoss*** Inc., adquirida por ***Red Hat*** en abril del 2006, fundada por Marc Fleury, el creador de la primera versión de ***JBoss***. El proyecto está apoyado por una red mundial de colaboradores. Los ingresos de la empresa están basados en un modelo de negocio de servicios.

JBoss implementa todo el paquete de servicios de J2EE.

JBoss AS es el primer servidor de aplicaciones de código abierto, preparado para la producción y certificado J2EE 1.4, disponible en el mercado, ofreciendo una plataforma de alto rendimiento para aplicaciones de ***e-business***. Combinando una arquitectura orientada a servicios revolucionaria con una licencia de código abierto, ***JBoss AS*** puede ser descargado, utilizado, incrustado y distribuido sin restricciones por la licencia. Por este motivo es la plataforma más popular de middleware para desarrolladores, vendedores independientes de ***software*** y, también, para grandes empresas. Las características destacadas de ***JBoss*** incluyen:

- Producto de licencia de código abierto sin coste adicional.
- Cumple los estándares.
- Confiable a nivel de empresa
- Incrustable, orientado a arquitectura de servicios.
- Flexibilidad consistente
- Servicios del middleware para cualquier objeto de Java
- Ayuda profesional 24x7 de la fuente
- Soporte completo para JMX

2.2.4. GlassFish.

GlassFish es un servidor de aplicaciones de ***software*** libre desarrollado por ***Sun Microsystems***, compañía adquirida por ***Oracle Corporation***, que implementa las tecnologías definidas en la plataforma Java EE y permite ejecutar aplicaciones que siguen esta especificación. La versión comercial es denominada ***Oracle GlassFish Enterprise Server*** (antes ***Sun GlassFish Enterprise Server***). Es gratuito y de código libre, se distribuye bajo un licenciamiento dual a través de la licencia CDDL y la GNU GPL.

GlassFish está basado en el código fuente donado por ***Sun*** y ***Oracle Corporation***, éste último proporcionó el módulo de persistencia ***TopLink. GlassFish*** tiene como base al servidor ***Sun Java System Application Server de Oracle Corporation***, un derivado de Apache ***Tomcat***, y que usa un componente adicional llamado ***Grizzly*** que usa Java NIO para escalabilidad y velocidad.

2.3. Lenguajes.

2.3.1. ASP.

El lenguaje ***ASP (Active Server Pages***), es un lenguaje de programación de servidores para generar páginas Web dinámicamente. Se conocen cuatro versiones de este lenguaje las 1.0, 2.0, 3.0 y la ***ASP.NET*** que se la conoce como la ASP Clásica.

El lenguaje de programación ASP nace aproximadamente en el año 1996, lo que ofrecía de nuevo este lenguaje era que se podía crear una página web en la que se pudiese programar para que nos ofreciera unos determinados datos. Esto era una gran ventaja porque en aquella época solo se podía dibujar una tabla e incluir unos pocos datos.

Posteriormente se crea el lenguaje ASP.Net que es un lenguaje mucho más complejo que el original ASP. Este lenguaje nos permite separar en las páginas webs la parte de diseño que contiene la página, no interviniendo para nada el código HTML. Así el trabajo de los diseñadores y programadores es mucho más sencillo. Cada cual se ocupa de su parte del trabajo dentro de la página web sin interferir en la parte de otro.

El ASP es un lenguaje de programación para servidores es adecuado para acceso a bases de datos, lectura de ficheros, etc. Se vale de dos lenguajes de ***Script***, como son el ***VBScript*** y el ***JavaScript*** para que lo que programemos con el ASP sea visible.

El lenguaje ASP a grandes rasgos funciona así: un computador cliente hace una petición de una página ASP. El computador servidor interpreta esta petición y le envía una página web. El resultado final es una página HTML que se le envía al cliente. El usuario no llega nunca a ver el código ASP, sino que ve el resultado de interpretar dicho código, es decir, una página HTML.

2.3.2. PHP.

PHP es un lenguaje de programación interpretado (Lenguaje de alto rendimiento), diseñado originalmente para la creación de páginas web dinámicas. Se usa principalmente para la interpretación del lado del servidor (***server-side scripting)*** pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica usando las bibliotecas Qt o GTK+.

PHP es un acrónimo recursivo que significa PHP Hipertexto Pre-procesador (inicialmente PHP Tools, o, Personal Home Page Tools). Fue creado originalmente por Rasmus Lerdorf en 1994; sin embargo la implementación principal de PHP es producida ahora por ***The PHP Group*** y sirve como el estándar de facto para PHP al no haber una especificación formal. Publicado bajo la ***PHP License,*** la Free ***Software Foundation*** considera esta licencia como ***software*** libre.

Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas sin costo alguno. El lenguaje PHP se encuentra instalado en más de 20 millones de sitios web y en un millón de servidores, el número de sitios en PHP ha compartido algo de su preponderante dominio con otros nuevos lenguajes no tan poderosos desde agosto de 2005. Es también el módulo Apache más popular entre las computadoras que utilizan Apache como servidor web.

El gran parecido que posee PHP con los lenguajes más comunes de programación estructurada, como C y Perl, permiten a la mayoría de los programadores crear aplicaciones complejas con una curva de aprendizaje muy corta. También les permite involucrarse con aplicaciones de contenido dinámico sin tener que aprender todo un nuevo grupo de funciones.

Aunque todo en su diseño está orientado a facilitar la creación de sitios webs, es posible crear aplicaciones con una interfaz gráfica para el usuario, utilizando la extensión PHP-Qt o PHP-GTK. También puede ser usado desde la línea de órdenes, de la misma manera como ***Perl*** o ***Python*** pueden hacerlo; a esta versión de PHP se la llama ***PHP-CLI (Command Line Interface)***.

2.3.3. Java.

Java es un lenguaje de programación orientado a objetos, desarrollado por ***Sun Microsystems*** a principios de los años 90. El lenguaje en sí mismo toma mucha de su sintaxis de C y C++, pero tiene un modelo de objetos más simple y elimina herramientas de bajo nivel, que suelen inducir a muchos errores, como la manipulación directa de punteros o memoria. La memoria es gestionada mediante un recolector de basura.

Las aplicaciones Java están típicamente compiladas en un ***bytecode***, aunque la compilación en código máquina nativo también es posible. En el tiempo de ejecución, el ***bytecode*** es normalmente interpretado o compilado a código nativo para la ejecución, aunque la ejecución directa por hardware del ***bytecode*** por un procesador Java también es posible.

La implementación original y de referencia del compilador, la máquina virtual y las bibliotecas de clases de Java fueron desarrolladas por ***Sun Microsystems*** en 1995. Desde entonces, ***Sun*** ha controlado las especificaciones, el desarrollo y evolución del lenguaje a través del ***Java Community Process***, si bien otros han desarrollado también implementaciones alternativas de estas tecnologías de ***Sun***, algunas incluso bajo licencias de ***software*** libre.

Entre diciembre de 2006 y mayo de 2007, ***Sun Microsystems*** liberó la mayor parte de sus tecnologías Java bajo la licencia GNU GPL, de acuerdo con las especificaciones del ***Java Community Process,*** de tal forma que prácticamente todo el Java de ***Sun*** es ahora ***software*** libre (aunque la biblioteca de clases de ***Sun*** que se requiere para ejecutar los programas Java aún no lo es).

2.3.4. Phyton.

Python es un lenguaje de programación de alto nivel cuya filosofía hace hincapié en una sintaxis muy limpia y que favorezca un código legible.

Se trata de un lenguaje de **programación multiparadigma** ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, usa tipiado dinámico, es fuertemente tipiado y multiplataforma. Es administrado por la ***Python Software Foundation***. Posee una licencia de código abierto, denominada ***Python Software Foundation License***, que es compatible con la Licencia pública general de GNU a partir de la versión 2.1.1, e incompatible en ciertas versiones anteriores.

Python es un lenguaje de programación multiparadigma. Esto significa que más que forzar a los programadores a adoptar un estilo particular de programación, permite varios estilos: programación orientada a objetos, programación imperativa y programación funcional. Otros paradigmas están soportados mediante el uso de extensiones. Usa tipiado dinámico y conteo de referencias para la administración de memoria.

Una característica importante de ***Python*** es la resolución dinámica de nombres; es decir, lo que enlaza un método y un nombre de variable durante la ejecución del programa (también llamado ligadura dinámica de métodos). Otro objetivo del diseño del lenguaje es la facilidad de extensión. Se pueden escribir nuevos módulos fácilmente en C o C++. ***Python*** puede incluirse en aplicaciones que necesitan una interfaz programable.

2.3.5. Perl.

Perl es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado ***bourne shell (sh), AWK, sed, Lisp*** y, en un grado inferior, de muchos otros lenguajes de programación. Estructuralmente, Perl está basado en un estilo de bloques como los del C o AWK, y fue ampliamente adoptado por su destreza en el procesador de texto y no tener ninguna de las limitaciones de los otros lenguajes de script. La estructura completa de Perl deriva ampliamente del lenguaje C. Perl es un lenguaje imperativo, con variables, expresiones, asignaciones, bloques de código delimitados por llaves, estructuras de control y subrutinas.

Perl también toma características de la programación Shell. Todas las variables son marcadas con un Sigilo precedente. Los sigilos identifican inequívocamente los nombres de las variables, permitiendo a Perl tener una rica sintaxis. Notablemente, los sigilos permiten interpolar variables directamente dentro de las cadenas de caracteres (***strings***). Como en los ***shell***, Perl tiene muchas funciones integradas para tareas comunes y para acceder a los recursos del sistema. Perl toma las listas del ***Lisp***, hash (memoria asociativa) del AWK y expresiones regulares del sed. Todo esto simplifica y facilita todas las formas del análisis sintáctico, manejo de texto y tareas de gestión de datos.

En Perl 5, se añadieron características para soportar estructuras de datos complejas, funciones de primer orden (p. e. clausuras como valores) y un modelo de programación orientada a objetos. Éstos incluyen referencias, paquetes y una ejecución de métodos basada en clases y la introducción de variables de ámbito léxico, que hizo más fácil escribir código robusto (junto con el ***pragma strict***). Una característica principal introducida en Perl 5 fue la habilidad de empaquetar código reutilizable como módulos. Larry Wall indicó más adelante que "la intención del sistema de módulos de Perl 5 era apoyar el crecimiento de la cultura Perl en vez del núcleo de Perl".3

2.4. Primera Generación (web 1.0 CGI).

Common Gateway Interface (CGI) fue la tecnología reinante desde aproximadamente 1993 hasta fines de los '90 cuando los lenguajes de scripting comenzaron a ganar importancia. CGI trabaja encapsulando la información provista por el usuario en variables de ambiente. Estas luego son accedidas por scripts o programas desarrollados comúnmente en Perl o C. Estos programas procesan la información provista por los usuarios, y luego envían código HTML con la información procesada a la salida estándar, que a su vez es capturada por el servidor Web y pasada al usuario.

2.4.1. Evolución de Aplicaciones web.

En un principio la web era sencillamente una colección de páginas estáticas, documentos, etc., para su consulta o descarga, con el paso del tiempo su evolución fue la inclusión de un método para elaborar páginas dinámicas que permitieran que lo mostrado tuviese carácter dinámico (es decir, generado a partir de los datos de la petición). Este método fue conocido como CGI ("***Common Gateway Interface***") y definía un mecanismo mediante el que se podía pasar información entre el servidor y ciertos programas externos. Los ***CGIs*** siguen utilizándose ampliamente; la mayoría de los servidores web permiten su uso

debido a su sencillez. Estas a su vez evolucionaron en ***Rich Internet Applications o RIAs*** por sus siglas en inglés) son aplicaciones de ***software*** que se ejecutan a través de un navegador web. Las Aplicaciones Web permiten que el usuario acceda a los datos de forma interactiva, por lo que ofrecen una experiencia cautivante y sofisticada que incrementa la satisfacción del usuario y la productividad en las empresas.

Beneficios de las aplicaciones web

- No necesitan instalación (solo es necesario mantener actualizado el navegador web).
- Las actualizaciones hacia nuevas versiones son automáticas.
- Se pueden utilizar desde cualquier ordenador con una conexión a Internet sin depender del sistema operativo que este utilice.
- Generalmente es menos probable la infección por virus, que utilizando por ejemplo programas ejecutables.
- Más capacidad de respuesta, ya que el usuario interactúa directamente con el servidor, sin necesidad de recargar la página.
- Ofrecen aplicaciones interactivas que no se pueden obtener utilizando solo HTML, incluyendo arrastrar y pegar, cálculos en el lado del cliente sin la necesidad de enviar la información al servidor.
- Evita la problemática del uso de diferentes navegadores al abstraerse de ellos a través de un ***framework***.

2.5. Plataformas de Desarrollo Web

Son un conjunto de herramientas como: servidor de aplicaciones web, lenguaje de programación de ambiente web, bases de datos de acceso para la aplicación web, en algunos casos el OS donde se ejecuten los servicios, integradas dentro de un paquete, el cual ya dispone de los servicio necesarios para crear aplicaciones web y que esta previamente configurados para que pueda ser ejecutado en cualquier maquina/servidor. Algunos de las plataformas de desarrollo web que podemos encontrar en la Internet (*Figura 2.1).*

Figura 2.1 Plataformas para Desarrollo Web

2.5.1-Frameworks

Framework es un concepto sumamente genérico, se refiere a "ambiente de trabajo, y ejecución", por ejemplo "***.Net***" es considerado un "***framework***" para desarrollar aplicaciones (Aplicaciones sobre Windows). En general los ***framework*** son soluciones completas que contemplan herramientas de apoyo a la construcción (ambiente de trabajo o desarrollo) y motores de ejecución (ambiente de ejecución).

Siguiendo con el ejemplo: "***.Net***" ofrece el "Visual Studio .net" (ambiente construcción o desarrollo) que le permite a los desarrolladores construir aplicaciones, y su motor es el "***.Net framework***" que permite ejecutar dichas aplicaciones. El motor de ".net" es un anexo al sistema operativo (un componente que se instala sobre el sistema operativo), y que ahora viene incluido en la mayoría de los sistemas operativos de Microsoft.

Framework puede ser algo tan grande como "***.NET***" o Java (también es un ***framework***), pero también el concepto se aplica a ámbitos más específicos, por ejemplo; dentro de Java en el ámbito especifico de aplicaciones Web tenemos los f***ramework: Struts, "Java Server Faces",*** o ***Spring.*** Estos ***frameworks*** de Java en la práctica son conjuntos de librerías (API's) para desarrollar aplicaciones Web, más librerías para su ejecución (o motor), y más un conjunto de herramientas para facilitar esta tarea (***debuggers***, ambientes de desarrollo como Eclipse, etc.).

Otros ejemplos de ***frameworks*** para ámbitos específicos:

- Ámbito: ***Webservices*** => ***Framework***: ***Axis***.
- Ámbito: Interfaz de Usuario Web Dinámica => ***Framework: Ajax*** – DWR

- Ámbito: Procesos de Negocio => BPMS (***WebSphere***, ***AquaLogic***, o Oracle)

2.6. Web 2.0

El término Web 2.0 está asociado a aplicaciones web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario1 y la colaboración en la ***World Wide Web.*** Un sitio Web 2.0 permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual, a diferencia de sitios web donde los usuarios se limitan a la observación pasiva de los contenidos que se ha creado para ellos. Ejemplos de la Web 2.0 son las comunidades web, los servicios web, las aplicaciones Web, los servicios de red social, los servicios de alojamiento de videos, las ***wikis, blogs, mashups y folcsonomías***.

2.6.1. Ventajas

- No se necesita configuración especial ni cambios en las computadoras de los usuarios.
- Bajos costos.
- Información centralizada, segura y fácil realización de backups.
- Las actualizaciones pueden ser realizadas fácil y rápidamente.
- La información es accesible para una gran audiencia en cualquier lugar del mundo.
- Información accesible las 24 horas los 7 días de la semana.
- Todo el mundo posee un navegador. Las interfaces familiares promueven el uso.
- Los usuarios pueden aprender manejando sus tiempos en la ubicación deseada.
- Compatibilidad multiplaforma.
- Menores requerimientos de memoria. Al residir y ser ejecutadas en los servidores, las aplicaciones Web tienen demandas de memoria muchas veces menores a las aplicaciones convencionales

2.6.2. Desventajas

- Interfaces de usuario no del todo sofisticadas.
- El desarrollo demanda más tiempo debido a la complejidad inherente.
- Riesgos de seguridad.

2.7. Vulnerabilidades

Es muy común encontrar vulnerabilidades Web ya que los programadores (o más bien el mercado) sigue priorizando la funcionalidad y usabilidad de la aplicación por encima de la seguridad y, normalmente, al desarrollar dichas aplicaciones web, no se tienen en cuenta las metodologías de programación segura para los diferentes lenguajes de programación utilizados, tampoco se revisa el código fuente antes de su paso a producción, etc.

2.7.1. Definiciones

Una vulnerabilidad es un agujero o una debilidad en la aplicación, que puede ser un defecto de diseño o un error que permite a un atacante causar daño a las partes de una aplicación. Las partes interesadas incluyen el propietario de la aplicación, los usuarios, y otras entidades que dependen de la aplicación. El término "vulnerabilidad" se utiliza a menudo de manera muy informal. Sin embargo, aquí tenemos que distinguir las amenazas, ataques y las contramedidas

Ejemplos de vulnerabilidades: La falta de validación de entrada de datos del usuario, la falta de un mecanismo de extracción suficiente, falla a abrir el control de errores, no cerrar la conexión de base de datos correctamente, para una gran visión de conjunto, echa un vistazo a la OWASP Top Ten del proyecto. Usted puede leer acerca de las vulnerabilidades principales y descargar un documento que se tratarán en detalle. Muchas organizaciones y agencias usan en el Top Ten, como una forma de crear conciencia sobre la seguridad de las aplicaciones

2.7.2. Vulnerabilidades en aplicaciones web de EC-Council

A continuación se muestra las vulnerabilidades más comunes en los sitios web basada en la metodología de EC-COUNCIL.

A1 Inyección

Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.

A2 Secuencia de Comandos en Sitios Cruzados (XSS)

Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador ***webs in*** una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la victima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

A3 Pérdida de Autenticación y Gestión de Sesiones

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, llaves, ***token de sesiones***, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.

A4 Referencia Directa Insegura a Objetos

Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.

A5 -Falsificación de Peticiones en Sitios Cruzados (CSRF)

Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la victima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.

A6 -Defectuosa Configuración de Seguridad

Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto.

Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.

A7 Almacenamiento Criptográfico Inseguro.

Muchas aplicaciones web no protegen adecuadamente los datos sensibles, tales como tarjetas de crédito, ***NSSs***, y credenciales de autenticación con mecanismos de cifrado o ***hashing***. Atacantes pueden modificar o robar tales datos protegidos inadecuadamente para conducir robos de identidad, fraudes de tarjeta de crédito u otros crímenes.

A8 Falla de Restricción de Acceso a URL.

Muchas aplicaciones web verifican los privilegios de acceso a ***URLs*** antes de generar enlaces o botones protegidos. Sin embargo, las aplicaciones necesitan realizar controles similares cada vez que estas páginas son accedidas, o los atacantes podrán falsificar ***URLs*** para acceder a estas páginas igualmente.

A9 Protección Insuficiente en la Capa de Transporte.

Las aplicaciones frecuentemente fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible. Cuando esto ocurre, es debido a la utilización de algoritmos débiles, certificados expirados, inválidos, o sencillamente no utilizados correctamente.

A10 -Redirecciones y reenvíos no validados.

Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de ***phishing*** o ***malware***, o utilizar reenvíos para acceder páginas no autorizadas.

2.8. Metodologías para el Análisis de Seguridad.

Las aplicaciones son hoy en día uno de los activos principales de cualquier empresa. Tanto si dan servicio a usuarios finales (por ejemplo aplicaciones de ***ebanking*** o ***ecommerce***) como si se trata de aplicaciones corporativas (una intranet), las aplicaciones manejan información cuya confidencialidad, disponibilidad e integridad es fundamental para las empresas.

Las Auditorías de Seguridad sobre Aplicaciones se han vuelto imprescindibles para evaluar la seguridad de los desarrollos (propios o realizados por terceros). Estas auditorías o evaluaciones deben realizarse periódicamente y teniendo en cuenta tanto la parte interna (accesos desde la red corporativa) como la parte externa (accesos con origen Internet) de los aplicativos.

La estrategia y metodología de seguridad de aplicaciones Web está formada por numerosos componentes que se complementan entre sí. Este apartado detalla los aspectos fundamentales a considerar para el diseño, desarrollo, mantenimiento y evaluación de la seguridad en entornos Web (*Figura 2.2)*.

Los elementos de seguridad principales de un entorno o aplicación Web deben incluir:

- Formación en seguridad de aplicaciones Web.
- Arquitectura e infraestructura (sistemas y redes) segura.
- Metodología de seguridad de desarrollo de aplicaciones Web.
- Metodología de análisis de seguridad de aplicaciones Web.

La estrategia y metodología de seguridad debe incluir adicionalmente los siguientes componentes:

- Formación en seguridad.
- Instalación y configuración segura de sistemas y redes (arquitectura).

Actualizaciones:

- Servidor Web y de aplicación.
- ***Framework***.
- Desarrollo de ***software*** seguro.

- Gestión de versiones y actualizaciones.
- ***Web Application Firewalls (WAF).***

Auditorías de seguridad.

- Caja negra: pruebas de intrusión y ***Web Application Security Scanners (WASS).***
- Caja blanca: revisión de código manual y automático.

La formación de seguridad debe centrarse en proporcionar un conocimiento adecuado a administradores y desarrolladores respecto a las vulnerabilidades y amenazas de seguridad en entornos Web, los diferentes tipos de ataques existentes y los mecanismos de defensa asociados, preferiblemente mediante ejemplos prácticos. El objetivo es disponer del conocimiento para construir una infraestructura y aplicación

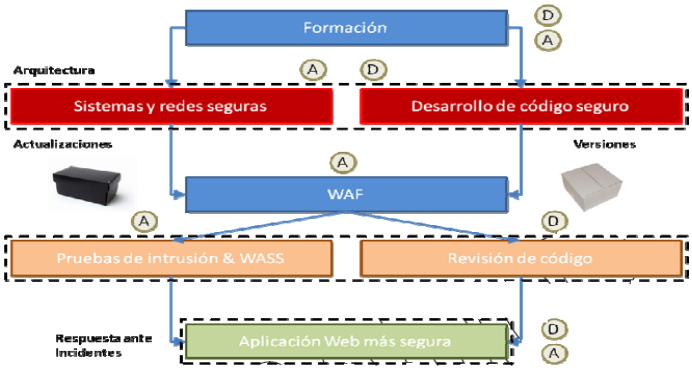


Figura2.2. Estrategia y Metodología de Seguridad de Apps WEB

2.8.1. OSSTMM (Manual de Metodología Abierta de Evaluación de Seguridad) de ISECOM (Information Security and Open Methodologies)

Es un conjunto de reglas y lineamientos para cuándo, qué y cuáles eventos son testeados. Esta metodología cubre únicamente el testeo de seguridad externo, es decir, testear la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado. Está también dentro del alcance de este documento proveer un método estandarizado para realizar un exhaustivo test de seguridad de cada sección con presencia de seguridad (por ejemplo, seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad

de las tecnologías de Internet, y seguridad de procesos) de una organización. Dentro de este método abierto y evaluado por expertos, para realizar exhaustivos testeos de seguridad, alcanzamos un estándar internacional en testeos de seguridad, que representa una línea de referencia para todas las metodologías de testeo de seguridad tanto conocidas como inexploradas.

La limitación al alcance del testeo de seguridad externo está dada por las diferencias considerables entre testeo externo a interno y testeo interno a interno. Estas diferencias radican fundamentalmente en los privilegios de acceso, los objetivos, y los resultados asociados con el testeo interno a interno.

El tipo de testeo que busca descubrir las vulnerabilidades inexploradas no está dentro del alcance de este documento ni dentro del alcance de un test de seguridad OSSTMM. El test de seguridad descrito a continuación es un test práctico y eficiente de vulnerabilidades conocidas, filtraciones de información, infracciones de la ley, estándares de la industria y prácticas recomendadas.

ISECOM exige que un test de seguridad solamente sea considerado un test OSSTMM si es:

- Cuantificable.
- Consistente y que se pueda repetir.
- Válido más allá del período de tiempo "actual".
- Basado en el mérito del testador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con leyes individuales y locales y el derecho humano a la privacidad.

ISECOM no asevera que el uso del OSSTMM (*Figura 2.3)* constituya una protección legal en todos los tribunales de justicia, sin embargo, cumple el papel del más alto nivel de profesionalismo en cuanto a testeos de seguridad cuando los resultados obtenidos son aplicados al perfeccionamiento de la seguridad dentro de un espacio de tiempo razonable.

ISECOM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet:

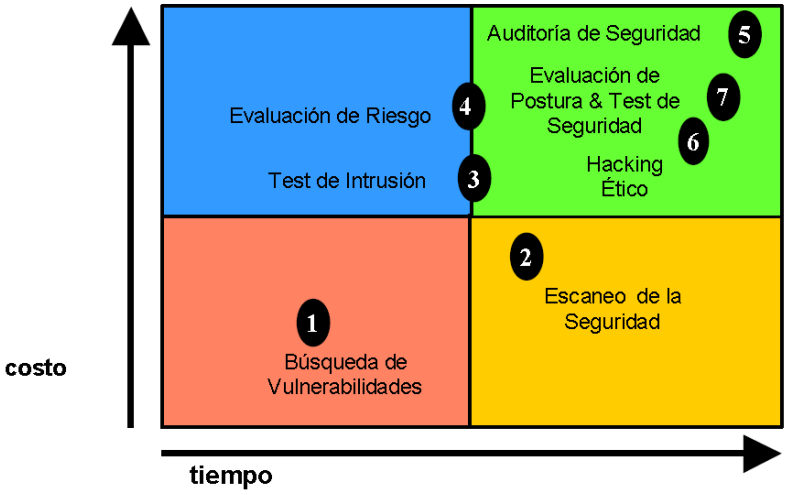


Figura 2.3. Definición de Ámbitos de ISECOM.

Búsqueda de Vulnerabilidades: se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

Escaneo de la Seguridad: se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.

Test de Intrusión: se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.

Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

Auditoría de Seguridad: hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

Hacking Ético: se refiere generalmente a los testes de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

Test de Seguridad y su equivalente militar, Evaluación de Postura, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

2.8.2. OWASP (Proyecto de Seguridad Abierta de Aplicaciones Web).

Una de las metodologías con más reconocimiento internacional a la hora de realizar auditorías de seguridad sobre aplicaciones es la ***OWASP Testing Guide*** que alcanza ya su tercera versión. La ***OWASP (Open Web Application Security Project***) lanzó este proyecto con el objetivo de crear un marco que incluyera las mejores prácticas en el desarrollo de ***tests*** de intrusión en aplicaciones. La última versión v3 (*Figura 2.4)* de la ***Testing*** Guide fue publicada en Diciembre de 2008 y está previsto que se la v4 de la guía se publicada en Enero de 2011

En cuanto a los riesgos de seguridad en aplicaciones, tenemos lo siguiente Los atacantes pueden potencialmente usar muchas diferentes rutas a través de su aplicación para causar daño en su negocio u organización. Cada una de estas rutas representa un riesgo que puede, o no, ser lo suficientemente serio como para merecer atención.

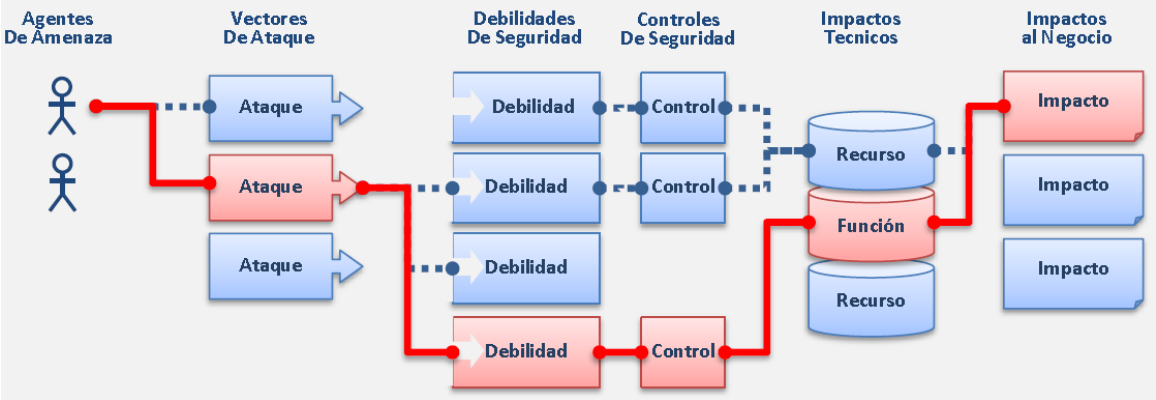


Figura 2.4. Riesgos de Seguridad en Aplicaciones desde el Punto de Vista OWASP

2.8.3. ISSAF (Information Security System Assessment Framework) de OISSG (Open Information System Security Group).

Constituye un ***framework*** detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad. La información contenida dentro de ***ISSAF***, se encuentra organizada alrededor de lo que se ha dado en llamar "Criterios de Evaluación", cada uno de los cuales ha sido escrito y/o revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes elementos:

- Una descripción del criterio de evaluación
- Puntos y Objetivos a cubrir
- Los pre-requisitos para conducir la evaluación
- El proceso mismo de evaluación
- El informe de los resultados esperados
- Las contramedidas y recomendaciones
- Referencias y Documentación Externa.

Por su parte y a fin de establecer un orden preciso y predecible, dichos "Criterios de Evaluación", se encuentran contenidos dentro de diferentes dominios entre los que es posible encontrar, desde los aspectos más generales, como ser los conceptos básicos de la "Administración de Proyectos de Testeo de Seguridad", hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL (SQL Injection) o como las "Estrategias del Cracking de Contraseñas.

A diferencia de lo que sucede con metodologías "más generales", si el framework no se mantiene actualizado, muchas de sus partes pueden volverse obsoletas rápidamente (específicamente aquellas que involucran técnicas directas de testeo sobre determinado producto o tecnología). Sin embargo esto no debería ser visto como una desventaja, sino como un punto a tener en cuenta a la hora de su utilización.

2.9. Herramientas para el Análisis de Seguridad

2.9.1. Nmap

Herramienta de exploración de redes y de sondeo de seguridad / puertos

Descripción

Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. ***Nmap*** utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza ***Nmap*** en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

La salida de ***Nmap*** es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede ser ***open*** (abierto), ***filtered*** (filtrado), ***closed*** (cerrado), o ***unfiltered*** (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que ***Nmap*** no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de ***Nmap***, pero para los que **Nmap** no puede determinar si se encuentran abiertos o cerrados. ***Nmap*** informa de las combinaciones de estado ***open|filtered*** y ***closed|filtered*** cuando no puede determinar en cuál de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. ***Nmap*** ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).

2.9.2. OpenVAS

El Sistema de Evaluación de la Vulnerabilidad (***Open OpenVAS***) es un marco de diversos servicios y herramientas que ofrecen un escaneo de vulnerabilidades completa y potente solución de gestión y la vulnerabilidad. El escáner de seguridad real se acompaña con una alimentación diaria actualizada de las

pruebas de vulnerabilidad de la red (NVTs), más de 25.000 personas en total (a partir de mayo de 2012).

Todos los productos openvas son ***Software*** Libre. La mayoría de los componentes están licenciados bajo la Licencia Pública General GNU (GNU GPL).

2.9.3. Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en ***nessusd***, el ***daemon Nessus***, que realiza el escaneo en el sistema objetivo, y ***nessus***, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola ***nessus*** puede ser programado para hacer escaneos programados con cron. En operación normal, ***nessus*** comienza escaneando los puertos con ***nmap*** o con su propio ***escaneador*** de puertos para buscar puertos abiertos y después intentar varios ***exploits*** para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de ***plugins***, son escritos en ***NASL (Nessus Attack Scripting Language,*** Lenguaje de ***Scripting*** de Ataque ***Nessus*** por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes. Opcionalmente, los resultados del escaneo pueden ser exportados en reportes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades. Algunas de las pruebas de vulnerabilidades de ***Nessus*** pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "***unsafe test***" (pruebas no seguras) antes de escanear.

2.9.4. Acunetix

Acunetix es una empresa de seguridad que se desarrolla un escáner de vulnerabilidades web que permite a las empresas para detectar posibles problemas de seguridad en sus aplicaciones web. La compañía fue fundada en 2004 y su producto ha estado en el mercado desde principios de 2005. Los Ingenieros de ***Acunetix*** mantienen un blog de seguridad que publica regularmente artículos sobre seguridad en aplicaciones web. Uno de esos artículos que tienen más relevancia son de las contraseñas en los servicios más populares de correo electrónico basados en web y se hace referencia en las principales publicaciones como:

CAPÍTULO III

Metodologías y Métricas Sobre Servicios Web

3.1. EC-COUNCIL

Uno de los grandes retos que tienen a menudo los técnicos de sistemas y redes de computadoras es que no cuentan con una forma estable para cuantificar la seguridad, únicamente se limitan a su cualificación, lo que les impide medir con exactitud, o llevar una estadística de variación del nivel de seguridad frente a cambios de configuración, escalabilidad, movilidad o cambios en las políticas de seguridad y en sí el aparecimiento de nuevas tecnologías que mal usadas pueden minimizar la seguridad.

La metodología utilizada se basa en una serie de etapas, donde se recolecta información, la cual es aprovechada después para realizar los ataques, terminando con la generación de recomendaciones más efectivas a fin de corregir las brechas encontradas.

La metodología, está basada en las siguientes etapas (*Figura* 3.1):

Exploración: en esta fase, se hace uso de información del dominio público, disponible en Internet para identificar vulnerabilidades e información de los sistemas operativos de los servidores y los servicios existentes.

Enumeración: habiendo obtenido una cantidad de información razonable, se procede a enumerar los hosts y servicios en la red interna, mediante herramientas de escaneo de puertos y vulnerabilidades.

Evaluación: teniendo la lista de los servicios activos, se procede a revisar dichos servicios por su naturaleza, versión de ***software*** y sistema operativo, en base a vulnerabilidades documentadas.

Pen-Test*:** las aplicaciones también son revisadas, se realizan pruebas como ***SQL-injections, pruebas de ***buffer overflows (BOF)***, ***cross-site scripting***, entre otras, a fin de evaluar el nivel de seguridad y si es posible obtener información de las bases de datos internas.

Corrección: Recomendar los controles técnicos necesarios para cerrar las vulnerabilidades encontradas para evitar su materialización.

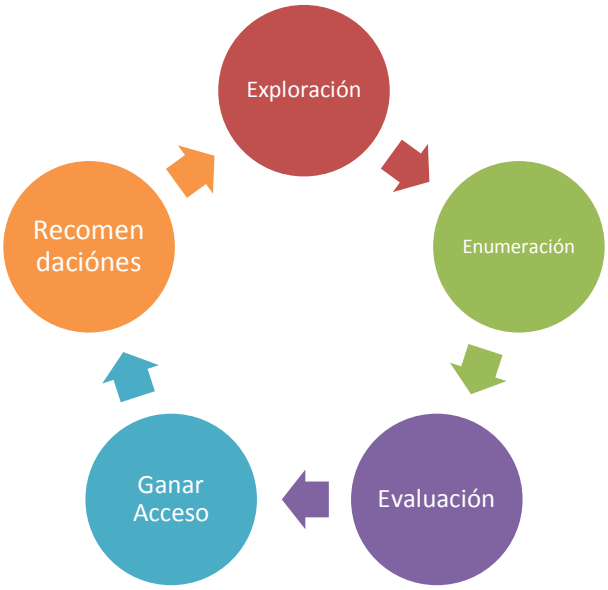


Figura 3.1. Flujo de Metodología EC- COUNCIL

3.1.1 Certificaciones Profesionales de EC-Council.

Certified Ethical Hacker (CEH)

En este curso, los estudiantes se sumergirán en un entorno interactivo en el que aprenderán como escanear, probar, ***hackear*** y asegurar sus propios sistemas. Las intensas prácticas de laboratorio brindan a cada uno el conocimiento profundo y experiencia práctica con los sistemas de seguridad actuales. Los estudiantes entenderán como trabajan las defensas perimetrales, exploración y ataques a las redes propias, sin dañar una red real. Asimismo, aprenderán como los intrusos escalan privilegios y que medidas deben ejecutar para proteger sus sistemas. La detección de intrusos es parte esencial del curso, creación de políticas, ingeniería social, ataques ***DDos***, desbordamientos de buffer y creación de virus, tendrán laboratorios interactivos y experiencia en ***hackeo*** ético.

Computer Hacking Forensic Investigator (CHFI)

El curso, proveerá al participante de las habilidades necesarias para identificar, extraer y recabar evidencias de ataques perpetuados por intrusos para ejercer acción legal hacia quien resulte responsable. Las herramientas más importantes del análisis forense serán utilizadas en este curso, incluyendo ***software***, hardware y técnicas especializadas. La necesidad de los negocios de ser más eficientes e

integrados entre sí, así como los usuarios finales han dado como resultado un nuevo tipo de criminal: ***"El ciber-criminal***". Actualmente la cuestión no es si la información de la empresa será atacada (***hackeada***). Hoy en día, la batalla entre corporaciones, gobiernos y países no son llevadas a cabo solo en típicas salas de juntas o campos de batalla utilizando la fuerza física, sino empiezan en un ámbito técnico que vincula a la gran mayoría de las etapas en la vida moderna. Al final los estudiantes van a ser capaz de identificar, rastrear y perseguir intrusos, ***hackers o ciber criminals.***

Certified Security Analyst (ECSA) / Licensed Penetration Tester (LPT)

ECSA / LPT es un curso de seguridad como ningún otro. Mediante experiencias del mundo real es el único que cubre a profundidad el ***hackeo*** avanzado y pruebas de penetración que abarcan todo tipo de infraestructuras de redes, sistemas operativos y ambientes de aplicación. El programa es altamente interactivo y diseñado para enseñar a profesionales en seguridad, los avanzados usos de la metodología de ***Licensed Penetration Tester***, herramientas y técnicas requeridas para llevar a cabo pruebas de seguridad en sus propios sistemas y redes. Los estudiantes aprenderán como diseñar, asegurar y probar redes para proteger su información contra amenazas que plantean los hackers y crackers; por medio de la enseñanza de herramientas y técnicas innovadoras para realizar pruebas de seguridad y penetración, el curso le ayudara a hacer una evaluación intensiva necesaria para identificar con eficiencia y reducir los riesgos de seguridad de su infraestructura. Los estudiantes aprenderán a detectar problemas de seguridad a fin de evitarlos y eliminarlos, ya que el curso incluye una cobertura de temas de análisis y pruebas de seguridad completa.

3.2 Métricas: Common Vulnerability Scoring System (CVSS)

La capacidad de valorar las vulnerabilidades de los sistemas es de extrema importancia para los trabajos de análisis de vulnerabilidades. El CVSS es un estándar de la industria en la homologación de los criterios para asignar valor a las vulnerabilidades. El sistema tiene 3 grupos de métricas, cada una dependiente de la anterior:

Métrica Base: Representa la severidad. Una vez descubiertas, analizadas y catalogadas, asumiendo que la información inicial es correcta, hay ciertos aspectos de las vulnerabilidades que no cambian. Estas características centrales no cambian con el tiempo, y tampoco cambian en los diferentes ambientes; para todos los efectos, una vez fijadas, son inmutables. El grupo de métricas base captura estas cualidades constantes, las que son el acceso y el impacto.

Métrica Temporal: Representa la urgencia. Durante el ciclo de vida de una vulnerabilidad, pueden ocurrir ciertos acontecimientos que afectan la urgencia de la amenaza planteada por la vulnerabilidad. Los tres factores que el CVSS procura capturar son: la confirmación de la vulnerabilidad, o de sus detalles técnicos, el estado de remediación de la vulnerabilidad y la disponibilidad del código o técnicas para explotarla. Cada uno de estos factores dinámicos es importante en el ajuste de la urgencia (es decir la prioridad) de una vulnerabilidad en un cierto plazo.

Métrica ambiental: Usada para priorizar respuestas. Diversos ambientes pueden impactar inmensamente en el riesgo que una vulnerabilidad plantea a una organización y a sus accionistas. El grupo de métricas ambientales del CVSS, captura características de las vulnerabilidades que se atan a la puesta en práctica y al ambiente.

3.2.1 Unión del CVSS dentro de la gestión del riesgo.

CVSS incluye dentro de sus Ecuaciones una destinada a recoger determinados aspectos que son dependientes de la organización en la que se presenta la vulnerabilidad. Estos aspectos se encuentran recogidos dentro del conjunto de métricas de entorno por las métricas denominadas:

- Requisito de Confidencialidad
- Requisito de Integridad
- Requisito de Disponibilidad

La cuestión que se plantea ante los requisitos de las métricas de entorno es referente a donde se obtienen esos valores, lo cual se contesta del análisis de riesgos de la organización. En ISO 27001, el punto 4.2.1.d recoge las actividades a realizar para la Identificación de Riesgos que se compone de:
Identificar los activos que están dentro del ámbito de aplicación del SGSI y a los propietarios de estos activos.
Identificar las amenazas a que están expuestos esos activos
Identificar las vulnerabilidades bajo las que podrían actuar dichas amenazas

CAPÍTULO IV

Aplicación de Auditoría al Servicio Web SISER AIyPF

4.1. Antecedentes.

En el área de Aseguramiento de Ingresos y Prevención de Fraudes (AIyPF) de Grupo Iusacell cuenta con una aplicación web de uso interno denominada Sistema Integral de Servicios de AIyPF (SISER AIyPF) donde se realiza la validación, facturación y objeciones para información de grupos terceros.

Debido a esto, se requiere que este portal sea seguro y confiable y garantice la seguridad de la información ya que la pérdida de esta puede generar riesgos económicos y de fraudes.

El sistema al no contar con una certificación de TI puede considerarse inseguro ya que no se ha validado el proceso del flujo de la información, ya que se realizo ateniendo a un requerimiento de prioridad alta y por su necesidad inmediata de desarrollo, no cuenta con ningún control de calidad. Como principales medidas de seguridad el acceso al sistema está restringido por IP y solo el usuario final puede tener conexión desde su PC pasando por un acceso validando usuario y contraseña.

Cuidando la confidencialidad e integridad de los datos que pudiesen ser sensibles dentro del sistema, se desarrolla una carta de autorización donde se detallan los aplicativos, alcance, equipo de trabajo y fechas en las cuales se realizaran las actividades anteriormente descritas en la propuesta. Esta carta de autorización también deslinda de cualquier responsabilidad a los consultores que realicen dichas pruebas. Es de suma importancia que esta carta este en posesión de ambas partes. (Para mayor información dirigirse al ***anexo [1] Carta de autorización***)

A fin de realizar la auditoria al aplicativo SISER, se genera primeramente un documento denominado propuesta, donde se hace de conocimiento a ambas partes (auditor y auditado), el entorno en el cual se encuentra actualmente dicho sistema, al igual que la justificación de las actividades a realizar. De igual forma se describen los servicios propuestos y un plan de implementación delimitando los alcances y las limitantes que pudiesen surgir durante la auditoria. El auditado por su parte tiene una línea de aceptación donde se denotan los entregables, así como los criterios de aceptación.

Esta propuesta además de incluir cuestiones técnicas y ejecutivas contiene una propuesta económica donde se desglosan los gastos de dicho estudio. (Para mayor información dirigirse al ***anexo [2] Propuesta***)

4.2. Alcance de la Auditoría.

La intención de realizar el análisis de vulnerabilidades al sistema web SISER es evidenciar las áreas de mejora en cuanto a la seguridad del Aplicativo. Esta auditoría va a aportar las presuntas vulnerabilidades que se pueden mitigar para que el servicio no quede sin disponibilidad, siendo critico para esta área.

De acuerdo a lo anterior se considera que las vulnerabilidades a explotar son en aplicaciones web guía de OWASP y desarrollo seguro (buenas prácticas). Todo lo anterior se deberá de analizar en el servidor que para mayor información dirigirse al ***anexo [3] Prerrequisitos Diagnostico y Alcance***, así mismo se muestra en la siguiente tabla:

Dominio	IP Servidor	Descripción de Servidor
http://172.19.235.122:8084/SISER	172.19.235.122	Denominada Sistema Integral de Servicios de AIyPF (SISER AIyPF) donde se realiza la validación, facturación y objeciones para información de grupos terceros.
Cabe mencionar que el área auditada solo nos da acceso al servidor web y no al servidor de base de datos, por lo que en este momento sólo nos atañe el análisis de vulnerabilidades a las aplicaciones web.		

Tabla 4.1 Alcance de la Auditoría

4.3. Plan de la Auditoría.

Se define y se acuerdan las fechas para iniciar con las pruebas del análisis de vulnerabilidades, esto también nos da fechas para control de accesos al área auditada. (Para mayor información dirigirse al ***anexo [4] Ficha de Pruebas***). Este documento describe las actividades realizadas así como el personal el cual realizo dichas actividades, todo perfectamente delimitado por fechas, al crearse una ficha de pruebas se puede tener el control de las veces que se ha realizado una actividad (prueba) sobre un aplicativo sistema o dispositivo.

Aunado al alcance y a la propuesta anterior se genera un plan de trabajo el cual se medirá en días, es importante hacer notar que debido a actividades propias de los miembros de del equipo del seminario y ajenas a dicha auditoria, solo se consideran 3 horas para día laborable de lunes a viernes, el plan se realizará en 9 días aproximadamente.

Nuestro plan de auditoría está dividido en 4 fases: Inicio de proyecto, Escaneo de Vulnerabilidades y pentest, documentación del respaldo de la valoración, Finalización del proyecto, mismas que serán explicadas a continuación.

PLANEACIÓN

FASE 1. Inicio de Proyecto: aproximadamente **1 día.**

Definición en tiempo y forma del análisis de vulnerabilidades.
Reunión con cliente, para definir la metodología a aplicar y las fechas del análisis.
Tenemos un *Hito: Fechas compromiso.*

DESARROLLO - EJECUCIÓN

FASE 2. Escaneo de Vulnerabilidades y Pentest: aproximadamente **5 días.**

Asignación de equipo de trabajo para supervisión de tareas.	1 día.
Definición de cita para visitar instalaciones.	
Tenemos un *Hito: Acceso al sistema*.	
Se realiza el Testing de acuerdo a la guía de OWASP	1 día.
Pruebas manuales, validación de instalaciones.	1 día.
Documentación de información sobre hallazgos	1 día.
Tenemos un *Hito: Se indica al proveedor que terminan pruebas*	1 día.

RESULTADOS

FASE 3. Documentación de Respaldo del Análisis **2 días**

Recopilación de la información y elaboración de reporte	1 día.
Confronta de resultados	1 día.

Tenemos un *Hito: se le entrega reporte al cliente y se revisan observaciones*.

CIERRE

FASE 4. Finalización del proyecto. **1 día.**

Reunión con el cliente para aclaración de informe 1día.
Tenemos un *Hito: Entrega del reporte final y firma de aceptación por parte del cliente*

Para mayor información dirigirse al ***anexo [5] Plan de Auditoría.***

4.4. Checklist.

Para el desarrollo de este análisis se sigue la metodología de OWASP que sigue un control estricto de vulnerabilidades, delimitadas por pruebas, que se engloban dentro de un checklist, este a su vez da un panorama de los pasos que ha seguido el proceso de la auditoria del aplicativo; dentro se describen las vulnerabilidades y conclusiones del auditor. La guía de OWASP está compuesta por 10 categorías de vulnerabilidades, de acuerdo a nuestro alcance, algunos no pudieron ser aplicados para nuestro análisis, por lo que en esta parte del documento sólo se mencionaran los que arrojaron una observación.

Categoría	Número de Ref.	Nombre de Prueba	Vul
Recopilación de Información	OWASP-IG-001	Spiders, Robots y Crawlers	
	OWASP-IG-002	Descubrimiento/Reconocimiento mediante motores de búsqueda	
	OWASP-IG-003	Identificación de puntos de entrada de la aplicación	
	OWASP-IG-004	Pruebas de firma digital de Aplicaciones Web	
	OWASP-IG-005	Descubrimiento de Aplicaciones	
	OWASP-IG-006	Análisis de Códigos de Errores	
Pruebas de Gestión de Configuración	OWASP-CM-001	Pruebas SSL/TLS (SSL versión, Algoritmos, longitud de Claves, Validez de Certificado Digital)	
	OWASP-CM-002	Prueba de DB Listener	
	OWASP-CM-003	Prueba de Gestión de Configuración de Infraestructura	
	OWASP-CM-004	Prueba de Gestión de Configuración de Aplicación	
	OWASP-CM-005	Prueba del Gestor de Extensión de Ficheros	
	OWASP-CM-006	Antiguo, backup y ficheros no referenciados	
	OWASP-CM-007	Interface de Administración de Aplicación e Infraestructura	
	OWASP-CM-008	Prueba de métodos HTTP y XST	
Pruebas de Autenticación	OWASP-AT-001	Transporte de Credenciales sobre canal cifrado	
	OWASP-AT-002	Prueba para Enumeración de usuarios	
	OWASP-AT-003	Prueba de detección de Cuentas de Usuario Adivinables (Diccionario)	
	OWASP-AT-004	Prueba de Fuerza Bruta	
	OWASP-AT-005	Prueba para evitar el esquemas de autenticación	
	OWASP-AT-006	Prueba de recordatorio de contraseña y restablecimiento	
	OWASP-AT-007	Prueba de Cierre de Sesión y Gestión de Cache de Navegación	
	OWASP-AT-008	Prueba de CAPTCHA	
	OWASP-AT-009	Prueba de Autenticación de Múltiple Factores	
	OWASP-AT-010	Prueba de Condiciones de Carrera	
Gestión de Sesiones	OWASP-SM-001	Prueba del Esquema de Gestión de Sesión	
	OWASP-SM-002	Prueba de atributos de Cookies	
	OWASP-SM-003	Prueba de Fijación de Sesión	
	OWASP-SM-004	Prueba de Variables de Sesión Expuestas	
	OWASP-SM-005	Prueba de CSRF	
Pruebas de Autorización	OWASP-AZ-001	Prueba de Ruta Transversal	
	OWASP-AZ-002	Prueba para Evitar Esquema de Autorización	
	OWASP-AZ-003	Prueba de escalada de Privilegios	
Pruebas de Lógica de Negocio	OWASP-BL-001	Prueba de Lógica de Negocio	
Pruebas de Validación de Datos	OWASP-DV-001	Prueba de XSS Reflejado	
	OWASP-DV-002	Prueba de XSS Almacenado	

	OWASP-DV-003	Prueba de XSS basado en DOM	
	OWASP-DV-004	Prueba de XSS basado en Flash	
	OWASP-DV-005	Inyección SQL	
	OWASP-DV-006	Inyección LDAP	
	OWASP-DV-007	Inyección ORM	
	OWASP-DV-008	Inyección XML	
	OWASP-DV-009	Inyección SSI	
	OWASP-DV-010	Inyección Xpath	
	OWASP-DV-011	Inyección IMAP/SMTP	
	OWASP-DV-012	Inyección de Código	
	OWASP-DV-013	Inyección de Ordenes del Sistema Operativo	
	OWASP-DV-014	Desbordamiento de *buffer*	
	OWASP-DV-015	Prueba de Vulnerabilidad incubada	
	OWASP-DV-016	Prueba de HTTP *Splitting/Smuggling*	
Pruebas de Denegación de Servicio	OWASP-DS-001	Prueba de Ataques a través de Comodines SQL	
	OWASP-DS-002	Bloqueo de Cuentas de Usuarios	
	OWASP-DS-003	Pruebas de DoS mediante Desbordamiento de *Buffer*	
	OWASP-DS-004	Asignación de Objeto de Usuario Especificado	
	OWASP-DS-005	Entrada de usuario como un contador de bucle	
	OWASP-DS-006	Prueba de Escritura en Disco de data provista por Usuario	
	OWASP-DS-007	Fallo en Liberar Recursos	
	OWASP-DS-008	Almacenamiento de demasiados datos en Sesión	
Pruebas de Servicios Web	OWASP-WS-001	Recopilación de Información de WS	
	OWASP-WS-002	Prueba de WSDL	
	OWASP-WS-003	Prueba en la Estructura del XML	
	OWASP-WS-004	Prueba del XML a nivel de contenido	
	OWASP-WS-005	Prueba de REST/parámetros HTTP GET	
	OWASP-WS-006	Adjuntos SOAP maliciosos	
	OWASP-WS-007	Prueba de Repetición	
Pruebas Ajax	OWASP-AJ-001	Vulnerabilidades Ajax	
	OWASP-AJ-002	Pruebas Ajax	

Tabla 4.2 Checklist de OWASP

4.5. Desarrollo- Ejecución de Análisis de Vulnerabilidades

Siguiendo la metodología de EC-Council acompañada de las mejores prácticas descritas en OWASP se dispuso a realizar un análisis de vulnerabilidades a los aplicativos: **Dominio: 172.19.235.122:8084/SISER** de la siguiente forma:

Exploración: Haciendo uso de la herramienta Nmap 5.0 se procedió a la Identificación de equipos y puertos abiertos con esta información disponible se busca información de los sistemas operativos de los servidores y los servicios existentes, Identificando los puertos, se deducen los servicios que se alojan en ellos, de la siguiente forma:

blackice-alerts (8082/tcp)
general/tcp
netbios-ns (137/udp)
ajp13 (8009/tcp)
apex-mesh (912/tcp)
epmap (135/tcp)
general/SMBClient
homepage (8182/tcp)
https (443/tcp)
icslap (2869/tcp)
ideafarm-chat (902/tcp)
microsoft-ds (445/tcp)
netbios-ssn (139/tcp)
rtsp (554/tcp)
general/CPE-T
general/HOST-T
pop3proxy (50000/tcp)
ssh (22/tcp)

Enumeración: Se enumeran las aplicaciones las cuales corren en el servidor seleccionado la cual es la aplicación SISER, esta aplicación tiene un login de entrada el cual se está bajo la dirección del mismo.

Evaluación: A continuación se muestran las evidencias de las pruebas realizadas para el análisis de vulnerabilidades del aplicativo web SISER.

Dominio: 172.19.235.122:8084/SISER

Se intenta ganar el acceso al servidor mediante la ejecución de exploits acción en la cual no se logra el objetivo.

Para mayor información dirigirse al ***anexo [6] Evidencias de Auditoría.*** En dicho archivo se podrán ver las pantallas de evidencias del análisis de vulnerabilidades aplicado al portal web SISER.

Haciendo el cruce de los resultados obtenidos (*ver evidencias)* contra el Checklist de la guía de OWASP, se pudieron obtener las siguientes vulnerabilidades que se muestran en la tabla 4.4 Resultados de Checklist de OWASP donde es necesario aclarar que en esta parte del trabajo solo se muestra un resumen del mismo. Para mayor información dirigirse al ***anexo [7] Checklist owasp v2***).

Cruce de Checklist

Categoría	Nombre de Prueba	Observación
Recopilación de Información	Identificación de puntos de entrada de la aplicación	Se logró observar el login de la aplicación en la ruta /SISER
Pruebas de Gestión de Configuración	Antiguo, backup y ficheros no referenciados	No vulnerable
	Prueba de métodos HTTP y XST	No vulnerable
Pruebas de Autenticación	Transporte de Credenciales sobre canal cifrado	Al utilizar el protocolo HTTP, las credenciales de los usuarios viaja en claro, permite el robo de credenciales e información sensible. Implementar HTTPS , de forma que las conexiones estén cifradas
	Prueba de CAPTCHA	El sistema no cuenta con un sistema de capthca lo que permite realizar ataques de fuerza bruta.
Gestión de Sesiones	Prueba de Variables de Sesión Expuestas	El sistema es vulnerable con la información de sus variables
	Prueba de CSRF	El sistema es vulnerable a una petición repetida de código reflejado
Pruebas de Autorización	Todas	El sistema no es vulnerable
Pruebas de Lógica de Negocio	Todas	El sistema no es vulnerable
Pruebas de Validación de Datos	Prueba de XSS Reflejado	Referirse a la siguiente liga http://172.19.235.122:8085/SISER/faces/index.jsp;jsessionid=3D361392BD8B9B4669A77C2EBBB14BD3
	Prueba de XSS Almacenado	Referirse a la siguiente liga http://172.19.235.122:8085/SISER/faces/index.jsp;jsessionid=3D361392BD8B9B4669A77C2EBBB14BD3
	Desbordamiento de buffer	El componente Mongoose Webserver es vulnerable al desbordamiento de buffer a través de la variable 'Content-Length'
	Inyección de Código	Se prueba la inyección de código permite la recepción de caracteres especiales
	Prueba de HTTP Splitting/Smuggling	La información del sistemas no viaja por un protocolo seguro como HTTPS
Pruebas de Denegación de Servicio	Todas	Para el Sistema Ninguna Aplica
Pruebas de Servicios	Todas	El sistema no es vulnerable
Pruebas Ajax	Todas	El sistema no es vulnerable

Tabla 4.3 Resultados de Checklist de OWASP

4.6 Resultados del Análisis de Vulnerabilidades

A continuación se muestra una tabla con los resultados obtenidos del análisis de vulnerabilidades *ver tabla 4.4 Resultados del análisis de Vulnerabilidades*, donde se refleja el cálculo del riesgo de acuerdo a la vulnerabilidad detectada, también se describe el impacto de la misma y las recomendaciones para mitigar el riesgo.

Nivel	Vulnerabilidad	Descripción	Impacto	Recomendación
Alto **7.8**	Negación de servicio	La falla se debe a la forma Mangosta servidor web se encarga de solicitud con una variable grande 'Content-Length' aplicación que causa la caída del servidor.	Una explotación exitosa permitirá que los atacantes no autenticados remotos provocaran una negación de servicio.	No hay solución o parche está disponible el 29 de diciembre de 2010. Por lo que se recomienda dejar de publicar este servicio
Medio **5.0**	Cross-site scripting (XSS).	Consiste en embeber código HTML peligroso en variables que son almacenadas en la base de datos; incluyendo así etiquetas como <script> o <iframe>.	Modificación visual y funcional del componente vulnerable a través de la ejecución de scripts, permitiendo la modificación visual de la página que podría confundir/engañar al visitante del sitio.	Se recomienda filtrar las variables del componente afectado por medio de funciones a fin de que no se permita la inyección de código malicioso. Para mayor información consultar: https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_%28OWASP-DV-001%29#Countermeasures
Medio **5.0**	Cross-site scripting (XSS).	Se está ejecutando un servidor web que no desinfecta adecuadamente las cadenas de solicitud de código JavaScript malicioso. Al aprovechar este problema, un atacante podría ser capaz de causar HTML arbitrario y código script que se ejecutará en el navegador de un usuario dentro del contexto de seguridad del sitio afectado.	Modificación visual y funcional del componente vulnerable a través de la ejecución de scripts, permitiendo la modificación visual de la página que podría confundir/engañar al visitante del sitio	Se recomienda filtrar las variables del componente afectado por medio de funciones a fin de que no se permita la inyección de código malicioso. Para mayor información consultar: https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_%28OWASP-DV-001%29#Countermeasures
	Apache Tomcat Múltiple Vulnerabilities	De acuerdo con su número de versión auto-reporte, el Apache Tomcat escuchando en el host remoto es anterior a como tal, puede ser afectada por una o más de los siguientes vulnerabilidades: - El servicio remoto puede ser	Un remoto no autenticado, atacante podría aprovechar este problema para inyectar HTML arbitrario o código de script en el navegador de un usuario a se ejecutará en el contexto de seguridad de los	Actualizar a la versión más reciente del servidor Apache Tomcat. Para mayor información: http://tomcat.apache.org/

Nivel	Vulnerabilidad	Descripción	Impacto	Recomendación
6.8		vulnerable a un recorrido de directorio (CVE-2008-5515) - El servicio remoto puede ser vulnerable a una denegación de ataque del servicio si está configurado para utilizar la AJP de Java conector. (CVE-2009-0033) - El servicio remoto puede ser vulnerable a un nombre de usuario ataque de enumeración si se ha configurado para usar el formulario de autenticación junto con la "MemoryRealm ' 'DataSourceRealm', o 'jdbcRealm los reinos de autenticación. (CVE-2009-0580) - El servicio remoto puede ser afectada por una inyección de escritura la vulnerabilidad, si la aplicación de ejemplo de JSP, 'cal2.jsp', está instalado. (CVE-2009-0781)	afectados sitio	
Nota	El aplicativo cuenta con un inicio de sesión http , por lo que puede ser vulnerable a la intercepción de información sensible como son las credenciales de autenticación, por lo que se recomienda implementa un sistema seguro a través de https			

Tabla 4.4 Resultado del Análisis de Vulnerabilidades.

De acuerdo al desarrollo anterior se pudieron observar las siguientes vulnerabilidades:

Nivel de criticidad	Total de Vulnerabilidades encontradas
Alto	**1**
Medio	**3**
Bajo	**0**

Tabla 4.5 Total de Vulnerabilidades

Gráfica de Análisis de Vulnerabilidades.

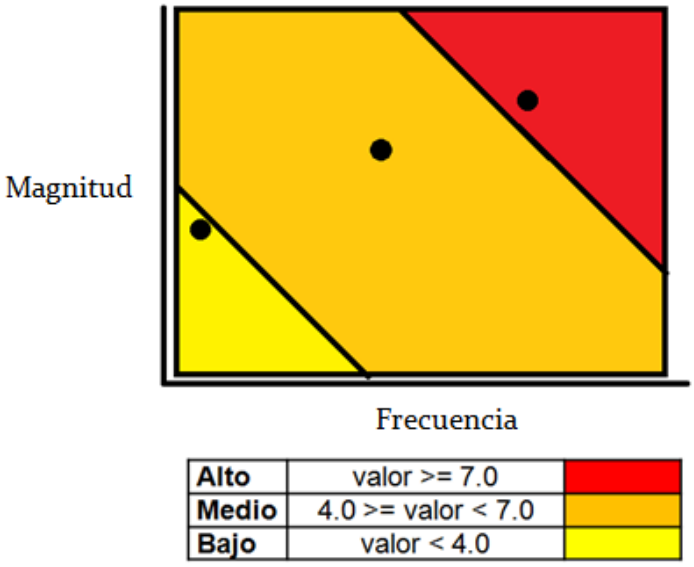


Figura 4.6 Gráfica de Análisis de Vulnerabilidades

Recomendaciones

A fin de ayudar a solventar las brechas de seguridad halladas en el servidor/ aplicación web se recomienda ejecutar las siguientes acciones:

- Se recomienda filtrar las variables del componente afectado por medio de funciones a fin de que no se permita la inyección de código malicioso.
- Actualizar a la versión más reciente del servidor Apache Tomcat.
- Dejar de publicar el servicio Mangosta
- Se recomienda implementa un sistema seguro a través de https

4.7. Cierre de la auditoría y Conclusiones

Cierre de Auditoría.

Esta actividad consiste enmostrar al cliente los hallazgos entroncados de forma sencilla y puntual enfocando el impacto y riesgo dirigido al negocio, de forma que al final se pida una firma de aceptación de los entregables dispuestos por el auditor, cerrando así el ciclo de la revisión y abriendo paso al cierre de hallazgos y seguimiento de recomendaciones por parte del auditado.

En esta fase se elabora y entrega el reporte de vulnerabilidades al cliente, documento que contiene un resumen ejecutivo y un reporte técnico que describe las vulnerabilidades del sistema; dentro se menciona el impacto que tendría dentro de la institución cada vulnerabilidad y recomendaciones por parte del auditor para, poder solventar dichas vulnerabilidades. Las vulnerabilidades son clasificadas y medidas a través de las métricas CVSS. (Para mayor información dirigirse al ***anexo [8] Reporte de Vulnerabilidades***)

Conclusiones.

Es necesario disminuir el riesgo que supone transferir la responsabilidad de los procesos comerciales de auditores humanos a aplicaciones y para ello nos encontramos con dos desafíos principales: la gestión de vulnerabilidades del software de terceras partes (que es principalmente una cuestión de actualizaciones y configuración) y la gestión de las vulnerabilidades del software desarrollado por la propia empresa. Este último paso requiere controles técnicos y de acciones, que servirían para dos fines: asegurar la confidencialidad, integridad y disponibilidad de los procesos comerciales una vez que se producen y reducir el coste de los incidentes de seguridad.

La mejor manera de instaurar las medidas adecuadas para salvaguardar las aplicaciones y procesos comerciales que sustentan es considerar la seguridad de las aplicaciones como los requisitos normativos que sirven para posibilitar los servicios web y limitar responsabilidades, dependiendo del público al que van dirigidos.

Derivado del análisis de vulnerabilidades realizado al aplicativo web “SISER”, se puede concluir que se encuentra en un nivel medio de criticidad, al descubrirse vulnerabilidades que pueden desembocar en la alteración visual y ejecución de código arbitrario así como probable fraude y robo de información confidencial, por tal motivo es necesario aplicar las recomendaciones expuestas en los anexos, lo que permitirá mitigar los riesgos a los que se encuentra actualmente expuesto el sistema.

ANEXOS

ANEXOS.

[1].- Carta de Autorización

[2].- Propuesta

[3].- Prerrequisitos Diagnostico y Alcance

[4].- Ficha de Pruebas

[5].- Plan de Auditoría

[6].- Evidencias de Auditoría

[7].- Checklist OWASP v2

[8].- Reporte de Vulnerabilidades

ANEXO [1].- Carta de Autorización

Asunto: Análisis de vulnerabilidades del sistema web SISER del área AIyPF Iusacell basado en la metodología de EC-Council

Fecha: 26/03/12

Para proteger adecuadamente los activos de la organización de tecnología de información, es necesario evaluar el grado de seguridad periódicamente mediante la realización de evaluaciones de vulnerabilidad y pruebas de penetración. Estas actividades suponen la revisión del **servidor de aplicaciones y elementos de red** propiedad de esta organización sobre una base regular y periódica, esto a fin de descubrir las vulnerabilidades presentes en estos sistemas. Sólo con el conocimiento de estas vulnerabilidades se pueden aplicar medidas correctivas u otros controles de compensación para mejorar la seguridad de nuestro medio ambiente.

El propósito de este documento es para conceder la autorización a los miembros específicos del equipo de seguridad de la información para llevar a cabo evaluaciones de vulnerabilidad y pruebas de penetración contra los bienes de esta organización. A tal fin, el firmante atestigua lo siguiente:

1) *Erick O. Ruiz Bernal,* tiene permiso para escanear el equipo de la organización de la computadora para encontrar vulnerabilidades. Este permiso se concede para el análisis de vulnerabilidades del día lunes 09 de abril al viernes 13 de abril del presente año.

2) *Julio González Aburto* tiene la autoridad para conceder este permiso para probar activos de la organización Tecnologías de la Información.

Periodo: 09-04-12 al 13-04-12

Firma: _____
Ing. Arturo Ulises Reyes Martínez
Líder de proyecto

Firma: _____
Ing. Julio González Aburto
Coordinador de Sistemas

Propuesta:

Análisis de vulnerabilidades basado en la metodología de EC-Council

Hacking Ético
CAJA GRIS

Para:

Sistema web SISER

Encargado:

Ing. Arturo Ulises Reyes Martínez

Fecha:

03 Febrero 2012

Elaboró:

Blancas Miranda Yadira.

Castillo Torres Adrian.

Eugenio Reyes Ernesto.

Reyes Martínez Arturo Ulises.

Ruiz Bernal Erick O.

(Versión 1.0)

ÍNDICE

1. ENTORNO

1.1 Confidencialidad

EQUIPO DE SEMINARIO DE TICS se obliga a guardar estricta confidencialidad sobre los elementos e información que proporcione **IUSACELL** así como sobre las operaciones que realizan para la generación de este documento. Lo anterior, en el entendido de que la información proporcionada por **IUSACELL** es clasificada por **EQUIPO DE SEMINARIO DE TICS** como confidencial. Por lo anterior **EQUIPO DE SEMINARIO DE TICS**, así como sus apoderados, empleados y/o funcionarios de cualquier clase, no podrán utilizar o divulgar la información sin la autorización expresa y por escrito de **IUSACELL** con un fin diferente al anteriormente especificado.

EQUIPO DE SEMINARIO DE TICS no se encuentra obligado a cumplir con la confidencialidad de la información proporcionada por **IUSACELL** en el caso de que una autoridad administrativa competente o judicial le requiera la información confidencial proporcionada, o bien que esta información ya sea conocida con anterioridad a la fecha de presentación de este documento por **EQUIPO DE SEMINARIO DE TICS**, o la información sea del dominio público.

1.2 Antecedentes del Proyecto.

En el área de Aseguramiento de Ingresos y Prevención de Fraudes (AIyPF) de Grupo Iusacell cuenta con una aplicación web de uso interno denominada Sistema Integral de Servicios de AIyPF (SISER AIyPF) donde se realiza la validación, facturación y objeciones para información de grupos terceros.

Debido a esto, se requiere que este portal sea seguro y confiable y garantice la seguridad de la información ya que la pérdida de esta puede generar riesgos económicos y de fraudes.

El sistema al no contar con una certificación de TI puede considerarse inseguro ya que no se ha validado el proceso del flujo de la información, ya que se realizo ateniendo a un requerimiento de prioridad alta y por su necesidad inmediata de desarrollo, no cuenta con ningún control de calidad.

Como principales medidas de seguridad el acceso al sistema está restringido por IP y solo el usuario final puede tener conexión desde su PC pasando por un acceso validando usuario y contraseña.

1.3 Objetivo de Negocio.

El objetivo principal de IUSACELL al contar con los servicios de outsourcing en consultoría por parte de EQUIPO DE SEMINARIO DE TICS consiste en tener la preparación de cumplimiento adecuada en Evidenciar las áreas de mejora en cuanto a la seguridad del Aplicativo Web SISER del grupo Iusacell para su posterior actualización.

1.4 Objetivo del Área.

El objetivo principal del área de sistemas al contar con este servicio es, garantizar que se cuenta con un sistema seguro para administrar y controlar la información de facturación de interconexión de carriers terceros.

2. JUSTIFICACIÓN

Mediante esta propuesta **IUSACELL** obtendrá los siguientes beneficios:

2.1 Beneficios del servicio propuesto.

El beneficio principal del servicio consiste en identificar y mitigar todas aquellas vulnerabilidades que la aplicación portal web SISER llegara a presentar durante el análisis.

Aseguramiento de la información utilizada en los distintos procesos dentro de la aplicación.

Le proporciona al usuario confiabilidad y certeza de la información que le proporciona el sistema.

2.2 Beneficios para T.I.

Adicional a los Beneficios para el Negocio, el área de Sistemas se verá beneficiada en los siguientes aspectos.

Alinear los sistemas de información a las políticas existentes de seguridad de la empresa.

Obtener un mayor grado de madurez en los procesos de sus aplicaciones.

2.3. Valores agregados

El valor agregado principal de esta propuesta consiste en proporcionar apoyo presencial a la Dirección de Operaciones cuando se presente la auditoría interna sin generar un costo adicional.

3. SERVICIOS PROPUESTOS

3.1 Descripción General.

La propuesta abarca la revisión, de un análisis de vulnerabilidades que consiste en realizar una evaluación de posibles fallos de seguridad, basado en el análisis de pruebas relacionadas con la identificación de puertos y servicios. Llevando a cabo un hacking ético de caja gris siendo la prueba más exhaustiva que se realiza a un sistema, su propósito es analizar íntegramente la seguridad de los sistemas de información utilizando técnicas de intrusión.

La duración del servicio es de una semana (5 hábiles) a partir del 09-04-12 al 13-04-12

El servicio implica el desarrollo de los siguientes puntos:

- Vulnerabilidades en aplicaciones web
- Inyección
- Secuencia de Comandos en Sitios Cruzados (XSS)
- Pérdida de Autenticación y Gestión de Sesiones
- Referencia Directa Insegura a Objetos
- Falsificación de Peticiones en Sitios Cruzados (CSRF)
- Defectuosa Configuración de Seguridad
- Almacenamiento Criptográfico Inseguro
- Falla de Restricción de Acceso a URL
- Protección Insuficiente en la Capa de Transporte
- Redirecciones y reenvíos no validados
- Desarrollo seguro
- Buenas prácticas
- Estándares y Normas

3.2 Personal

El personal que realizará el servicio cuenta con experiencia en:

- Desarrollo de sistemas en java
- Buenas prácticas de programación.
- Servidores de aplicaciones y Redes
- Administración de proyectos
- Hacking ético

El personal considerado para este servicio es el siguiente:

Equipo de Seminario de TICs

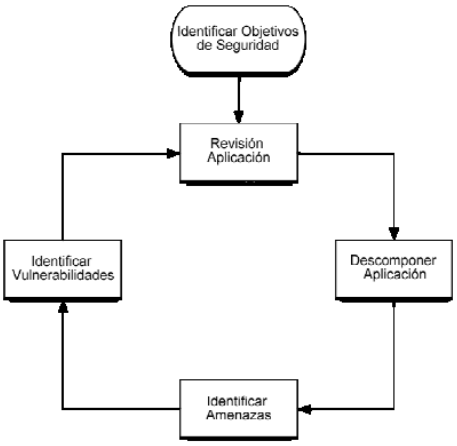
- Blancas Miranda Yadira
- Castillo Torres Adrian

- Eugenio Reyes Ernesto
- Reyes Martínez Arturo Ulises
- Ruiz Bernal Erick O.

3.3 Procesos

Los procesos involucrados en el desarrollo del servicio son:

De acuerdo a la guía para el desarrollo de aplicaciones web owasp



RIESGO	Agentes De Amenaza	Vectores de Ataque	Vulnerabilidades de Seguridad		Impactos Técnicos	Impactos al Negocio
		Explotación	Prevalencia	Detección	Impacto	
A1-Inyeccion		FACIL	COMUN	MEDIA	SEVERO	
A2-XSS		MEDIA	MUY DIFUNDIDA	FACIL	MOERADO	
A3-Autent'n		MEDIA	COMUN	MEDIA	SEVERO	
A4-DOR		FACIL	COMUN	FACIL	MODERADO	
A5-CSRF		MEDIA	MUY COMUN	FACIL	MODERADO	
A6-Config		FACIL	COMUN	FACIL	MODERADO	
A7-Crypto		DIFICIL	POCO COMUN	DIFICIL	SEVERO	
A8-Accesso URL		FACIL	POCO COMUN	MEDIA	MODERADO	
A9-Transporte		DIFICIL	COMUN	FACIL	MODERADO	
A10-Redirects		MEDIA	POCO COMUN	FACIL	MODERADO	

Con el modelo propuesto se garantiza:

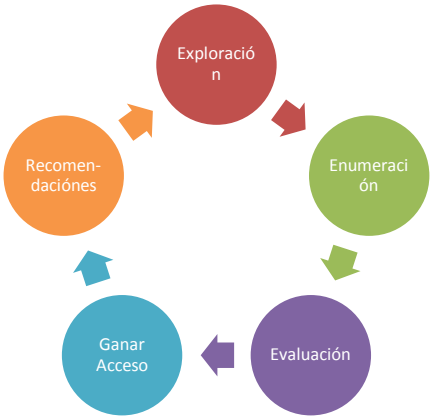
A. Beneficios para el Negocio

- Confiabilidad en procesos obtenida del sistema
- Integridad de la información contenida en el sistema SISER
- Disponibilidad de la información

B. Entregable

El modelo de convergencia está compuesto por los siguientes componentes:

Modelo del servicio propuesto:



3.4 Infraestructura

La infraestructura requerida para este servicio es:

- 1 lugar de trabajo para el consultor cuando este se presente en las instalaciones.
- 2 Conexión a subred.
- 3 Computadora, con herramientas para auditar aplicaciones web.

3.5 Alcances y Limitantes

Alcances.

Hacking Ético, caja gris de Sistema Web SISER.

Limitantes.

No es aceptable la intrusión a base de datos o sistemas productivos, encontrados en la misma subred.

4. PLAN DE IMPLEMENTACIÓN

4.1 Requerimientos

Esta sección describe las funciones y responsabilidades del **IUSACELL**. El cumplimiento de **EQUIPO DE SEMINARIO DE TICS** está condicionado a que las siguientes responsabilidades sean satisfechas por **IUSACELL** de acuerdo los siguientes puntos:

Los siguientes requerimientos son esenciales para llevar a cabo el servicio:

- Un representante y o encargado del sistema SISER deberá estar siempre presente cuando las pruebas se lleven a cabo.
- Una conexión a la red interna con alcance al servidor y o sistema al cual se le realizaran las pruebas.

4.2 Metodología

Uno de los grandes retos que tienen a menudo los técnicos de sistemas y redes de computadoras es que no cuentan con una forma estable para cuantificar la seguridad, únicamente se limitan a su cualificación, lo que les impide medir con exactitud, o llevar una estadística de variación del nivel de seguridad frente a cambios de configuración, escalabilidad, movilidad o cambios en las políticas de seguridad y en sí el aparecimiento de nuevas tecnologías que mal usadas pueden minimizar la seguridad.

La metodología utilizada se basa en una serie de etapas, donde se recolecta información, la cual es aprovechada después para realizar los ataques, terminando con la generación de recomendaciones más efectivas a fin de corregir las brechas encontradas.

La metodología, está basada en las siguientes etapas:

Exploración: en esta fase, se hace uso de información del dominio público, disponible en Internet para identificar vulnerabilidades e información de los sistemas operativos de los servidores y los servicios existentes.

Enumeración: habiendo obtenido una cantidad de información razonable, se procede a enumerar los hosts y servicios en la red interna, mediante herramientas de escaneo de puertos y vulnerabilidades.

Evaluación: teniendo la lista de los servicios activos, se procede a revisar dichos servicios por su naturaleza, versión de software y sistema operativo, en base a vulnerabilidades documentadas.

Pen-Test: las aplicaciones también son revisadas, se realizan pruebas como SQL-injections, pruebas de buffer overflows (BOF), cross-site scripting, entre otras, a fin de evaluar el nivel de seguridad y si es posible obtener información de las bases de datos internas.

Corrección: Recomendar los controles técnicos necesarios para cerrar las vulnerabilidades encontradas para evitar su materialización.

4.3 Equipo de Trabajo

Para el desarrollo del proyecto por parte de **EQUIPO DE SEMINARIO DE TICS** participarán:

Blancas Miranda Yadira

Castillo Torres Adrian

Eugenio Reyes Ernesto

Reyes Martínez Arturo Ulises

Ruiz Bernal Erick O.

4.4. Calendario de actividades

1		Proyecto Hacking Ético - Caja Gris Sistema Web SISER	8.88 días	vie 06/04/12	mar 17/04/12
1.1		FASE 1. Inicio del Proyecto	0.88 días	vie 06/04/12	vie 06/04/12
1.1.1		Definición de target, tiempo y forma para análisis de vulnerabilidades	0.88 días	vie 06/04/12	vie 06/04/12
1.1.1.1		Reunión con cliente	0.88 días	vie 06/04/12	vie 06/04/12
1.1.1.1.1		Definición de metodología para análisis	0 días	vie 06/04/12	vie 06/04/12
1.1.1.1.2		Definición de fechas para análisis	0 días	vie 06/04/12	vie 06/04/12
1.1.2		Hito: Fechas compromiso de pruebas	0 días	vie 25/11/11	vie 25/11/11
1.2		FASE 2. Escaneo de Vulnerabilidades y pentest	4.88 días	lun 09/04/12	vie 13/04/12
1.2.1		Asignación del equipo de trabajo para supervisión de pruebas	0 días	lun 09/04/12	lun 09/04/12
1.2.2		Confirmación de target	1 día	lun 09/04/12	lun 09/04/12
1.2.3		FASE 2.2 Caja Gris	1.88 días	mar 10/04/12	mié 11/04/12
1.2.3.1		Definición de cita para visita a instalaciones	0 días	mar 10/04/12	mar 10/04/12
1.2.3.1.1		Agendar y confirmar cita	0 días	mar 10/04/12	mar 10/04/12
1.2.3.2		Hito: Cliente - Datos de acceso a sistema (Cuenta Demo)	0 días	mar 10/04/12	mar 10/04/12
1.2.3.3		[Caja Gris] - Testing	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.1		Recopilación de Información	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.2		Pruebas de Gestión de Configuración	0.8 días	mar 10/04/12	mar 10/04/12
1.2.3.3.3		Pruebas de Autenticación	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.4		Gestión de Sesiones	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.5		Pruebas de Autorización	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.6		Pruebas de Lógica de Negocio	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.7		Pruebas de Validación de Datos	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.8		Pruebas de negación de Servicio *Solo Mirror	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.9		Pruebas de Servicios Web	1 día	mar 10/04/12	mar 10/04/12
1.2.3.3.10		Pruebas Ajax	1 día	mar 10/04/12	mar 10/04/12
1.2.3.4		[Caja Gris] - Validation	1 día	mié 11/04/12	mié 11/04/12
1.2.3.4.1		Pruebas manuales	1 día	mié 11/04/12	mié 11/04/12
1.2.3.4.2		Visita a instalaciones	0.5 días	mié 11/04/12	mié 11/04/12
1.2.3.4.2.1		Recepción a instalaciones	0.5 días	mié 11/04/12	mié 11/04/12
1.2.3.5		[Caja Gris] - Research	1 día	jue 12/04/12	jue 12/04/12
1.2.3.5.1		Documentación de Información sobre hallazgos	1 día	jue 12/04/12	jue 12/04/12
1.2.3.5.2		Contramedidas, mejores prácticas y recomendaciones	1 día	jue 12/04/12	jue 12/04/12
1.2.4		Hito: Email, termino pruebas caja gris	0 días	vie 13/04/12	vie 13/04/12
1.3		FASE 3 Documentación de respaldo de Assessment	2.13 días	sáb 14/04/12	dom 15/04/12
1.3.1		Recopilación de información para Assessment	0 días	sáb 14/04/12	sáb 14/04/12
1.3.2		Hito: Entregable Informe de resultados final	1 día	dom 15/04/12	dom 15/04/12
1.3.3		Revisión y Recepción de informe de resultados	1 día	dom 15/04/12	dom 15/04/12
1.4		FASE 5 Finalización del proyecto	1 día	lun 16/04/12	lun 16/04/12
1.4.1		Reunión de aclaración de informe de resultado final	1 día	lun 16/04/12	lun 16/04/12
1.4.1.1		Validación de informe final	0.5 días	lun 16/04/12	lun 16/04/12
1.4.1.2		Reunión de termino de proyecto	0.5 días	lun 16/04/12	lun 16/04/12
1.4.2		Hito: Carta de aceptación del reporte por parte del cliente	0 días	lun 16/04/12	lun 16/04/12

4.5 Riesgos del Proyecto

- Falta de atención por parte del cliente hacia el auditor.
- Inexistencia de conexión entre el equipo del auditor y el auditado.
- Fechas compromiso no cumplidas.
- Desinterés por parte del cliente.
- Falta de conocimiento por parte del equipo técnico
- Provocar una negación de servicio al aplicativo y o sistema.
- Fallas de infraestructura.

5. ACEPTACIÓN

5.1 Entregables

Informe Ejecutivo

Compuesto por:

- Introducción
- Objetivo
- Alcance de las tareas realizadas.
- Sumario hallazgos (Formato Gráfico Ejecutivo)
- Principales fortalezas*
- Principales debilidades*
- Recomendaciones
- Conclusión

Informe Técnico

Compuesto por:

- Introducción
- Objetivo
- Alcance de las tareas realizadas.
- Principales fortalezas*
- Principales debilidades identificadas
- Evidencias
- Recomendaciones
- Conclusión

Presentación Final (opcional)

Compuesto por:

- Exposición presencial de Conclusiones ante Directivos
- Exposición presencial de Conclusiones ante personal Técnico.

5.2 Criterios de Aceptación

Los criterios para dar como aceptado el servicio son:

El auditor hará entrega de toda la documentación de forma confidencial en tiempo y forma según lo acordado en la propuesta.

6. PROPUESTA ECONÓMICA

6.1 Cotización

El precio del proyecto, es el siguiente:

CONCEPTO	COSTO
Hacking Ético Caja Gris a sistema SISER	9000
Subtotal	9000
IVA	1350
Total	10350

ANEXO [3].- Prerrequisitos Diagnostico y Alcance 1

Diagnostico y alcance

Prerrequisitos y entregables

Privacidad: Este documento está sujeto a las clausulas de confidencialidad.

Propósito del Documento: Este documento describe los entregables por parte del cliente para ser sometido a la evaluación de seguridad.

CONTROL DE VERSIONES:

Versión	Fecha	Autores	Descripción del cambio
1.0	03/Abril/2012	Erick Ruiz y Arturo U. Reyes	Generación de documento

CONTENIDO

Datos generales

Nombre de la empresa:	Iusacell S.A de C.V
Dirección:	Montes Urales 460
Contacto:	aureyes@iusacell.com.mx, 51095654
Actividad o giro:	Telecomunicaciones

Marque con una X para indicar su entrega.

Proporciona:	X
Organigrama General del área de TI:	-
Número total de empleados:	-
Número de empleados del área de TI:	-
Número de empleados que acceden a sistemas de TI.	-
Número de oficinas y centros de procesamiento, comunicación o almacenamiento de datos.	-

Oficinas y centros de procesamiento:

Nombre	Ubicación	Funciones/Observaciones	Responsable
Corporativo	Montes Urales 460	Administración	
Torre Unefon	Periférico Sur 4121	Sistemas	
SAI Toluca	Toluca	Monitoreo	

Aplicaciones

Nombre de Aplicación	Descripción	Desarrollo interno/externo	Tecnología(s)
SISER/	SISER AIyPF Sistema Integral de Servicios de Aseguramiento de Ingresos y Prevención de Fraudes (Gestiona la Facturación de Carriers Terceros)	Interno	Java, JSFs, PrimeFaces, RichFaces, JavaBeans

Portales		
Nombre/Dominio/Subdominios	Descripción	Tecnología(s)
172.19.235.122:8080/ SISER/	Sistema Integral de Servicios AIyPF	Java, JSFs,

Sistemas

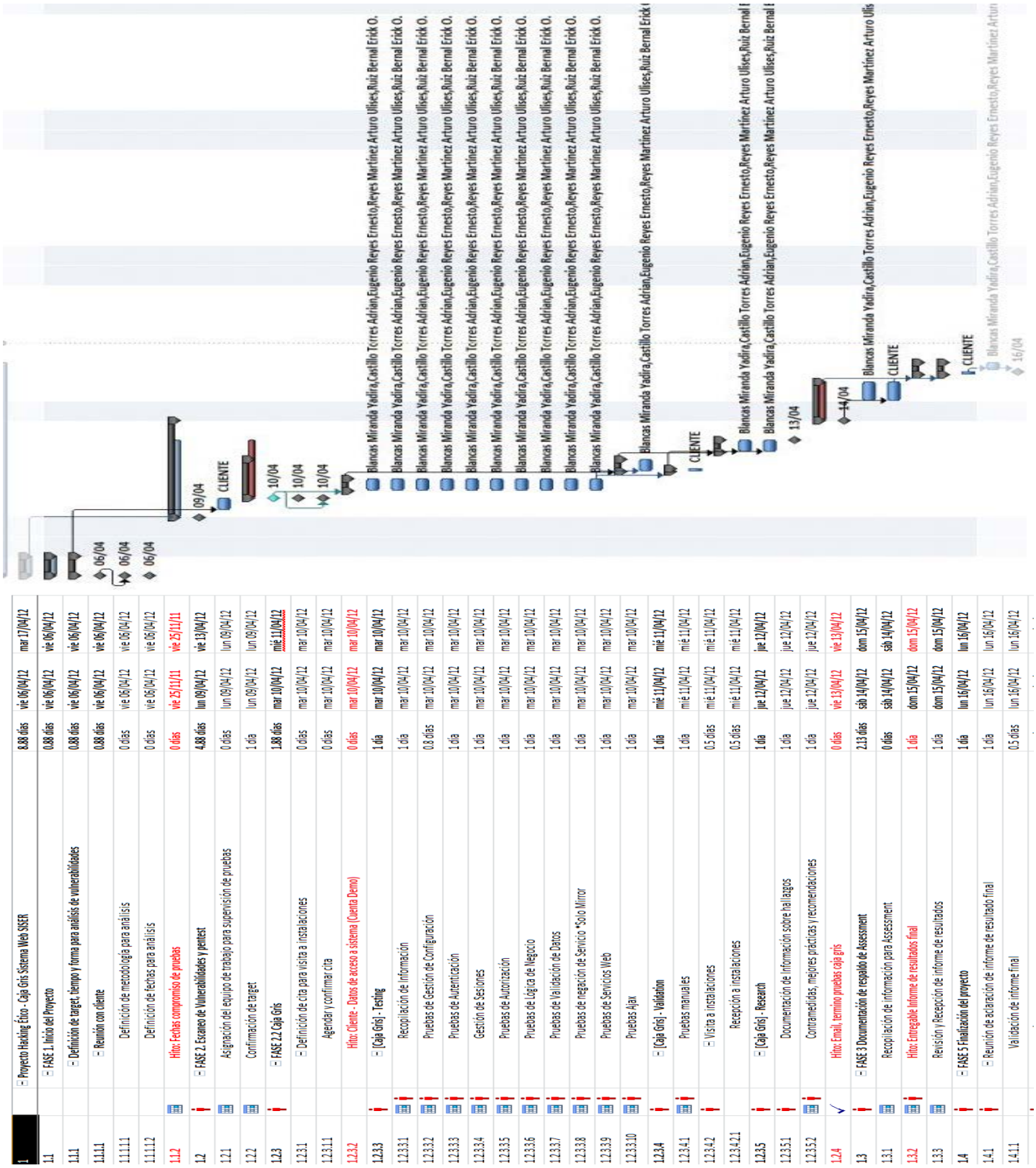
Producto	Versión	Sistema operativo	Tecnología(s)
SISER	3.0	UNIX	Java SDK
Apache Tomcat	7.0.2	UNIX	Servidor de aplicaciones
Shell Unix	2.6.18-164.el5	i386	Servidor
JVM	1.6.0_21-b06	UNIX	Maquina virtual de java

Sistemas Operativos		
Sistema	Propósito	Dependencias
Shell Unix (siafraud)	Almacenar y gestionar servicios web	merida
HP-UX (merida)	Base de datos y procesamiento de shell	Independiente y siafraud

Ficha de Pruebas

Fecha y hora de inicio de las pruebas:	09/04/2012 – 7:00pm
Fecha y hora de término de las pruebas:	13/04/2012 – 9:00pm
Equipos/Aplicaciones a evaluar, especificando dirección IP:	172.19.235.122:8084/SISER
Nombre del responsable del Equipo/Aplicaciones a Evaluar:	Arturo Ulises Reyes Martínez / Sistema Web SISER
Datos de contacto del Responsable del Equipo/Aplicaciones a evaluar:	aureyes@iusacell.com.mx, Tel: 51095654, Cel.: 5530308023
Nombre del equipo o persona que realizará las pruebas:	Erick O. Ruiz Bernal y Arturo Ulises Reyes Martínez
Datos de contacto del equipo o persona que realizará las pruebas:	Erick O. Ruiz Bernal 55 38 79 29 02
Nombre del solicitante de las pruebas:	Arturo Ulises Reyes Martínez

ANEXO [5].- Plan de Auditoría 1



1	Proyecto Hacking Ético - Caja Gris Sistema Web SISER	8.88 días	vie 06/04/12	mar 17/04/12	
1.1	FASE 1. Inicio del Proyecto	0.88 días	vie 06/04/12	vie 06/04/12	
1.1.1	Definición de target, tiempo y forma para análisis de vulnerabilidades	0.88 días	vie 06/04/12	vie 06/04/12	
1.1.1.1	Reunión con cliente	0.88 días	vie 06/04/12	vie 06/04/12	
1.1.1.1.1	Definición de metodología para análisis	0 días	vie 06/04/12	vie 06/04/12	
1.1.1.1.2	Definición de fechas para análisis	0 días	vie 06/04/12	vie 06/04/12	
1.1.2	Hito: Fechas compromiso de pruebas	0 días	vie 25/11/11	vie 25/11/11	
1.2	FASE 2. Escaneo de Vulnerabilidades y pentest	4.88 días	lun 09/04/12	vie 13/04/12	
1.2.1	Asignación del equipo de trabajo para supervisión de pruebas	0 días	lun 09/04/12	lun 09/04/12	
1.2.2	Confirmación de target	1 día	lun 09/04/12	lun 09/04/12	
1.2.3	FASE 2.2 Caja Gris	1.88 días	mar 10/04/12	mié 11/04/12	
1.2.3.1	Definición de cita para visita a instalaciones	0 días	mar 10/04/12	mar 10/04/12	
1.2.3.1.1	Agendar y confirmar cita	0 días	mar 10/04/12	mar 10/04/12	
1.2.3.2	Hito: Cliente - Datos de acceso a sistema (Cuenta Demo)	0 días	mar 10/04/12	mar 10/04/12	
1.2.3.3	[Caja Gris] - Testing	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.1	Recopilación de información	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.2	Pruebas de Gestión de Configuración	0.8 días	mar 10/04/12	mar 10/04/12	
1.2.3.3.3	Pruebas de Autenticación	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.4	Gestión de Sesiones	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.5	Pruebas de Autorización	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.6	Pruebas de Lógica de Negocio	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.7	Pruebas de Validación de Datos	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.8	Pruebas de negación de Servicio *Solo Mirror	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.9	Pruebas de Servicios Web	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.3.10	Pruebas Ajax	1 día	mar 10/04/12	mar 10/04/12	
1.2.3.4	[Caja Gris] - Validation	1 día	mié 11/04/12	mié 11/04/12	
1.2.3.4.1	Pruebas manuales	1 día	mié 11/04/12	mié 11/04/12	
1.2.3.4.2	Visita a instalaciones	0.5 días	mié 11/04/12	mié 11/04/12	
1.2.3.4.2.1	Recepción a instalaciones	0.5 días	mié 11/04/12	mié 11/04/12	
1.2.3.5	[Caja Gris] - Research	1 día	jue 12/04/12	jue 12/04/12	
1.2.3.5.1	Documentación de información sobre hallazgos	1 día	jue 12/04/12	jue 12/04/12	
1.2.3.5.2	Contramedidas, mejores prácticas y recomendaciones	1 día	jue 12/04/12	jue 12/04/12	
1.2.4	Hito: Email, termino pruebas caja gris	0 días	vie 13/04/12	vie 13/04/12	
1.3	FASE 3 Documentación de respaldo de Assessment	2.13 días	sáb 14/04/12	dom 15/04/12	
1.3.1	Recopilación de información para Assessment	0 días	sáb 14/04/12	sáb 14/04/12	
1.3.2	Hito: Entregable informe de resultados final	1 día	dom 15/04/12	dom 15/04/12	
1.3.3	Revisión y Recepción de informe de resultados	1 día	dom 15/04/12	dom 15/04/12	
1.4	FASE 5 Finalización del proyecto	1 día	lun 16/04/12	lun 16/04/12	
1.4.1	Reunión de aclaración de informe de resultado final	1 día	lun 16/04/12	lun 16/04/12	
1.4.1.1	Validación de informe final	0.5 días	lun 16/04/12	lun 16/04/12	

En este documento se muestran las evidencias de las pruebas realizadas para el análisis de vulnerabilidades del aplicativo web SISER.

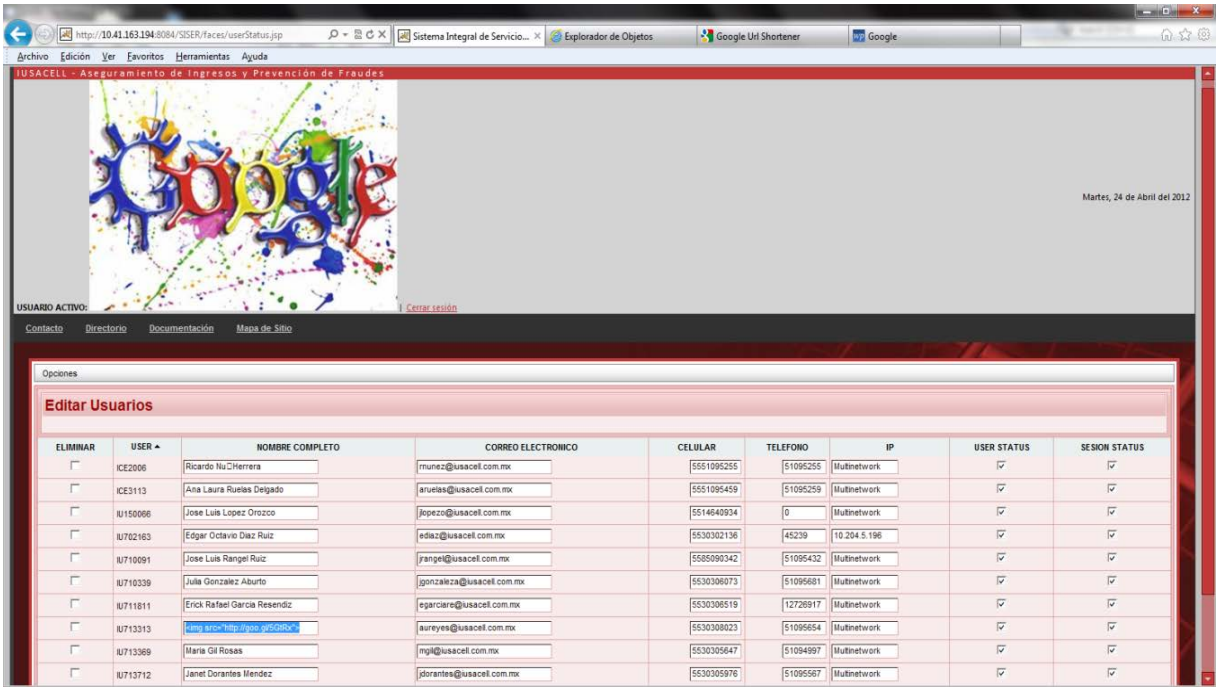
1.1. Dominio: 172.19.235.122:8084/SISER

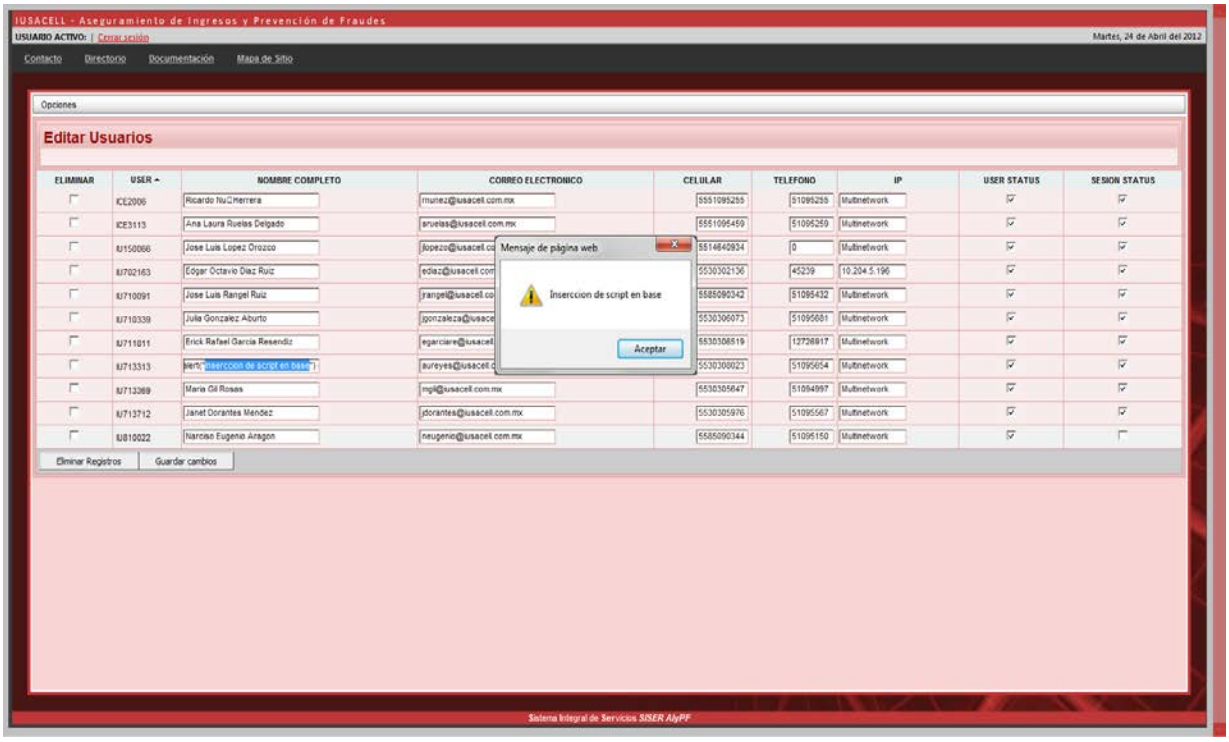
1.1.1. Negación de servicio

High (CVSS: 7.8) blackice-alerts (8082/tcp)
NVT: Mongoose Webserver Content-Length Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.900268)

```
Overview:
This host is running Mongoose Webserver and is prone to denial of service
vulnerability.
Vulnerability Insight:
The flaw is caused due to the way Mongoose webserver handles request with a
big nagitive 'Content-Length' causing application crash.
Impact:
Successful exploitation will let the remote unauthenticated attackers to
cause a denial of service or possibly execute arbitrary code.
Impact Level: Application
Affected Software/OS:
Mongoose webserver version 2.11 and prior.
Fix: No solution or patch is available as on 29th December, 2010. Information
regarding this issue will be updated once the solution details are available.
For updates refer, http://code.google.com/p/mongoose/
References:
http://code.google.com/p/mongoose/
http://www.johnleitch.net/Vulnerabilities/Mongoose.2.11.Denial.Of.Service/74
```

1.1.2. XSS


IUSACELL - Aseguramiento de Ingresos y Prevención de Fraudes
Martes, 24 de Abril del 2012
USUARIO ACTIVO:
Cerrar sesión
Contacto
Directorio
Documentación
Mapa de Sitio
Opciones
Editar Usuarios


IUSACELL - Aseguramiento de Ingresos y Prevención de Fraudes
Mensaje de página web
Inserccion de script en base
Aceptar
Editar Usuarios
Eliminar Registros
Guardar cambios

1.1.3 XSS

PORT WWW (8082/TCP)

Plugin ID: **10815**

Web Server Generic XSS

Plugin Output

The request string used to detect this flaw was :

/<script>cross_site_scripting.nasl</script>.asp

The output was :

HTTP/1.0 404 No Encontrado
Content-Type: text/html
Content-Length: 266
Servlet-Engine: Tomcat Web Server/3.2 (final) (JSP 1.1; Servlet 2.2; Java 1.7.0_03; Windows 7 6.1 amd64; java.vendor=Oracle Corporation)

<head><title>No se encuentra (404)</title></head>
<body><h1>No se encuentra (404)</h1>
Request original: /<script>cross_site_scripting.nasl</script>.asp

No se ha encontrado el request: /<script>cross_site_scripti [...]

1.3.4 Apache Tomcat múltiples vulnerabilidades

PORT WWW (8082/TCP)

Plugin ID: **46753**

Apache Tomcat < 4.1.40 / 5.5.28 / 6.0.20 Multiple Vulnerabilities

Synopsis
The remote Apache Tomcat service may be affected by multiple vulnerabilities.

Description
According to its self-reported version number, the Apache Tomcat listening on the remote host is earlier than Tomcat 4.1.40 / 5.5.28 / 6.0.20 and, as such, may be affected by one or more of the following vulnerabilities :

- The remote service may be vulnerable to a directory traversal attack if a RequestDispatcher obtained from a Request object is used. A specially crafted value for a request parameter can be used to access potentially sensitive configuration files or other files, e.g., files in the WEB-INF directory. (CVE-2008-5515)

- The remote service may be vulnerable to a denial of service attack if configured to use the Java AJP connector. An attacker can send a malicious request with invalid headers which causes the AJP connector to be put into an error state for a short time. This behavior can be used as a denial of service attack. (CVE-2009-0033)

- The remote service may be vulnerable to a username enumeration attack if configured to use FORM authentication along with the 'MemoryRealm', 'DataSourceRealm', or 'JDBCRealm' authentication realms.

Categoría	Número de Ref.	Nombre de Prueba	Elementos	Conclusión	Comentarios/ Solución	Riesgo
Recopilación de Información	OWASP-IG-001	Spiders, Robots y Crawlers	INFORMATIVO			
	OWASP-IG-002	Descubrimiento/Reconocimiento mediante motores de búsqueda	N/A			
	OWASP-IG-003	Identificación de puntos de entrada de la aplicación	SISTEMA SISER	Se logró observar el login de la aplicación en la ruta /SISER		
	OWASP-IG-004	Pruebas de firma digital de Aplicaciones Web	N/A			
	OWASP-IG-005	Descubrimiento de Aplicaciones	N/A			
	OWASP-IG-006	Análisis de Códigos de Errores	N/A			
Pruebas de Gestión de Configuración	OWASP-CM-001	Pruebas SSL/TLS (SSL Versión, Algoritmos, longitud de Claves, Validez de Certificado Digital)	N/A	N/A	N/A	N/A
	OWASP-CM-002	Prueba de DB Listener	N/A			
	OWASP-CM-003	Prueba de Gestión de Configuración de Infraestructura	N/A			
	OWASP-CM-004	Prueba de Gestión de Configuración de Aplicación	N/A			
	OWASP-CM-005	Prueba del Gestor de Extensión de Ficheros	N/A			
	OWASP-CM-006	Antiguo, backup y ficheros no referenciados	NO VULNERABLE			
	OWASP-CM-007	Interface de Administración de Aplicación e Infraestructura	N/A			
	OWASP-CM-008	Prueba de métodos HTTP y XST	NO VULNERABLE			
Pruebas de Autenticación	OWASP-AT-001	Transporte de Credenciales sobre canal cifrado	SISTEMA SISER	Al utilizar el protocolo HTTP , las credenciales de los usuarios viajan en claro	Implementar HTTPS , de forma que las conexiones estén cifradas	
	OWASP-AT-002	Prueba para Enumeración de usuarios	N/A			
	OWASP-AT-003	Prueba de detección de Cuentas de Usuario Adivinables (Diccionario)	NO VULNERABLE			
	OWASP-AT-004	Prueba de Fuerza Bruta	NO VULNERABLE	No se logro la entrada satisfactoria al panel de administración a través de fuerza bruta		
	OWASP-AT-005	Prueba para evitar el esquemas de autenticación	NO VULNERABLE	NO ULNERABLE	NV	NV
	OWASP-AT-006	Prueba de recordatorio de contraseña y restablecimiento	NO VULNERABLE			
	OWASP-AT-007	Prueba de Cierre de Sesión y Gestión de Cache de Navegación	NO VULNERABLE	NV	NV	NV
	OWASP-AT-008	Prueba de CAPTCHA	SISTEMA SISER	El sistema no cuenta con un sistema de capthca lo que permite realizar ataques de fuerza bruta.		
	OWASP-AT-009	Prueba de Autenticación de Múltiple Factores	NO VULNERABLE			
	OWASP-AT-010	Prueba de Condiciones de Carrera	NO VULNERABLE			

Categoría	Número de Ref.	Nombre de Prueba	Elementos	Conclusión	Comentarios/ Solución	Riesgo
Gestión de Sesiones	OWASP-SM-001	Prueba del Esquema de Gestión de Sesión	NO VULNERABLE			
	OWASP-SM-002	Prueba de atributos de Cookies	NO VULNERABLE			
	OWASP-SM-003	Prueba de Fijación de Sesión	NO VULNERABLE			
	OWASP-SM-004	Prueba de Variables de Sesión Expuestas	SISTEMA SISER	El sistema es vulnerable con la información de sus variables		
	OWASP-SM-005	Prueba de CSRF	SISTEMA SISER	El sistema es vulnerable a una petición repetida de código reflejado		
Pruebas de Autorización	OWASP-AZ-001	Prueba de Ruta Transversal	NO VULNERABLE			
	OWASP-AZ-002	Prueba para Evitar Esquema de Autorización	NO VULNERABLE			
	OWASP-AZ-003	Prueba de escalada de Privilegios	NO VULNERABLE			
Pruebas de Lógica de Negocio	OWASP-BL-001	Prueba de Lógica de Negocio	NO VULNERABLE			
Pruebas de Validación de Datos	OWASP-DV-001	Prueba de XSS Reflejado	SISTEMA SISER	http://172.19.235.122:8085/SISER/faces/index.jsp;jsessionid=3D361392BD8B9B4669A77C2EBBB14BD3		
	OWASP-DV-002	Prueba de XSS Almacenado	SISTEMA SISER	http://172.19.235.122:8085/SISER/faces/index.jsp;jsessionid=3D361392BD8B9B4669A77C2EBBB14BD3		
	OWASP-DV-003	Prueba de XSS basado en DOM	NO VULNERABLE			
	OWASP-DV-004	Prueba de XSS basado en Flash	NO VULNERABLE			
	OWASP-DV-005	Inyección SQL	NO VULNERABLE			
	OWASP-DV-006	Inyección LDAP	NO VULNERABLE			
	OWASP-DV-007	Inyección ORM	NO VULNERABLE			
	OWASP-DV-008	Inyección XML	NO VULNERABLE			
	OWASP-DV-009	Inyección SSI	NO VULNERABLE			
	OWASP-DV-010	Inyección Xpath	NO VULNERABLE			
	OWASP-DV-011	Inyección IMAP/SMTP	NO VULNERABLE			
	OWASP-DV-012	Inyección de Código	SISTEMA SISER	Se prueba la inyección de código		
	OWASP-DV-013	Inyección de Ordenes del Sistema Operativo	NO VULNERABLE			
	OWASP-DV-014	Desbordamiento de *buffer*	SISTEMA SISER	El componente Mongoose Webserver es vulnerable al desbordamiento de buffer a través de la variable 'Content-Length'		
	OWASP-DV-015	Prueba de Vulnerabilidad incubada	NO VULNERABLE			
	OWASP-DV-016	Prueba de HTTP *Splitting/Smuggling*	SISTEMA SISER			

Categoría	Número de Ref.	Nombre de Prueba	Elementos	Conclusión	Comentarios/ Solución	Riesgo
Pruebas de Denegación de Servicio	OWASP-DS-001	Prueba de Ataques a través de Comodines SQL	N/A			
	OWASP-DS-002	Bloqueo de Cuentas de Usuarios	N/A			
	OWASP-DS-003	Pruebas de DoS mediante Desbordamiento de *Buffer*	N/A			
	OWASP-DS-004	Asignación de Objeto de Usuario Especificado	N/A			
	OWASP-DS-005	Entrada de usuario como un contador de bucle	N/A			
	OWASP-DS-006	Prueba de Escritura en Disco de data provista por Usuario	N/A			
	OWASP-DS-007	Fallo en Liberar Recursos	N/A			
	OWASP-DS-008	Almacenamiento de demasiados datos en Sesión	N/A			
Pruebas de Servicios Web	OWASP-WS-001	Recopilación de Información de WS	NO VULNERABLE			
	OWASP-WS-002	Prueba de WSDL	NO VULNERABLE			
	OWASP-WS-003	Prueba en la Estructura del XML	NO VULNERABLE			
	OWASP-WS-004	Prueba del XML a nivel de contenido	NO VULNERABLE			
	OWASP-WS-005	Prueba de REST/parámetros HTTP GET	NO VULNERABLE			
	OWASP-WS-006	Adjuntos SOAP maliciosos	NO VULNERABLE			
	OWASP-WS-007	Prueba de Repetición	NO VULNERABLE			
Pruebas Ajax	OWASP-AJ-001	Vulnerabilidades Ajax	NO VULNERABLE			
	OWASP-AJ-002	Pruebas Ajax	NO VULNERABLE			

Análisis de Vulnerabilidades Interno

CAJA GRIS

Para:

Sistema Web SISER

Encargado:

Arturo Ulises Reyes Martínez

Fecha:

09 Abril 2012 – 15 Abril 2012

Elaboró:

Blancas Miranda Yadira.

Castillo Torres Adrian.

Eugenio Reyes Ernesto.

Reyes Martínez Arturo Ulises.

Ruiz Bernal Erick O.

(Versión 1.0)

ÍNDICE

ÍNDICE

ANEXO [8].- Reporte de Vulnerabilidades 3

1 Administración de la documentación

1.1. Confidencialidad

EL EQUIPO DEL SEMINARIO DE TITULACIÓN se obliga a guardar estricta confidencialidad sobre los elementos e información que proporcione **IUSACELL** así como sobre las operaciones que realizan para la generación de este documento. Lo anterior, en el entendido de que la información proporcionada por **IUSACELL** es clasificada por **EL EQUIPO DEL SEMINARIO DE TITULACIÓN** como confidencial. Por lo anterior **EL EQUIPO DEL SEMINARIO DE TITULACIÓN,** así como sus apoderados, empleados y/o funcionarios de cualquier clase, no podrán utilizar o divulgar la información sin la autorización expresa y por escrito de **IUSACELL** con un fin diferente al anteriormente especificado.

EL EQUIPO DEL SEMINARIO DE TITULACIÓN no se encuentra obligado a cumplir con la confidencialidad de la información proporcionada por **IUSACELL** en el caso de que una autoridad administrativa competente o judicial le requiera la información confidencial proporcionada, o bien que esta información ya sea conocida con anterioridad a la fecha de presentación de este documento por **EL EQUIPO DEL SEMINARIO DE TITULACIÓN,** o la información sea del dominio público.

1.2 Manejo de versiones

El presente documento será considerado válido y con vigencia siempre que los cambios hayan sido autorizados y aprobados por los responsables definidos en la siguiente sección

1.3 Elaboración del documento

LEVANTAMIENTO DE INFORMACIÓN: ERICK RUIZ		09/04/2012
REVISADO Y AUDITADO : BLANCAS MIRANDA YADIRA		17/04/2012
REVISADO Y AUDITADO : ERNESTO EUGENIO REYES		17/04/2012
REVISADO Y AUDITADO: ADRIAN CASTILLO TORRES		17/04/2012

1.4 Control de versiones

RESPONSABLE	REVISION	FECHA DE REVISION
BLANCAS MIRANDA YADIRA	1	17/04/2012

1.5 Control y mantenimiento de la información.

Dueño del Documento:	IUSACELL
Información del contacto para las correcciones o las adiciones de la documentación:	Arturo Ulises Reyes Martínez
Accesibilidad de la documentación antes y durante las pruebas:	Arturo Ulises Reyes Martínez

1.6 Glosario de términos.

Término	Definición
CVSS	Common Vulnerability Scoring System
OWASP	The Open Web Application Security Project
ASVS	OWASP Application Security Verification Standard
XSS	Cross-site scripting

2. Resumen ejecutivo

2.1. Contexto

Durante el período comprendido del 09/04/2012 .13/04/2012 se llevaron a cabo pruebas de **caja gris** de Sistema Web SISER

Las pruebas realizadas están denotadas con las siguientes actividades:

- Identificación de equipos y puertos abiertos mediante la ejecución de herramientas como Nmap 5.0.
- Detección de vulnerabilidades mediante las herramientas: Tenable Nessus, Nikto v2.1.4 y Acunetix.
- Aplicación de pruebas de seguridad manuales a los servicios Web detectados.
- Verificación de los hallazgos detectados por las herramientas anteriormente mencionadas.

2.2. Objetivos

El propósito de las pruebas fue determinar si existen vulnerabilidades en los aplicativos seleccionados:

Sistema Web SISER

Una vez identificadas y verificadas las vulnerabilidades, se procederá a dar las recomendaciones pertinentes para cerrar las vulnerabilidades encontradas para evitar su materialización.

2.3. Hallazgos

2.3.1. Resumen de Hallazgos

Evidencia	Impacto	Recomendaciones
Negación de Servicio. Se evidencia la falta restricción de puertos, dejando servicios obsoletos que podrían provocar una negación del servicio del aplicativo. *Falta de actualizaciones en servicios Web.* Se evidencia la falta de un procedimiento formal para asegurar la correcta y oportuna aplicación de actualizaciones de seguridad en servicios Web. Se evidencia la falta de un procedimiento formal para asegurar la correcta implementación de aplicaciones web, sustentadas en buenas prácticas y programación segura.	Perdida de la continuidad de los servicios activos del aplicativo web. Perdida de la continuidad de los servicios activos en el servidor. Perdida de información y continuidad de los servicios así como daño a la imagen corporativa	• Delimitar los puertos y servicios que se encuentren activos en el servidor , así como mantener una actualización de dichos componentes • Antes de aplicar alguna actualización, realizar un estudio de funcionalidad para verificar que los aplicativos funcionan después de los cambios. • Elaborar e implementar un procedimiento para la administración de actualizaciones de los servicios Web, considerando el control de cambios, pruebas y gestión de configuraciones. • Basar desarrollo en la GUIA OWASP que describe buenas prácticas en el diseño e implementación de aplicativos web, probar las aplicaciones después de la actualización de código, asegurando que no permanezcan las vulnerabilidades descritas. • Monitorear y aplicar filtros de calidad a los aplicativos web antes de su liberación a producción.

3. Marco de referencia

3.1. Metodología

Uno de los grandes retos que tienen a menudo los técnicos de sistemas y redes de computadoras es que no cuentan con una forma estable para cuantificar la seguridad, únicamente se limitan a su cualificación, lo que les impide medir con exactitud, o llevar una estadística de variación del nivel de seguridad frente a cambios de configuración, escalabilidad, movilidad o cambios en las políticas de seguridad y en sí el aparecimiento de nuevas tecnologías que mal usadas pueden minimizar la seguridad.

La metodología utilizada se basa en una serie de etapas, donde se recolecta información, la cual es aprovechada después para realizar los ataques, terminando con la generación de recomendaciones más efectivas a fin de corregir las brechas encontradas.

La metodología, está basada en las siguientes etapas:

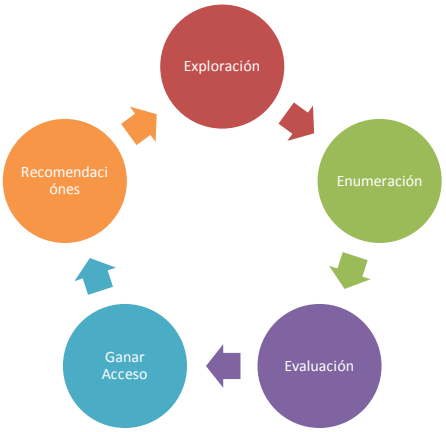
Exploración: en esta fase, se hace uso de información del dominio público, disponible en Internet para identificar vulnerabilidades e información de los sistemas operativos de los servidores y los servicios existentes.

Enumeración: habiendo obtenido una cantidad de información razonable, se procede a enumerar los hosts y servicios en la red interna, mediante herramientas de escaneo de puertos y vulnerabilidades.

Evaluación: teniendo la lista de los servicios activos, se procede a revisar dichos servicios por su naturaleza, versión de software y sistema operativo, en base a vulnerabilidades documentadas.

Pen-Test: las aplicaciones también son revisadas, se realizan pruebas como SQL-injections, pruebas de buffer overflows (BOF), cross-site scripting, entre otras, a fin de evaluar el nivel de seguridad y si es posible obtener información de las bases de datos internas.

Corrección: Recomendar los controles técnicos necesarios para cerrar las vulnerabilidades encontradas para evitar su materialización.



3.2. Métricas: Common Vulnerability Scoring System (CVSS)

La capacidad de valorar las vulnerabilidades de los sistemas es de extrema importancia para los trabajos de análisis de vulnerabilidades. El CVSS es un estándar de la industria en la homologación de los criterios para asignar valor a las vulnerabilidades. El sistema tiene 3 grupos de métricas, cada una dependiente de la anterior:

Métrica Base: Representa la severidad. Una vez descubiertas, analizadas y catalogadas, asumiendo que la información inicial es correcta, hay ciertos aspectos de las vulnerabilidades que no cambian. Estas características centrales no cambian con el tiempo, y tampoco cambian en los diferentes ambientes; para todos los efectos, una vez fijadas, son inmutables. El grupo de métricas base captura estas cualidades constantes, las que son el acceso y el impacto.

Métrica Temporal: Representa la urgencia. Durante el ciclo de vida de una vulnerabilidad, pueden ocurrir ciertos acontecimientos que afectan la urgencia de la amenaza planteada por la vulnerabilidad. Los tres factores que el CVSS procura capturar son: la confirmación de la vulnerabilidad, o de sus detalles técnicos, el estado de remediación de la vulnerabilidad y la disponibilidad del código o técnicas para explotarla. Cada uno de estos factores dinámicos es importante en el ajuste de la urgencia (es decir la prioridad) de una vulnerabilidad en un cierto plazo.

Métrica ambiental: Usada para priorizar respuestas. Diversos ambientes pueden impactar inmensamente en el riesgo que una vulnerabilidad plantea a una organización y a sus accionistas. El grupo de métricas ambientales del CVSS, captura características de las vulnerabilidades que se atan a la puesta en práctica y al ambiente.

4. Resultados obtenidos en. pruebas de caja gris

A continuación se presenta el detalle de las vulnerabilidades identificadas en los servidores/aplicativos Web durante las pruebas de Caja Gris.

Dominios seleccionados para las pruebas:

Dominio	IP Servidor	Descripción de Servidor
http://172.19.235.122:8084/SISER	172.19.235.122	Denominada Sistema Integral de Servicios de AIyPF (SISER AIyPF) donde se realiza la validación, facturación y objeciones para información de grupos terceros.

Dependiendo del tipo de hallazgo se le ha asignado un código de color que representa su valor de acuerdo al "Common Vulnerability Scoring System" (CVSS) con las métricas base, donde:

Alto	valor >= 7.0	
Medio	4.0 >= valor < 7.0	
Bajo	valor < 4.0	

4.1. Sistema web SISER

Nivel de criticidad	Total de Vulnerabilidades encontradas
Alto	1
Medio	3
Bajo	0

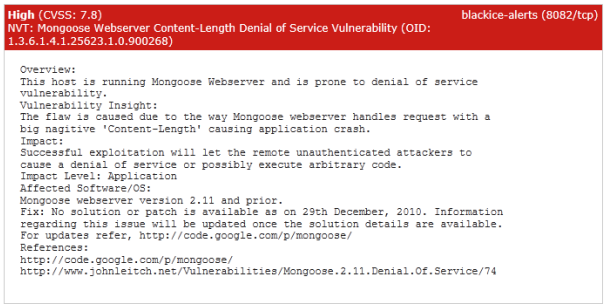
Nivel	Vulnerabilidad	Descripción	Impacto	Recomendación
Alto 7.8	Negación de servicio	La falla se debe a la forma Mangosta servidor web se encarga de solicitud con una variable grande 'Content-Length' aplicación que causa la caída del servidor.	Una explotación exitosa permitirá que los atacantes no autenticados remotos provocaran una negación de servicio	No hay solución o parche está disponible el 29 de diciembre de 2010. Por lo que se recomienda dejar de publicar este servicio
Medio 5.0	Cross-site scripting (XSS).	Consiste en embeber código HTML peligroso en variables que son almacenadas en la base de datos; incluyendo así etiquetas como <script> o <iframe>. Componente afectado:	Modificación visual y funcional del componente vulnerable a través de la ejecución de scripts, permitiendo la modificación visual de la página que podría confundir/engañar al visitante del sitio.	Se recomienda filtrar las variables del componente afectado por medio de funciones a fin de que no se permita la inyección de código malicioso. Para mayor información consultar: https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_%28OWASP-DV-001%29#Countermeasures
Medio 5.0	Cross-site scripting (XSS).	Se está ejecutando un servidor web que no desinfecta adecuadamente las cadenas de solicitud de código JavaScript malicioso. Al aprovechar este problema, un atacante podría ser capaz de causar HTML arbitrario y código script que se ejecutará en el navegador de un usuario dentro del contexto de seguridad del sitio afectado.	Modificación visual y funcional del componente vulnerable a través de la ejecución de scripts, permitiendo la modificación visual de la página que podría confundir/engañar al visitante del sitio	Se recomienda filtrar las variables del componente afectado por medio de funciones a fin de que no se permita la inyección de código malicioso. Para mayor información consultar: https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_%28OWASP-DV-001%29#Countermeasures
Alto 6.8	Apache Tomcat Múltiple Vulnerabilities	De acuerdo con su número de versión auto-reporte, el Apache Tomcat escuchando en el host remoto es anterior a como tal, puede ser afectada por una o más de los siguientes vulnerabilidades: - El servicio remoto puede ser vulnerable a un recorrido de directorio (CVE-2008-5515) - El servicio remoto puede ser vulnerable a una denegación de ataque del servicio si está configurado para utilizar la AJP de Java conector. (CVE-2009-0033) - El servicio remoto puede ser vulnerable a un nombre de usuario ataque de enumeración si se ha configurado para usar el formulario de autenticación junto con la "MemoryRealm ' 'DataSourceRealm', o 'jdbcRealm los reinos de autenticación. (CVE-2009-0580) - El servicio remoto puede ser afectada por una inyección de escritura la vulnerabilidad, si la aplicación de ejemplo de JSP, 'cal2.jsp', está instalado. (CVE-2009-0781)	Un remoto no autenticado, atacante podría aprovechar este problema para inyectar HTML arbitrario o código de script en el navegador de un usuario a se ejecutará en el contexto de seguridad de los afectados sitio	Actualizar a la versión más reciente del servidor Apache Tomcat. Para mayor información: http://tomcat.apache.org/
Nota	El aplicativo cuenta con un inicio de sesión http , por lo que puede ser vulnerable a la intercepción de información sensible como son las credenciales de autenticación, por lo que se recomienda implementa un sistema seguro a través de https			

5. Evidencias

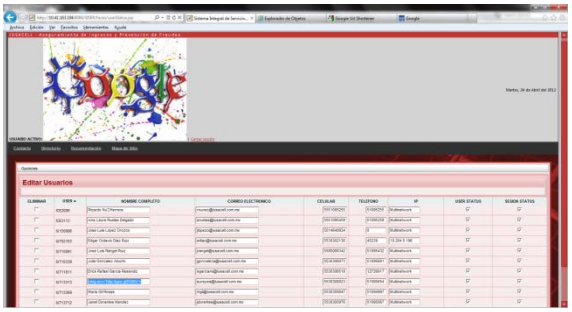
En este apartado se muestran las evidencias de las pruebas anteriormente mencionadas.

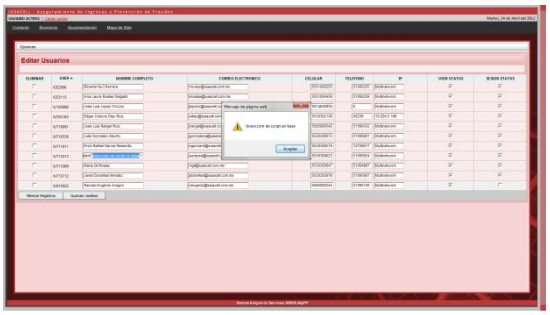
5.1. Dominio: 172.19.235.122:8084/SISER

5.1.1. Negación de servicio



5.1.2. XSS





5.1.3. Apache Tomcat múltiples vulnerabilidades

6. Conclusiones

Derivado del análisis realizado, se puede concluir que la aplicación “SISER” se encuentra en un nivel medio de criticidad, al descubrirse vulnerabilidades que pueden desembocar en la alteración visual y ejecución de código arbitrario así como probable fraude y robo de información confidencial.

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO

GLOSARIO DE TÉRMINOS.

Aplicaciones web: Una aplicación web es cualquier aplicación que es accedida vía web por una red como internet o una intranet, el término también se utiliza para designar aquellos programas informáticos que son ejecutados en el entorno del navegador.

TIC (Tecnologías de la Información y las Comunicaciones): surge como convergencia tecnológica de la electrónica, el software y las infraestructuras de telecomunicaciones. La asociación de estas tres tecnologías da lugar a una concepción del proceso de la información, en el que las comunicaciones abren nuevos horizontes y paradigmas.

AlyPF: Área de Aseguramiento de Ingresos y Prevención de Fraudes perteneciente al grupo Iusacell.

Iusacell: Empresa del remo de las telecomunicaciones.

SISER: Aplicativo web del área AlyPF, para confirmar pagos de y a terceros.

Software: Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Hardware: Es compuesto por todas las partes físicas y tangibles que componen todo el sistema que hace posible el funcionamiento del proceso de datos.

Informática: Proviene del alemán informatik acuñado por Karl Steinbuch en 1957. Y se refiriere a la aplicación de las computadoras para almacenar y procesar la información. Es una contracción de las palabras (información automática).

Middleware: Es la parte de la arquitectura encargada de abstraer a las aplicaciones de los detalles de las plataformas de explotación, mediante las *Application Programs Interfaces (APIs).*

APIS (Interfaz de programación de aplicaciones): *Application Programming Interface* es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

Sistema Operativo (SO): es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, y se ejecuta en modo privilegiado respecto de los restantes.

Cliente/Servidor: La arquitectura cliente-servidor es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes. Un cliente realiza peticiones a otro programa, el servidor, que le da respuesta.

Flujogramas: Es un gráfico que muestra la situación de las interrelaciones de las personas y también de los recursos de la empresa, de una manera clara. Además, es un diagrama de uso más frecuente en sistemas y procedimientos.

Amenaza: Evento con el potencial de afectar negativamente la Confidencialidad, Integridad o Disponibilidad de los Activos de Información.

Vulnerabilidad: Una debilidad que facilita la materialización de una amenaza.

Riesgo: La posibilidad de que una amenaza en particular explote una vulnerabilidad y afecte un activo.

MMC (Modelo de Madurez de Capacidades): *Capability Maturity Model (CMM*), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software.

SEI: (*Software Engineering Institute):* Instituto de Ingeniería de Software, proporciona formación a evaluadores certificados (***Lead Assesors***) capacita.

Aplicaciones de e-business: Es un programa con sustento o no en la web, utilizada para dar soporte a diversas actividades que tu negocio requiera gestionar, este tipo de software no solamente funciona para negocios en línea, sino también para cualquier tipo de negocio tradicional.

Outsourcing: Es La subcontratación o tercerización, es el proceso económico en el cual una empresa mueve o destina los recursos orientados a cumplir ciertas tareas hacia una empresa externa por medio de un contrato.

ITIL (IT Infrastructure Library): Biblioteca de infraestructura de TI = Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

Checklist: Es un listado de procedimientos para la consecución de un objetivo, en este caso, la instalación y correcto funcionamiento de la aplicación a investigar. Además, sirve para ayudar a asegurar la consistencia e integridad en el desarrollo de la tarea, de tal modo, que sea reproducible siguiendo todos los pasos que constituyen el checklist.

.NET: Es un Framework de Microsoft que hace un énfasis en la transparencia de redes, con independencia de plataforma de hardware y que permita un rápido desarrollo de aplicaciones. Basado en ella, la empresa intenta desarrollar una estrategia horizontal que integre todos sus productos, desde el sistema operativo hasta las herramientas de mercado.

PHP Es un lenguaje de programación interpretado (Lenguaje de alto rendimiento), diseñado originalmente para la creación de páginas web dinámicas. Se usa principalmente para la interpretación del lado del servidor pero actualmente puede ser utilizado desde una interfaz de línea de comandos.

Bytecode: Es un código intermedio más abstracto que el código máquina. Habitualmente es tratado como un fichero binario que contiene un programa ejecutable similar a un módulo objeto, que es un fichero binario producido por el compilador cuyo contenido es el código objeto o código máquina.

LISP: Es una familia de lenguajes de programación de computadora de tipo multiparadigma con una larga historia y una sintaxis completamente entre paréntesis.

Programación Multiparadigma: Es el cual soporta más de un paradigma de programación. Según lo describe Bjarne Stroustrup, permiten crear "programas usando más de un estilo de programación". El objetivo en el diseño de estos lenguajes es permitir a los programadores utilizar el mejor paradigma para cada trabajo, admitiendo que ninguno resuelve todos los problemas de la forma más fácil y eficiente posible.

CGI (Common Gateway Interface): Interfaz de entrada común es una importante tecnología de la World Wide Web que permite a un cliente (navegador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el

programa. Es un mecanismo de comunicación entre el servidor web y una aplicación externa cuyo resultado final de la ejecución son objetos MIME.

Rich Internet Applications o RIAs: Aplicaciones de Internet enriquecidas, son aplicaciones web que tienen la mayoría de las características de las aplicaciones de escritorio tradicionales. Estas aplicaciones utilizan un navegador web estandarizado para ejecutarse y por medio de complementos o mediante una máquina virtual se agregan las características adicionales.

Encripción: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.

Framework: Son soluciones completas que contemplan herramientas de apoyo a la construcción (ambiente de trabajo o desarrollo) y motores de ejecución (ambiente de ejecución).

Debuggers: Depurador, es un programa usado para probar y depurar (eliminar los errores) de otros programas. El código a ser examinado puede alternativamente estar corriendo en un simulador de conjunto de instrucciones (ISS).

Hashing: A las funciones hash también se les llama funciones picadillo, funciones resumen o funciones de digest, Una función hash H es una función computable mediante un algoritmo: H: U $\rightarrow$ M x $\rightarrow$ h(x), que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M.

URL *Uniform Resource Locator*: Localizador de recursos uniforme, es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones digitales, etc.

Phishing: Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Malware: Código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Web service: Servicio web es una pieza de software que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet.

Web 2.0: Permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual, a diferencia de sitios web donde los usuarios se limitan a la observación pasiva de los contenidos.

Kernel: En informática, un núcleo o kernel es un software que constituye la parte más importante del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso

seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

Servidor HTTP: Es un programa informático que procesa una aplicación del lado del servidor realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente. El código recibido por el cliente suele ser compilado y ejecutado por un navegador web.

ISS Internet Information Services: Es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Proporcionan las herramientas y funciones necesarias para administrar de forma sencilla un servidor web seguro.

Nmap: Mapeador de redes, es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.

Ecommerce: El comercio electrónico, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas.

Active Server Pages (ASP): Es una tecnología de Microsoft del tipo "lado del servidor" para páginas web generadas dinámicamente, que ha sido comercializada como un anexo a Internet Information Services (IIS).

Testing: Las Pruebas de Software, o "Testing" es una investigación empírica y técnica cuyo objetivo es proporcionar información objetiva e independiente sobre la calidad del producto bajo pruebas a la parte interesada o Stakeholder. Las Pruebas de Software son una actividad más en el proceso de “Aseguramiento de la Calidad”.

Nessus: El escáner de vulnerabilidades Nessus tiene una alta velocidad de descubrimientos, auditoria de configuración, perfilado de activos, descubrimiento de información sensible y análisis de vulnerabilidades del punto de vista de la seguridad de la organización.

OWASP: (Open Web Application Security Project) Es un nuevo tipo de organización. Libre intenciones comerciales, siguiendo un enfoque que permite ofrecer información imparcial, práctica y rentable de la información sobre seguridad de aplicaciones. OWASP no está afiliado a ninguna empresa de tecnología, a pesar de que apoyan el uso informado de tecnologías de seguridad comercial.

BIBLIOGRAFÍA

BIBLIOGRAFÍA.

Referencias Bibliográficas.

Gonzalo Cuevas Agustín: Una Guía del CMM. Para Comprender el Modelo de Madurez de Capacidad del ***Software***. Traducción del Inglés "A Guide to the CMM" de Kenneth M. Dymond. 1998.

Chacón Paredes, Vladimir. El Control Interno como herramienta fundamental contable y controladora de las organizaciones

Gómez, Giovanni E. Manuales de procedimientos y su aplicación dentro del Control Interno

Sergio Luján Mora1), Programación en Internet: clientes Web. Editorial Club Universitario. 2001

Knowlton, Jim, (en español). Python. tr: Fernández Vélez, María Jesús (1 edición). Anaya Multimedia-Anaya Interactiva. 2009.

M. Domínguez-Dorado,. Todo Programación. Nº 1. Págs. 24-26. Editorial Iberprensa (Madrid). DL M-13679-2004. Julio, 2004. Introducción a las aplicaciones web con ASP e IIS.

Andy jones, Debi Ashender. Risk Management for Computer Security

Referencias de Sitios Web.

Sitio web de isaca.org: http://www.isaca.org

Sitio web del Proyecto Apache: http://www.apache.org

OWASP Secure *Software* Contract Annex:

http://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

http://www.owasp.org/index.php/OWASP_Legal_Project

Penetration Testing Framework 0.50.

http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Spring: http://www.springframework.org/

Struts: http://struts.apache.org/

Primefaces: http://primefaces.org/

Richfaces: http://www.jboss.org/richfaces

IceFaces: http://www.icesoft.org/

.Net: http://msdn2.microsoft.com/es-mx/netframework/default.aspx

Axis: http://ws.apache.org/axis/

Ajax – DWR: http://getahead.org/dwr

BPMS: http://soaagenda.com/journal/articulos/que-es-bpm-que-es-bpms/

NMAP: http://nmap.org/man/es/

OPENVAS: http://www.openvas.org/about.html