INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

Modelo de Auditoría en Seguridad para Sistemas de Información

T E S I S

QUE PARA OBTENER EL GRADO DE:
MAESTRO EN INGENIERÍA EN SEGURIDAD
Y TECNOLOGÍAS DE LA INFORMACIÓN.

P R E S E N T A:

ING. AZUCENA SANTIAGO LÓPEZ

ASESOR:

DR. RUBÉN VÁZQUEZ MEDINA

AGRADECIMIENTO AL CONACYT Y AL IPN
POR LAS BECAS DE POSGRADO
QUE ME OTORGARON EN MI PROCESO DE FORMACIÓN

MÉXICO, D. F., ABRIL 2011

SIP-14

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D. F. siendo las 12:00 horas del día 7 del mes de enero del 2011 se reunieron los miembros de la Comisión Revisora de Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULH para examinar la tesis titulada:

"Modelo de Auditoría en Seguridad para Sistemas de Información"

Presentada por el alumno:

Santiago	**López**	**Azucena**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

A	0	9	0	4	7	6

aspirante de:

MAESTRÍA EN INGENIERÍA EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

Después de intercambiar opiniones, los miembros de la Comisión manifestaron ***APROBAR LA DEFENSA DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director de tesis

Dr. Rubén Vázquez Medina

Dr. Héctor Manuel Pérez Meana

Dr. Miguel Cruz Irisson

Dr. José de Jesús Vázquez Gómez

Dr. César Jalpa Villanueva

INSTITUTO POLITÉCNICO NACIONAL ESTADOS UNIDOS MEXICANOS S.E.P. SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION ESIME CULHUACAN

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Gonzalo Isaac Duchen Sánchez

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, DF. el día 28 del mes Marzo del año 2011, el (la) que suscribe Azucena Santiago López alumno (a) del Programa de Maestría en Ingeniería en Seguridad y Tecnologías de la Información con número de registro A090476, adscrito a SEPI-ESIME CULHUACAN, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección del Dr. Rubén Vázquez Medina y cede los derechos del trabajo intitulado Modelo de Auditoría en Seguridad para Sistemas de Información, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección asantiagol0800@ipn.mx. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Ing. Azucena Santiago López

Nombre y firma

AGRADECIMIENTOS

Agradezco a mi alma mater, el Instituto Politécnico Nacional y muy en especial a la Sección de Estudios de Posgrado e Investigación de la ESIME Culhuacán, por darme la oportunidad de pertenecer a la primera generación de la Maestría en Ingeniería en Seguridad y Tecnologías de la Información.

Agradezco infinitamente al Dr. Rubén Vázquez Medina, por su valioso tiempo, dedicación, compromiso, experiencia, consejos y apoyo. Gracias Rubén por toda la confianza brindada.

Agradezco a mis sinodales por tomarse el tiempo para revisar mi tesis y enriquecer mi trabajo con sus valiosos comentarios y observaciones, muy en especial al Dr. Jesús Vázquez por sus valiosas observaciones.

Agradezco a mis padres y a mis hermanos, por apoyarme en cada una de mis decisiones, por engrandecer cada uno de mis pequeños pasos, por su infinito amor, dedicación y paciencia, gracias por creer en mí y sobre todo, gracias por ser mi soporte, guía, luz y ejemplo a seguir.

Agradezco infinitamente a mis amigos y a todas las personas que confiaron en mí y que siempre me alentaron para lograr mis sueños. Gracias pollito, gracias Bob por ser parte de mi familia, los amo.

Y finalmente, aunque no menos importante, quiero agradecer infinitamente a Dios y a la vida, por lo bondadosos que ha sido conmigo. Gracias por ponerme en el lugar, momento y con las personas indicadas.

RESUMEN

El activo más importante dentro de cualquier organización es la información, a través de su procesamiento se puede crear valor y se puede contribuir al logro de objetivos organizacionales. Por ello, las organizaciones, como parte de sus procesos de negocio, crecimiento e innovación, adquieren tecnologías que apoyen el procesamiento de información y la toma de decisiones, así como la automatización de sus procesos de negocio. Muchas organizaciones adquieren tecnología de software, aplicaciones diseñadas a la medida, mediante consultores informáticos especializados, quienes emplean diversos modelos y metodologías de ciclo de vida de desarrollo de software para concebir el Sistema de Información (SI) especificado.

Generalmente, los desarrolladores de aplicaciones orientan su tiempo, conocimientos, recursos y esfuerzo a la funcionalidad especificada, sin considerar a la par, la implementación de controles de seguridad en sus desarrollos. Dejan la fase de validación de seguridad para el final y la mayoría de los casos es independiente al proceso de desarrollo. Con este proceder es una tarea difícil establecer un nivel determinado de seguridad en los sistemas que se desarrollan. Esta situación genera incertidumbre en las organizaciones propietarias de los SI, pues sus SI interactúan con otros sistemas a través de las redes de datos, lo cual generalmente pone en evidencia un conjunto de vulnerabilidades propias del SI.

Para los dueños de los SI, especialistas en informática, desarrolladores y auditores de seguridad de la información debe ser importante contar con un mecanismo que les permita tener un grado de certeza en la seguridad de sus SI. En este trabajo se propone que para un SI, desarrollado o adquirido, debe considerarse como prioridad cumplir no solo con los requisitos funcionales, sino también con requisitos mínimos de seguridad.

A lo largo de este trabajo se abordan dos opciones para dotar de seguridad a los SI: la primera (a priori), que sugiere la adopción de una metodología que considere el ciclo de vida de desarrollo seguro, La segunda opción (a posteriori), sugiere el uso de un modelo de auditoría de seguridad de SI, el cual garantice que las aplicaciones desarrolladas cuenten con los controles necesarios que

reduzcan la vulnerabilidad típica de las aplicaciones. Se pretende que estas dos opciones en el aseguramiento de un SI sirvan como recomendaciones para reducir su riesgo y vulnerabilidad.

Finalmente este trabajo define la alternativa más viable, no con ello afirmando que sea la mejor para dotar de seguridad a los SI, la opción de adoptar un modelo de auditoría de SI. Partiendo de ello, se realiza la propuesta de un modelo de auditoría de seguridad de SI y para apoyar la adopción de este modelo dentro de cualquier organización, se define una metodología y un conjunto de Procedimientos Operativos Estándar.

ABSTRACT

The most important asset within any organization is information. Through its processing, creating value and achieving organizational goals can be done. Therefore, the organizations, as part of their business processes, growth and innovation, acquire technologies that hold the information processing, the decision making and the automating of their business processes. Many organizations obtain software technology and custom-designed applications by specialist computer consultants, who use several Software Development Life Cycle (SDLC) models and methodologies to design the specific information system (IS).

Generally, the application developers focus their time, knowledge, resources and effort to the specified functionality, and forgetting at the same time, the implementation of security controls in their development. The most part of the time, the security validation is the last phase that is considered or even, it´s insolated to the development process. Given this situation, it´s a hard task to establish a specific security level to the systems that are developed. In this case, uncertainty is created in the organizations that own the IS, due to their IS interact with other systems via data-network, which reveals a set of vulnerabilities associated of the IS.

For the IS owners, computer specialists, developers and security information auditors, should be important to have a mechanism that allows them to have a security certainty degree of there IS. In this paper, it is proposed that for IS, developed or acquired, should be considered as a priority not only meet the functional requirements but also with minimum safety requirements.

Throughout this paper examines two options for providing security to the IS: the first (a priori), which suggests the adoption of a methodology that considers the life cycle of safe, the second option (a posteriori) suggests using a model of IS security audit, which ensures that applications developed have the necessary controls to reduce the typical vulnerability applications. It is intended that these two options in securing a IS will serve as recommendations to reduce risk and vulnerability.

Finally, this paper identifies the most viable alternative, not saying that this is the best for providing security to the IS, the option of adopting a model of audits. On this basis, the proposal is made of a model of IS security audit and to support the adoption of this approach within any organization, defines a methodology and a set of Standard Operating Procedures.

ORGANIZACIÓN DE LA TESIS

Esta tesis se encuentra dividida en cinco capítulos. Inicialmente, se incluye una sección donde se definen las bases para desarrollar el trabajo de investigación. En esta se identifica el problema existente, se destaca la importancia por la que debe desarrollarse el proyecto, y se definen los objetivos y alcance del trabajo de tesis.

En el primer capítulo se ofrece un panorama general sobre la situación actual que guardan las organizaciones al adquirir e implementar sistemas de información (SI) como parte de sus procesos productivos. Se presentan las consideraciones actuales dentro del ciclo de vida de los SI, y la importancia de integrar seguridad en cada fase del ciclo de vida de desarrollo del SI. Se presenta un resumen de algunas publicaciones acerca de las vulnerabilidades en los SI y el estado del arte del tema de investigación.

En el segundo capítulo se presentan los conceptos clave, las bases y las definiciones necesarios para el desarrollo de esta tesis. Los temas que abarca este capítulo son: generalidades de los SI y los Procedimientos Operativos Estándar (POE); se definen también los estándares y las mejores prácticas en el desarrollo de SI, auditoría de seguridad de SI y calidad del software. Se ofrecen generalidades de auditoría informática y auditoría de seguridad informática, finalmente se describen las metodologías de auditoría informática.

El tercer capítulo aborda la importancia de que los SI nazcan seguros; es decir, se enfatiza en que se debe pasar de un enfoque en el que la seguridad es la parte final del proceso de implantación del SI, a un enfoque en el que la seguridad es parte integral del proceso de desarrollo, donde en cada etapa del ciclo de vida se incluyen las consideraciones necesarias para dotar a la aplicación de seguridad desde su nacimiento. Los puntos que se incluyen en este capítulo son: El ambiente de operación en el que se diseñan, desarrollan e implementan los SI, se presentan 2 metodologías de desarrollo seguro y los principales retos en la implementación y adopción de un ciclo de vida de desarrollo de software seguro.

En el capítulo cuatro se presentan los requerimientos funcionales y de seguridad que los SI deben cumplir. Los requerimientos funcionales se enfocan en que el SI cumpla con el objetivo para el que fue diseñado, mientras que los requerimientos de seguridad se enfocan en que el SI cuente con una seguridad mínima, la cual debe ser congruente con los requerimientos funcionales y con las necesidades de seguridad de la organización. En el mismo sentido, se presentan las

consideraciones necesarias para determinar el cumplimiento de los requerimientos funcionales y de seguridad; es decir, el grado en que el SI cumple con los requerimientos especificados en su concepción. De igual manera, se incluye una lista de los errores de programación más graves en los SI, errores de los que un SI auditado debe estar libre. Finalmente, se concluye el capítulo con una lista de las consideraciones de los requisitos mínimos funcionales y de seguridad que se deben abordar en una auditoría de SI.

Finalmente, el quinto capítulo describe el modelo de auditoría resultado de esta tesis, el cual estará orientado a revisar la existencia y suficiencia de los requerimientos funcionales y de seguridad presentados en el capítulo 4. Para implementar el modelo de auditoría de seguridad propuesto, se establece una metodología para auditar la seguridad de un SI y un conjunto de POEs que apoyan el proceso de auditoría. En ese sentido, se presenta un conjunto de recomendaciones generales propuestas para implementar este modelo de auditoría. Se concluye con una aproximación de la aplicación del modelo de auditoría en los SI organizacionales.

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

PLANTEAMIENTO DEL PROBLEMA

La información es un recurso vital para toda organización, y el buen manejo de esta puede significar la diferencia entre el éxito o el fracaso, para todos los proyectos que se emprendan dentro de una organización. De lo anterior, se deriva la creciente adquisición por parte de las organizaciones, de nuevas tecnologías que apoyen al procesamiento de información, automatización de procesos y de apoyo en la toma de decisiones.

La mayoría de las organizaciones, realizan la adquisición de tecnología de software (aplicaciones), mediante el apoyo de consultores Informáticos especializados, los cuales mediante diversas metodologías, realizan un análisis de requerimientos, diseño del sistema, desarrollo de aplicaciones, pruebas unitarias e integrales de la funcionalidad de las aplicaciones, implementación del sistema, y finalmente, el mantenimiento y apoyo a las aplicaciones.

Comúnmente, los desarrolladores de estas aplicaciones se enfocan y orientan su tiempo, conocimiento y esfuerzo por desarrollar la funcionalidad especificada, sin considerar a la par, la implementación de controles de seguridad en sus desarrollos. Los desarrolladores dejan la fase de validación de seguridad para el final. Erróneamente, este proceso de revisión de la seguridad en las aplicaciones, se lleva de manera independiente al código. De lo anterior se deriva que, para los desarrolladores es una tarea difícil establecer un nivel determinado de seguridad en los sistemas que desarrolla, ya que la gran mayoría sólo se preocupa por que sus aplicaciones sean funcionales; aunque esto no implica que se sigan medidas de seguridad básicas para defenderse de diversos ataques. Esta situación genera gran incertidumbre a las organizaciones propietarias de los sistemas de información.

El tema que se pretende abordar, responderá a las siguiente pregunta: ¿Cómo se asegurará el desarrollador y los dueños de los SI, que sus aplicaciones tienen los requisitos mínimos de seguridad y cumplen con el nivel de seguridad adecuado para preservar la integridad, disponibilidad y confidencialidad de la información que en ellos se maneja?

HIPÓTESIS

Existen 2 maneras mediante las cuales tanto desarrolladores como propietarios de los SI pueden asegurar que sus aplicaciones cumplen con los requisitos mínimos de seguridad:

- La primera, de manera a priori; mediante la adopción de una metodología de Ciclo de Vida de Desarrollo seguro[1], la cual sea un modelo a seguir en el proceso de desarrollo de aplicaciones en una organización[2]; y

- La segunda de manera a posteriori, mediante el uso de un modelo de auditoría de seguridad de SI, el cual garantice que las aplicaciones desarrolladas y/o adquiridas cuentan con los controles necesarios que reduzcan las típicas vulnerabilidades de las aplicaciones y de igual manera sirva de apoyo al emitir recomendaciones de seguridad para reducir el riesgo y vulnerabilidad encontrada en la auditoría de los SI.

[1] Modelo de desarrollo de software seguro que considera e implementa acciones de seguridad en cada una de las etapas del Ciclo de Vida de desarrollo de software.

[2] En el mantenimiento de SI, se debería aplicar (en el esquema a priori) el mismo modelo a los nuevos elementos de SI agregados, modificados o sustituidos.

OBJETIVO GENERAL

Elaborar un modelo de auditoría en seguridad para los Sistemas de Información (SI) antes de su puesta en operación, el cual permita, tanto a desarrolladores como a propietarios, conocer y dar cierto grado de certeza en la seguridad de los SI desarrollados, y garantizar que los SI auditados cumplen con los requisitos mínimos de seguridad y están listos para su puesta en operación.

OBJETIVOS ESPECÍFICOS

- Entender el ciclo de vida de desarrollo de aplicaciones y sistemas de información.
- Revisar los documentos de estándares y mejores prácticas relacionados con la auditoría en seguridad a SI.
- Conocer los Procedimientos Operativos Estándar (POE) y entender cómo se pueden aplicar en la auditoría de sistemas de información
- Realizar un comparativo entre diversos estándares para determinar los requisitos mínimos de seguridad de un SI.
- Establecer los requisitos mínimos funcionales y de seguridad que deben cumplir los SI antes de ser puestos en operación.
- Establecer un conjunto de POE´s que apoyen a la metodología de auditoría en seguridad para SI propuesta.
- Elaborar un POE orientado a la auditoría de seguridad de SI.
- Proponer una metodología de auditoría en seguridad para SI que apoye la implementación del modelo de auditoría en seguridad de SI propuesto.
- Realizar una aproximación del modelo de auditoría de seguridad de SI propuesto.
- Publicar resultados en congresos nacionales.

ALCANCE

El modelo propuesto para auditar la seguridad en los Sistemas de Información (SI), pretende servir de guía para:

- Evaluar y conocer el nivel de seguridad que tienen las aplicaciones desarrolladas.
- Identificar las vulnerabilidades típicas en los SI.
- Identificar los requerimientos mínimos que un SI debe incluir antes de ser puesto en operación.
- Identificar los requerimientos mínimos de seguridad de las aplicaciones.
- Establecer características de Calidad en las aplicaciones, basadas en estándares y mejores prácticas.
- Emitir recomendaciones de seguridad para reducir el nivel de riesgo y vulnerabilidades encontradas.

JUSTIFICACIÓN

Hoy en día, se pueden tomar muchas medidas para crear SI seguros, las cuales minimicen el impacto de probables fallas de seguridad y la posibilidad de ataques a las aplicaciones.

Desafortunadamente, aunque empieza a existir una conciencia en el desarrollo de sistemas seguros, las estrategias usadas son poco conocidas y poco aceptadas por los desarrolladores, los cuales solamente consideran la seguridad de los SI en las etapas finales del diseño y no como parte integral del Ciclo de Vida de Desarrollo de Sistemas, tal como describe Jesús Vázquez Gómez en el trabajo desarrollado con el título de 'Inseguridad de los sistemas' en Junio de 2008 **[1]**.

En la mayoría de estos casos la seguridad es considerada como una corrección a los desarrollos en operación, después de detectarse algún problema. En este sentido la empresa estadounidense Cenzic, proveedor de soluciones de seguridad en aplicaciones Web, publica semestralmente su informe de tendencias en seguridad de aplicaciones Web **[2]**. En el informe correspondiente al segundo semestre de 2009, mediante el análisis de reportes de vulnerabilidades de fuentes estadounidenses como el NIST (National Institute of Standards and Technology), MITRE Corporation, SANS (SysAdmin, Audit, Network, Security), US-CERT (United States Computer Emergency Readiness Team), OSVDB (The Open Source Vulnerability Database), así como bases de datos de terceros para las cuestiones de seguridad de aplicaciones Web, Cenzic logró identificar un total de 2,165 vulnerabilidades en aplicaciones comerciales, lo cual corresponde al 82 % del total de vulnerabilidades publicadas de 2,650.

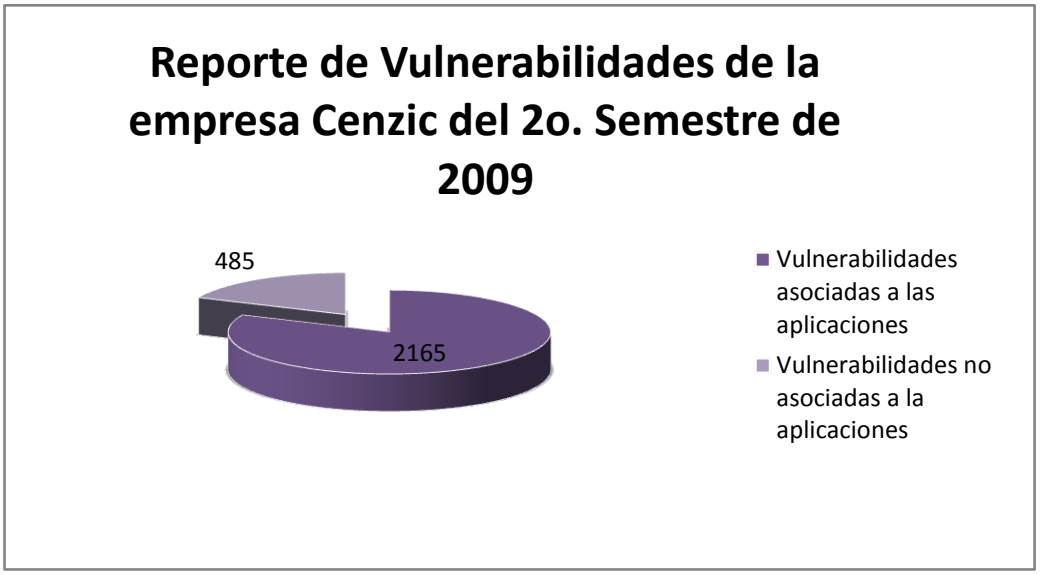


Fig 1. Reporte de vulnerabilidades de la empresa Cenzic correspondiente al 2º. Semestre del 2009.

De lo anterior, se deriva la importancia de proveer un modelo de procedimiento de auditoría para efectuar una revisión integral de seguridad en:

- Aplicaciones que están próximas a ser liberadas y puestas en producción; a nuevas aplicaciones y a cambios en las versiones productivas, las cuales no implementan la seguridad en el ciclo de vida de desarrollo de sus aplicaciones;

- Aplicaciones desarrolladas bajo un enfoque considerando, el ciclo de vida de desarrollo de Software Seguro.

- Aplicaciones que ya se encuentran en operación, para garantizar que los controles de seguridad implementados son eficientes a través del tiempo.

Se espera que esto permita garantizar que las aplicaciones cumplan con los requisitos mínimos de seguridad y que son aptas para minimizar el impacto causado por fallos, violaciones o alteraciones que se pudieran llegar a efectuar sobre dichas aplicaciones.

Se establece la clasificación anterior, porque se pretende que este modelo de procedimiento pueda apoyar a las áreas de sistemas, desarrolladores y propietarios; así como conocer, concientizar y adoptar un nuevo enfoque en el desarrollo de SI.

Se pretende que este modelo de procedimiento de auditoría valide que las aplicaciones desarrolladas cuentan con los controles necesarios que reduzcan las típicas vulnerabilidades de las aplicaciones.

CAPÍTULO 1: MARCO CONTEXTUAL

Resumen

Este capítulo pretende dar un panorama general sobre la situación actual de las organizaciones al adquirir e implementar sistemas de información (SI), como parte de sus procesos productivos. Se revisan las consideraciones actuales dentro del ciclo de vida de los SI y la importancia de integrar seguridad en cada fase de su ciclo de vida y de desarrollo de un SI. De igual manera, se presenta un resumen de algunas publicaciones acerca de las vulnerabilidades de seguridad en los SI. Finalmente, se describe el estado del arte del tema de investigación.

1.1 Sistemas de Información, consideraciones de desarrollo, implementación y seguridad.

Actualmente la mayoría de las organizaciones, como parte de su crecimiento e innovación han incluido, dentro de sus procesos productivos y de toma de decisiones, el uso de SI. Parten de que el activo más importante que tienen es la información y que, a través de su procesamiento, una compañía puede crear valor, y puede contribuir a alcanzar sus objetivos.

Un SI concentra todos los elementos que forman parte de un proceso productivo, se podría decir que un SI es la realización en software de un conjunto de tareas y actividades del mundo real orientados a un objetivo en común. Esta realización incluye parte de la administración, alimentación de información al sistema, procesamiento de datos, transporte de la información generada, formateo y distribución dentro y fuera de la organización.

Últimamente se asocia el crecimiento económico de una empresa con el número de procesos que esta tiene automatizados, y por la inclusión de SI dentro de sus procesos productivos que le permitan automatizar y reducir costos de operación. Por ello, en los últimos años las empresas adquieren cada vez más SI. En este sentido, en el artículo "La inversión en Tecnologías de la Información crecerá a nivel mundial un 4.6 por ciento en 2010 " publicado en enero de 2010 **[3]**, Martín Pérez hace una investigación acerca de la inversión de los mercados de TI y con respecto a la adquisición de software, comenta que el gasto en software va a experimentar un crecimiento de 4.9%, alcanzando los 231,500 millones de dólares a nivel mundial. Por otro lado, SoftServe, proveedor de desarrollo de software, en una encuesta entre abril y junio de 2009 realizada a más de 6,000 ejecutivos y profesionales de desarrollo de software, muestra un incremento del 10% en los presupuestos de desarrollo **[4]**. La encuesta puso de manifiesto que el 60% de los participantes afirman haber observado un incremento en los desarrollos de software para 2009. Concretamente un 36% de los encuestados indicaron que los presupuestos se han incrementado un 10% respecto los gastos de 2008. Taras Kytsmey, presidente de SoftServe afirma en el informe que "incluso en medio de la incertidumbre y la confusión económica, la mayoría de las compañías escogen invertir más, y no menos, en iniciativas de desarrollo de software de misión crítica para fortalecerse".

Comúnmente se habla de una clasificación de los SI por parámetros como los objetivos que persiguen, o la funcionalidad que estos implementan. Para cualquiera de las clasificaciones de los SI, una decisión importante a considerar, es la forma en que la organización adquirirá el sistema de información.

Al adquirir un SI se pueden encontrar 2 tipos de aplicaciones:

- aplicaciones comerciales y
- aplicaciones diseñadas a la medida.

Las aplicaciones comerciales, incluido las de código abierto (Opensource), dentro de sus funciones aportan un comportamiento global del proceso que automatizan; es decir, parten y se crean de la totalidad de funciones posibles del proceso. Lo anterior conlleva a que, al adquirir una aplicación comercial, será necesario definir parámetros dentro de las funciones que integran a la aplicación (personalizar, parametrizar el SI que se ha adquirido). Además, cuando se adquieren aplicaciones comerciales muchas de sus funciones son desaprovechadas por la organización, ya sea porque no se alinean a la cultura organizacional o porque simplemente el modelo de negocio no lo requiere. Por otro lado, las aplicaciones diseñados a la medida, dan la certeza de que el SI adquirido, refleja en su totalidad el proceso que automatiza; es decir, la funcionalidad se diseña única y exclusivamente para los requerimientos del negocio para el que ha sido concebido. Esto genera un mejor aprovechamiento de recursos, procesos alineados al negocio y aseguramiento por parte de la organización de que el SI que les ha sido entregado cumple en un 100% con las expectativas funcionales, de negocio y requerimientos especificados, además de proveer una aplicación exclusiva para la organización. También ha aumentado el número de adquisiciones de SI´s, tanto comerciales como desarrollados a la medida.

Día tras día los técnicos y especialistas más experimentados desarrollan distintas innovaciones en los aspectos de seguridad de SI, para que éstos sean lo menos vulnerable posible, tratando de evitar todo aquello que pueda afectar el funcionamiento de un sistema. El concepto de seguridad informática sigue siendo, para varios, de carácter utópico, ya que no se ha revelado en la actualidad un sistema que pueda ser 100% seguro. Morrie Gasser en su libro "Building a Secure Computer System" **[5],** describe que "A pesar de los avances significativos en el estado del arte de la seguridad informática, en los últimos años, la información en las computadoras es más vulnerable que nunca. Cada avance tecnológico importante en informática plantea nuevas amenazas de seguridad que requieren nuevas soluciones, la tecnología avanza más rápido que la velocidad con la que este tipo de soluciones se desarrollan…". "Probablemente no podamos cambiar la manera en que funciona el mundo, pero si entender por qué funciona de esa manera, lo que nos puede ayudar a evitar las fallas típicas y optar por soluciones de seguridad aceptables".

El aumento de riesgos en los SI que, en ocasiones, pueden ser críticos, pone en riesgo a la información organizacional y afectan la continuidad del negocio.

Actualmente, la seguridad en las aplicaciones se lleva como una parte independiente; las organizaciones se preocupan por invertir en seguridad perimetral que les proporcione algún grado de certeza de que su infraestructura informática está protegida. El error en esta concepción e implementación de seguridad se deriva de que la mayor parte de las vulnerabilidades se encuentra en el diseño de las propias aplicaciones, no en su infraestructura. En el artículo "The Top Cyber Security Risks" publicado en el portal de SANS en Septiembre de 2009 **[6]**, se hace alusión al punto anterior y se resume en la figura 2.

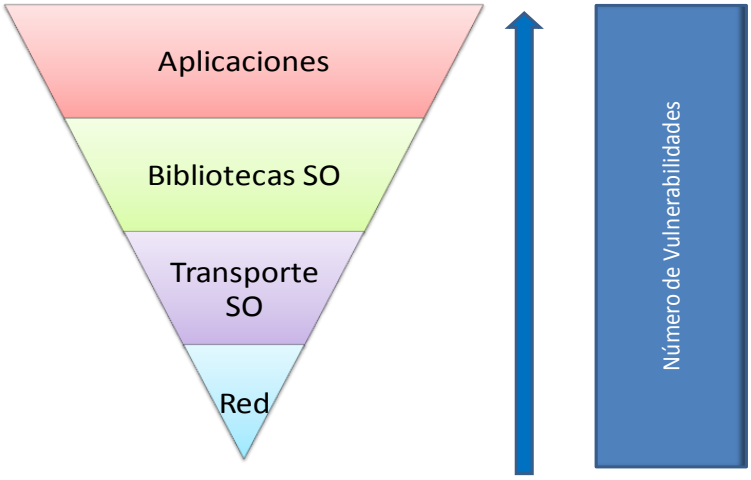


Fig 2. Número de Vulnerabilidades en Red, SO y aplicaciones.

1.2 Cifras relevantes de los Sistemas de Información y seguridad.

La seguridad en las aplicaciones se ha vuelto una prioridad, afortunadamente las organizaciones ya están tomando conciencia de ello. Cada vez más y más portavoces se unen a esta nueva visión de aplicaciones seguras independientes de la infraestructura de seguridad que implementan **[7]**.

A continuación se presenta una selección de artículos, publicados por organizaciones y revistas internacionales, las cuales muestran aspectos relacionados con las vulnerabilidades de las aplicaciones.

Urgen a proteger aplicaciones Web.

Carlos Fernández de Lara, publicó el artículo 'Urgen a proteger aplicaciones Web' en la revista Netmedia en Noviembre de 2009, en el marco del congreso 5º Día de la Seguridad de la Información, organizado por la Secretaría de Hacienda y Crédito Público (SCHP) **[7]**. El autor resalta las siguientes declaraciones hechas por Ariel Sucari, gerente de la Consultora Itera:

"Con el crecimiento acelerado de los servicios de Internet, las empresas y responsables de la seguridad IT deben comenzar a priorizar proteger las aplicaciones Web y no exclusivamente los servidores e infraestructura del negocio".

"Las empresas tienen que establecer esquemas de protección con base en la ubicación de sus datos sensibles, con políticas de control y manejo de riesgos y con un análisis profundo para determinar los puntos rojos en temas de vulnerabilidades".

"La protección de las aplicaciones Web se coloca como uno de los vectores más urgentes y olvidados en términos de vulnerabilidades y resguardo, por parte de las organizaciones".

"Diversos análisis muestran que 54.9% de las aplicaciones Web cuentan con vulnerabilidades o riesgos potenciales. Peligros que en el 74% de los casos no han sido solucionados luego de un año de estar expuestos".

"El total de los ataques a las organizaciones, 75% van dirigidos a las aplicaciones Web y el resto a la infraestructura de red y servidores de la empresa. Sin embargo, irónicamente 90% del presupuesto de seguridad IT se invierte en reforzar la

infraestructura en servidores y, únicamente 10% se gasta en mejorar la protección de las aplicaciones Web".

"Las empresas no están enfocando la seguridad hacia sus aplicaciones Web, a pesar de que siete de cada diez ataques están dirigidos a sus servicios en Internet. El tema no es dejar de proteger la infraestructura, pero es necesario comenzar a mirar nuevos vectores de riesgo".

"La seguridad en las aplicaciones Web debe comenzar desde su gestación, pues el 64% de los programadores en las compañías desconocen cómo escribir códigos y programas sin errores o vulnerabilidades".

"La seguridad es problema de todos, desde los departamentos de seguridad IT, los programadores de las herramientas, hasta los usuarios que las utilizan. Definir de antemano procesos, responsables por área, tiempos de despliegue y de ejecución puede ahorrar muchos problemas y riesgos para el negocio".

Fallas importantes tienen 9 de 10 aplicaciones.

La empresa estadounidense Cenzic, proveedor de soluciones de seguridad en aplicaciones Web, publica semestralmente su informe de tendencias en seguridad de aplicaciones Web. El informe correspondiente al primer semestre de 2009, lleva por título "Web Application Security Trends Report Q1-Q2, 2009" publicada en Noviembre de 2009**[8]**. En este informe, se afirma que la información de las organizaciones está en riesgo, ya que casi 9 de 10 aplicaciones Web tienen vulnerabilidades que pueden ser explotadas en cualquier momento. Específicamente, Cenzic encontró que de las aplicaciones Web analizadas 87% tienen serias vulnerabilidades que potencialmente pueden ocasionar la exposición de la información sensible o datos confidenciales producto de transacciones de compradores en línea. En el mismo sentido, Cenzic afirma que el 90% de las vulnerabilidades de las aplicaciones Web se encuentran en aplicaciones comerciales y solo 8% en los navegadores que las corren.

Las vulnerabilidades de aplicaciones exceden las Vulnerabilidades de los SO.

Cada vez se da más importancia a proteger las aplicaciones, basándose en el hecho de que las vulnerabilidades en las aplicaciones exceden a las vulnerabilidades de los Sistemas Operativos, tal como se describe en el artículo "The Top Cyber Security Risks" publicado en el portal de SANS[3] en Septiembre de 2009 **[6]:**

"Durante los últimos años, el número de vulnerabilidades descubiertas en las aplicaciones es mucho mayor que el número de vulnerabilidades descubiertas en los sistemas operativos. Como resultado, se han registrado más intentos de explotación a los programas de aplicación...".

[3] SysAdmin, Audit, Network, Security

Evaluaciones de vulnerabilidades en los SI

Con respecto a las vulnerabilidades de los sistemas de información, Joseph Feiman en el trabajo titulado "Building Secure Applications" **[9]**, realizó un análisis y detectó que las vulnerabilidades de los SI son concebidos desde las primeras etapas del ciclo de vida de los mismos, el porcentaje que le dio a la inserción de vulnerabilidades por cada etapa del ciclo de vida de desarrollo se puede apreciar en la tabla 1.

Vulnerabilidades encontradas en cada etapa del Ciclo de vida de desarrollo de Software (CVDS)			
Vulnerabilidades encontradas	**Fases CVDS**	**Madurez de herramientas y prácticas**	**Aportación de vulnerabilidades****
Vulnerabilidades en la toma de requerimientos, definición de flujos de procesos de negocio y algoritmos.	Análisis	En desarrollo	15%
Vulnerabilidades causadas por interrelaciones de módulos y servicios (Web), lógica y flujo de datos.	Diseño	En desarrollo	40%
Vulnerabilidades en las instrucciones propias del lenguaje, implementación de la lógica y flujo de datos	Construcción	Bajo	35%
Vulnerabilidades en ejecutables, interfaz de usuario. Montaje de servicios de seguridad	Pruebas	Bajo	10%
Falta de actualizaciones, errores administrativos, errores de configuración. Si se encuentran vulnerabilidades se regresa al análisis.	Operación	Bajo-Medio	

Tabla 1.- Evaluación de vulnerabilidades en las distintas fases del Ciclo de Vida de Desarrollo de Software CVDS.

Como se puede observar en la tabla 1, el mayor porcentaje de vulnerabilidades en el Software es insertado en las etapas de diseño y desarrollo. Y esto se debe en gran parte a que los diseñadores y desarrolladores de software enfocan su tiempo, conocimiento, recursos y esfuerzos en diseñar y desarrollar la funcionalidad especificada en el tiempo y forma especificada; sin tomar a la par

** Las vulnerabilidades aportadas en cada fase, pueden aunque no son necesariamente vulnerabilidades de seguridad. Dentro de cada fase del CVDS pueden agregarse también vulnerabilidades de negocio o funcionales, es decir que no se logre conceptualizar las necesidades reales del negocio, como suele suceder en las etapas de análisis y diseño.

consideraciones mínimas de seguridad y mejores prácticas en el desarrollo de software.

La mayoría de las veces las deficiencias encontradas resultan de un mismo origen, el desconocimiento de las implicaciones y prácticas de seguridad por parte de los equipos de trabajo. Es decir, no se planea, diseña y programa pensando en seguridad.

Lo anterior ha impactado en que los SI se hayan convertido en el blanco preferido por los atacantes, debido a que el mayor número de vulnerabilidades encontradas en estos SI, son vulnerabilidades ya conocidas, explotadas, documentadas y ampliamente difundidas.

Por ello, surge la necesidad de no conformarnos solamente con la seguridad perimetral a la que actualmente se encuentran sometidos los SI en la organización, sino ir más allá, es decir no confiar plenamente en los mecanismos de seguridad externos y optar por fortalecer a los SI desde su creación.

El presente trabajo de tesis proporciona una alternativa de perfeccionamiento de los SI antes y durante su puesta en operación, mediante la cual tanto desarrolladores y propietarios de los SI pueden asegurar que sus aplicaciones cumplen con los requisitos mínimos de seguridad y que los controles implementados reducen las típicas vulnerabilidades de las aplicaciones.

1.3 Estado del arte

La mayor parte de las investigaciones existentes conforme al desarrollo de Sistemas de Información Seguros y a la auditoría de Seguridad de los Sistemas de Información, se ven reflejados en un conjunto de estándares y mejores prácticas utilizadas en la actualidad. Las de mayor aceptación y que se toman como base para el desarrollo de esta tesis son los siguientes:

ISO/IEC 15408: Define un criterio estándar para la evaluación de las propiedades y características de seguridad de determinado producto o sistema informático. Proporciona un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto con base en el conjunto de requisitos de seguridad y garantía que satisface respecto a esta norma, obteniendo de esa forma una certificación oficial de nivel de seguridad que satisface.

ISO 9126: Es un estándar internacional para la evaluación del Software. Está dividido en cuatro partes: modelo de calidad, métricas externas, métricas internas y calidad en las métricas de uso. Este estándar está pensado para los desarrolladores, adquirentes, personal que asegure la calidad y evaluadores independientes, responsables de especificar y evaluar la calidad del producto software. Se ocupará como base del modelo de auditoría de seguridad propuesto en esta tesis.

ISO 12207: Establece un marco de referencia común para los procesos del ciclo de vida software, con una terminología bien definida, que puede ser referenciada por la industria software. En este marco se definen los procesos, actividades (que forman cada proceso) y tareas (que constituyen cada Actividad) presentes en la adquisición, suministro, desarrollo, operación y mantenimiento del software.

NIST SP800-64: Emitido por el Instituto Nacional de Estándares y Tecnologías de EUA (NIST, por sus siglas en inglés). Aborda el tema de consideraciones de seguridad en el ciclo de vida de desarrollo de SI. Presenta un capítulo exclusivo para la incorporación de la seguridad dentro del ciclo de vida de desarrollo de SI. Este documento servirá de base para desarrollar el tema de ciclo de vida de desarrollo seguro.

NIST SP800-37 (versión anterior): Emitido por el Instituto Nacional de Estándares y Tecnologías de EUA (NIST, por sus siglas en inglés). Es una guía para la certificación y acreditación de seguridad de los Sistemas de Información Federales. El propósito de esta publicación es proporcionar las directrices y tareas necesarias

para cada una de las fases en el proceso de certificación y acreditación de la seguridad para los sistemas de información federales.

COBIT (Objetivos de Control de la Tecnologías de la Información): Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, por sus siglas en inglés), y el Instituto de Gobierno de Tecnologías de la Información (ITGI[4], por sus siglas en inglés). COBIT ofrece a directivos, auditores y a usuarios de TI un conjunto de medidas de aceptación general, indicadores, procesos y mejores prácticas para asistirlos a maximizar los beneficios procedentes de la utilización de TI y el desarrollo adecuado gobierno de TI y control en una empresa. COBIT 4.1 se conforma de 34 procesos de alto nivel, los cuales cubren 210 objetivos de control clasificados en 4 dominios: Planear y Organizar, Adquirir e implantar, Entrega y Soporte, y Monitorear y Evaluar. Se aprovechará esta base para desarrollar los temas de capítulo 4 y 5 de esta tesis.

ISO 27002: Se conforma como un código internacional de buenas prácticas de seguridad de la información. Puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad. Se aprovechará para desarrollar el tema de requerimientos de auditoría de seguridad de los SI.

Manual de Metodología Abierta de Evaluación de Seguridad (OSSTMM, por sus siglas en inglés). Es el documento de una metodología Abierta de evaluación de seguridad emitido por el Instituto para la seguridad y metodologías abiertas (ISECOM, por sus siglas en inglés). Es un conjunto de reglas y lineamientos para determinar cuándo, qué y cuáles eventos deben ser evaluados. Esta metodología cubre únicamente la prueba de seguridad externa, es decir, evaluar la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado. El objetivo de este manual es crear un método aceptado para la realización de pruebas de seguridad en profundidad.

Guía de Pruebas OWASP[5]. Es una metodología Abierta para realizar pruebas de penetración a aplicaciones Web, emitida por la organización OWASP. Esta guía incluye las "mejores prácticas" de pruebas de penetración para ser aplicadas

[4] IT Governance Institute, es una entidad sin fines de lucro, de investigación independiente que proporciona orientación a la comunidad mundial de negocios sobre temas relacionados con el gobierno empresarial de los activos de TI. El ITGI fue establecido en 1998 por ISACA, asociación de miembros sin fines de lucro.

[5] Open Web Application Security Project

tanto a nivel de empresa como a nivel de proyecto de desarrollos de software orientados a la Web.

Publicaciones e Investigaciones

Se han publicado una serie de documentos que apoyan e inducen a los lectores a optar por una construcción de aplicaciones seguras. Entre ellos se pueden encontrar las siguientes:

"Building Secure Applications", publicado en el año 2007 por Joseph Feiman y soportado por la firma internacional, Gartner. Presenta un artículo de 17 hojas en las que introduce a las aplicaciones seguras; su teoría se basa en que las vulnerabilidades de los SI se conciben desde las primeras etapas del ciclo de vida del mismo. Provee de la misma manera, un estudio de las vulnerabilidades más comunes en los SI y la perspectiva de SI entre los desarrolladores y los expertos de seguridad.

"A Guide to Building Secure Web Applications and Web Services", publicada en 2002 por OWASP. El proyecto OWASP es una comunidad abierta de colaboración entre profesionales y expertos en la seguridad de aplicaciones Web. Entre sus muchos proyectos se incluye la Guía de pruebas, un manual de referencia con vulnerabilidades, contramedidas y una completa metodología para la revisión y evaluación del estado de seguridad de las aplicaciones. El marco de trabajo descrito en este documento pretende alentar a las personas a evaluar y tomar medidas de seguridad a través de todo el proceso de desarrollo.

"Elaboración de un modelo de ciclo de vida para el desarrollo de sistemas de información basados en WEB", tesis elaborada por Carlos León Martínez Valle, y publicada en Junio 2006 para obtener el título de Maestro en Ciencias en Computación en el Centro de Investigación en Computación del Instituto Politécnico Nacional. Esta tesis define un modelo de ciclo de vida aplicable para el desarrollo de Sistemas de Información para WEB. Toma como base modelos clásicos de ingeniería y nuevas teorías de Ingeniería WEB; así como, el estándar ISO/IEC 12207. La tesis se encuentra estructurada en 7 capítulos: Introducción, Marco Teórico, Análisis, Diseño, Prototipo de Prueba, Pruebas y resultados y finalmente Conclusiones y futuros trabajos.

1.4 Comentarios del capítulo

Existe una creciente adquisición de SI por parte de las organizaciones, como parte de sus procesos productivos. Cada avance tecnológico en materia de informática plantea a su vez, nuevos retos de seguridad que requieren ser atendidos y solucionados. Desafortunadamente, la tecnología avanza más rápido que las soluciones a los retos de seguridad que la misma tecnología impone.

Se debe tener presente que el entorno en el que se encuentran los SI no es estático. Por ello, no se puede considerar que un SI sea 100% seguro. No se puede asegurar que un SI esté libre de vulnerabilidades, ya que conforme pasa el tiempo y avanza el desarrollo tecnológico, también se descubren nuevas vulnerabilidades. Lo que sí se puede asegurar es que los SI desarrollados están exentos de las vulnerabilidades típicas y comúnmente conocidas.

Como lo mostraron las cifras presentadas en este capítulo, la mayor parte de las vulnerabilidades se encuentra en el diseño de los SI, no en su infraestructura. De ahí surge la necesidad de atender no solamente la seguridad perimetral sino ir más allá. Es decir no se debe confiar plenamente en los mecanismos de seguridad externos y optar por el fortalecimiento de los SI desde su diseño y concepción.

CAPÍTULO 2: MARCO TEÓRICO

Resumen

Este capítulo, se presentan las bases, definiciones y conceptos de los que se parte para el desarrollo de esta tesis.

Los temas que se tratan en este capítulo son:

- Sistemas de información y la seguridad en los mismos
- Estándares y mejores prácticas en el desarrollo de sistemas, auditoría de seguridad, calidad del software
- Procedimiento Operativo Estándar
- Generalidades de auditoría y auditoría de seguridad
- Metodologías de auditoría informática

2.1 Generalidades de los Sistemas de Información

Un sistema de información es un conjunto de elementos interrelacionados con el fin de obtener, procesar, almacenar, administrar, formatear, difundir y en determinado momento destruir la información procesada.

En la medida en que más funciones de las organizaciones se han automatizado, los Sistemas de Información (SI) se han tornado aceleradamente más especializados, dando origen a distintos tipos. Sin importar la clasificación a la que pertenezcan o la forma de adquisición, todos los SI convergen en el hecho relevante de aportar valor a la organización.

Un SI seguro es aquel que garantiza la confidencialidad, integridad y disponibilidad de los recursos del sistema y de la Información que maneja, mediante la aplicación de controles de seguridad, derivados del previo establecimiento de los requerimientos mínimos de seguridad a satisfacer.

Para ampliar la información correspondiente a las definiciones de sistemas, SI, componentes de un SI, seguridad, seguridad informática y sistemas de información seguros, se recomienda consultar el apéndice A: GENERALIDADES DE LOS SISTEMAS DE INFORMACIÓN.

2.2 Consideraciones de Procedimiento Operativo Estándar

Un procedimiento es un documento que indica claramente los pasos consecutivos para iniciar, desarrollar y concluir una actividad u operación relacionada con un proceso, los elementos técnicos a emplear, las condiciones requeridas, los alcance limitaciones fijadas, el número y características del personal que intervienen, etc.**[17].**

Un POE (Procedimiento Operativo Estándar), es un procedimiento documentado, de manera formal, que incluye un conjunto de instrucciones que describen la manera en que deben realizarse las tareas repetitivas en una organización. Los POEs constituyen un conjunto de instrucciones que tienen el carácter de una directiva y se definen para asegurar y mantener la calidad de los procesos que ocurren en un sistema y principalmente donde no existen procedimientos propiamente establecidos.

Un procedimiento se vuelve obligatorio y es parte de las políticas de seguridad dentro de una organización **[18]**.

Frecuentemente, los POEs están conformados de componentes operacionales y técnicos. Cuando los POEs han sido diseñados de manera clara y efectiva se convierten en elementos esenciales para el desarrollo y la implementación de cualquier solución. Todo buen sistema de calidad está basado en POEs.

Inicialmente los POEs eran usados en el área médica; actualmente se ha extendido su uso a la industria de las tecnologías de información, entre las tareas donde son utilizados los POEs se encuentran todas aquellas relacionadas con mejores prácticas en el mantenimiento y desarrollo de hardware y software **[19]**.

Así, los POEs resultan ser elementos que contribuyen al desarrollo de metodologías que puedan ser usadas en el proceso de auditoría de seguridad de los sistemas de Información.

De acuerdo con la Royal Pharmaceutical Society of Great Britain (RPSGB) **[20]** algunos de los beneficios que ofrece el trabajar mediante POEs son:

- Aseguran la calidad y consistencia de un servicio.
- Garantizan el uso y aplicación de las mejores prácticas en todo momento.
- Proporcionan la oportunidad de utilizar la experiencia del personal involucrado en la tarea a realizar.
- Permiten segregar y delegar funciones, así como liberar tiempo del personal para otras actividades.
- Ayudan a evitar confusiones entre las funciones de las personas involucradas (esclarecimiento de funciones).
- Proporcionan consejo y orientación a suplentes y personal de medio tiempo.
- Son herramientas útiles para la capacitación de nuevos miembros de trabajo.
- Contribuyen al proceso de auditoría.

Los POEs frecuentemente se definen y utilizan como guías prácticas donde no existe una doctrina oficial ó un marco legal ó institucional al respecto. Los POEs se utilizan para proporcionar detalles prácticos sobre el trabajo en una organización y para un área laboral específica, deben ser lo suficientemente generales para poder manejar los pasos básicos en un proceso de auditoría y a su vez deben

proveer flexibilidad para responder a circunstancias únicas que puedan surgir. Adicionalmente, los POEs pueden facilitar la integración y documentación de la evidencia de auditoría obtenida en el proceso de auditoría, pues ellos especifican de manera escrita lo que se debe hacer, cuándo, dónde y por quién.

Si bien existen varias metodologías para desarrollar una auditoría de sistemas, guías para probar la seguridad, diversos estándares y mejores prácticas en el desarrollo de aplicaciones, son escasos los procedimientos que definen los pasos a seguir en la revisión de la existencia y suficiencia de los requerimientos mínimos funcionales y de seguridad que debe cubrir un SI. Por ello, se ha decidido que para esta tesis, se hará uso de los POEs para conformar una metodología de auditoría de seguridad de SI.

Diseño de POE

Según RPSGB **[20]**, para iniciar el proceso de diseño de un POE, es recomendable contestar las preguntas presentadas en la tabla 2.

Aspectos a considerar en el diseño de un POE	
Aspectos a cubrir por el POE	Preguntas a responder al diseñar un POE
Objetivos	¿Qué es lo que el POE intenta lograr?
Campo de aplicación	¿Qué áreas de trabajo serán cubiertas por este POE?
Etapas del proceso	¿Cómo se llevará a cabo la tarea? ¿Cuáles son los pasos necesarios para realizar la tarea?
Responsabilidad	¿Quién es el responsable de efectuar cada etapa o escenario del proceso en condiciones normales o excepcionales?
Otra información útil	¿Hay alguna otra información que pueda ser incluida en el POE?
Revisión	¿Cómo te asegurarás de que el POE continuará siendo útil, relevante y actualizado?

Tabla 2.- Aspectos a considerar en el diseño de un POE

Estructura General de un POE

Lucio Santes Galván, en la tesis con título "Propuesta de una metodología de análisis forense para dispositivos de telefonía celular" **[19]**, describe la estructura general de un POE. Los elementos que conforman a un POE son:

- **Una cabecera:** Contiene el nombre de la institución y del departamento que diseña y utiliza al procedimiento. Además también se compone de: Título, número de POE, número de revisión, fecha de vigencia, número de hojas.

- **Objetivo:** Que describe brevemente la finalidad del POE.

- **Alcance:** El procedimiento deberá indicar las restricciones de su aplicación. En otras palabras, deberá especificar ya sea los elementos con los que puede trabajar o establecer las circunstancias en las que deberá detenerse.

- **Responsable:** Establece explícitamente la persona encargada de efectuar el procedimiento documentado. Se debe incluir el papel en la investigación forense así como el nombre propio para evitar confusiones, en caso de que dos personas tengan la misma función.

- **Definiciones:** En donde se aclaran aquellos términos que se consideren convenientes.

- **Materiales:** Hardware y software. Especifica los dispositivos físicos y aplicaciones que serán utilizados en el procedimiento.

- **Aspectos de seguridad:** Especifican aquellas medidas que se deben tomar en cuenta al momento de realizar el trabajo, y de esta manera efectuar el procedimiento de manera exitosa.

- **Procedimiento:** Es la sección que corresponde al cuerpo del POE en donde se presentan los pasos que forman al procedimiento.

- **Referencias:** Referencias a publicaciones originales, y otras publicaciones relevantes.

2.3 Generalidades de Auditoría

Auditoría

Carlos Muñoz en el libro "Auditoría de Sistemas Computacionales" **[21]**, define la auditoría como la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación.

Roberto Sobrinos en el libro "Planificación y Gestión de Sistemas de Información" **[22]**, define la auditoría como la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Se pueden descomponer los conceptos anteriores en los elementos fundamentales que a continuación se especifican:

- Contenido: una opinión profesional.
- Actuación: auditor
- Justificación: sustentada en determinadas técnicas, métodos y procedimientos especializados.
- Finalidad: determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas. Evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa.
- Objetivo final: emitir un dictamen profesional e independiente.

En todo caso es una función que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

Auditoría Interna y Auditoría Externa

La auditoría informática tanto interna como externa debe ser una actividad exenta de cualquier contenido o matiz político ajena a la propia estrategia y política general de la empresa.

Auditoría Interna

La Auditoría Interna es una función independiente de evaluación establecida dentro de una organización, para examinar y evaluar sus actividades como un servicio a la organización. El objetivo de la auditoría interna consiste en apoyar a los miembros de la organización en el desempeño de sus responsabilidades. Para ello la auditoría interna les proporciona, análisis, evaluaciones, recomendaciones, asesoría e información concerniente con las actividades revisadas **[23]**.

Auditoría Externa

A diferencia de la auditoría interna, esta se realiza por personas ajenas a la organización, lo que deriva una mayor objetividad comparado con una auditoría interna, debido al mayor distanciamiento entre auditor y auditado.

Base Conceptual

Con base en el SI auditado, el auditor realizará un estudio y análisis siguiendo alguna metodología de trabajo, pero sin desviarse de la base conceptual del SI de la empresa auditada.

Los SI tienen sus bases en algunos aspectos importantes dentro de cualquier organización, entre ellos se tienen los siguientes:

- **Aspectos económicos.-** Considerar los recursos con los que cuenta la organización.
- **Aspectos tecnológicos.-** Equipo físico dentro de la organización. Se deben considerar las nuevas adquisiciones, sustituciones y cambios, ya sea de software o hardware.
- **Aspectos sociales.-** Mejoras orientadas hacia los empleados de la empresa, por ejemplo, cursos, capacitación, etc.

- **Aspecto político legal.-** Estándares y leyes vigentes para las empresas, tanto internas como externas, se debe cuidar, el aspecto legal, especialmente en el Software.

- **Aspecto Administrativo.-** Relación a nivel de gerencias, mayor confianza en la toma de posiciones, decisiones o fortunas, siempre a favor de las empresas.

Tipos de auditoría

Existe una amplia gama de tipos de auditoría, se presentan los tipos de auditoría de interés en el área de Informática y cómputo:

Auditoría Informática de Explotación

La explotación informática se ocupa de producir resultados, tales como listados, archivos soportados magnéticamente, órdenes automatizadas, modificación de procesos, etc. Para realizar la explotación informática se dispone de datos, las cuales sufren una transformación y se someten a controles de integridad y calidad.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones

La función de desarrollo es una evaluación del llamado Análisis de programación y sistemas. Todas estas fases del desarrollo de un proyecto, deben estar sometidas a un exigente control interno, de lo contrario, pueden producirse insatisfacción del cliente, insatisfacción del usuario, altos costos, etc. Por lo tanto, la auditoría deberá comprobar la seguridad de los programas, en el sentido de garantizar que el servicio ejecutado por la máquina, los resultados sean exactamente los previstos y no otros.

Auditoría de sistemas

Conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente de acuerdo con las normas informáticas y generales existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

Auditoría Informática de Comunicación y Redes

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real.

En este tipo de auditoría se investiga sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. Se deberá determinar cuántas líneas existen, cómo son y dónde están instaladas, y sobre ellas hacer una suposición de la Inoperatividad Informática. Todas estas actividades deben estar coordinadas y dependientes de una sola organización.

Auditoría de la Seguridad Informática

Se debe tener presente la cantidad de información almacenada en el computador, la cual en muchos casos puede ser confidencial, ya sea para los individuos, las empresas o las instituciones, lo que significa que se debe cuidar del mal uso de esta información, de los robos, los fraudes, sabotajes y sobre todo de la destrucción parcial o total. En la actualidad se debe también cuidar la información de los virus informáticos, los cuales permanecen ocultos y dañan sistemáticamente los datos.

Auditoría de la Seguridad de los Sistemas de Información

Una auditoría de Seguridad se refiere a aquellos trabajos de análisis, revisión, evaluación y propuesta de perfeccionamiento de los SI, de forma tal que se contribuya a que su uso apoye las funciones para los que fueron creados. Una auditoría de seguridad da una visión exacta del nivel de exposición de los SI a nivel de seguridad.

Papel del Auditor de Seguridad de SI

El papel de auditor debe estar encaminado hacia la búsqueda de problemas existentes dentro de los SI evaluados, y a la vez proponer soluciones para corregir las vulnerabilidades encontradas en el SI.

Etapas de una Auditoría

Se requieren varios pasos para realizar una auditoría. En general un proceso de auditoría se compone de las siguientes etapas **[21]**:

- **Preliminares:** El primer paso para realizar una auditoría es definir las actividades necesarias para su ejecución, lo cual se logrará mediante una adecuada planeación de estas; es decir, se deben identificar claramente las razones por las que se va a realizar la auditoría y la determinación de objetivos de la misma, así como el diseño de los métodos, técnicas y procedimientos necesarios para llevarla a cabo y para preparar los documentos que servirán de apoyo para su ejecución, culminando con la elaboración documental de los planes, programas y presupuestos para esta auditoría.

- **Ejecución:** Estará determinada por las características concretas, los puntos y requerimientos que se estimaron en la etapa de planeación.

- **Dictamen de la auditoría:** Se emite un dictamen, el cual es el resultado final de la auditoría. Esta etapa incluye la elaboración de un informe con las situaciones detectadas, elaboración del dictamen final y la presentación del informe de auditoría.

2.4 Auditoría de Seguridad de Sistemas de Información

Una auditoría de seguridad informática de sistemas de información (SI) es el estudio que comprende el análisis, revisión, evaluación y propuesta de perfeccionamiento de los SI, para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva del SI. De forma tal que, el uso del SI apoye las funciones para lo que fue creado.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los dueños y responsables quienes deberán establecer medidas correctivas y preventivas de refuerzo tomando en cuenta las recomendaciones emitidas por el auditor, siguiendo siempre un proceso secuencial que permita mejorar la seguridad de sus SI aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización y cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad. Es decir, da una visión exacta del nivel de exposición de los SI a nivel de seguridad.

Una auditoría se realiza con base en un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar se puede encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información. Éste puede considerarse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los SI. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría **[24]**.

2.5 Metodologías de Auditoría de Seguridad de SI

Una metodología se define como la descripción secuencial de la manera de efectuar una operación o una serie de operaciones que conducen a un objetivo establecido.

Mario Piattini en el libro "Auditoría Informática" **[25]**, describe que todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informático, se puede agrupar, según su función, en dos grandes familias:

Cuantitativas: Basadas en un modelo matemático numérico que ayuda a la realización del trabajo, están diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numérico. Están diseñadas para producir una lista de riesgos que pueden compararse entre si con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Cualitativas: Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada. Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Basadas en métodos estadísticos y lógica borrosa, que requiere menos recursos humanos/tiempo que las metodologías cuantitativas.

La auditoría de seguridad informática identifica el nivel de exposición por la falta de controles **[25]**. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un conjunto de medidas que minimicen el riesgo de que las amenazas exploten vulnerabilidades del SI y se materialicen en hechos.

Una metodología de auditoría de seguridad de SI es la descripción secuencial de la manera de de efectuar el análisis, revisión, evaluación y propuesta de perfeccionamiento de los SI, dando una visión exacta del nivel de exposición de los SI.

Las metodologías de auditoría de seguridad son de tipo cualitativas, es decir, son subjetivas por excelencia. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen gran profesionalidad y formación continua.

2.6 Estándares y Mejores Prácticas

Estándar

Un estándar[6] es una regla, norma o especificación publicada que establece un lenguaje común para realizar un conjunto de procesos y actividades, con el fin de conseguir un objetivo determinado con un grado óptimo de orden **[26]**.

Mejores Prácticas

La Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI) **[27]**, define a las mejores prácticas como una compilación de las prácticas que empresas y organizaciones con un alto reconocimiento han implementado, y las cuales les han aportado buenos resultados.

Las mejores prácticas no son propiedad de una sola compañía, es decir, tienen aplicación universal en todas las compañías. Pero es obvio que no exista una práctica única que le sirva a todo el mundo. El términos mejores, significa "mejores para cada quien".

Las organizaciones e instituciones en su afán de estandarizar sus procesos, han diseñado, desarrollado e implementado un conjunto de estándares y mejores prácticas que apoyan a los procesos organizacionales y que son reconocidas por su eficacia comprobada. Los estándares y mejores prácticas, se utilizan para describir el trabajo sólido, respetable y actualizado que se realiza en un campo específico.

Existen diversos estándares y mejores prácticas aceptadas internacionalmente en el área de TI, por conveniencia de esta tesis, se han agrupado en 3 bloques:

1) en el desarrollo de aplicaciones,
2) en la auditoría informática y de seguridad, y
3) en la calidad en los SI.

A continuación se describe cada uno de los estándares y mejores prácticas correspondientes a estos 3 bloques.

[6] Para el BSI (The British Standards Institución), un estándar es una especificación publicada que establece un lenguaje común, y contiene las especificaciones técnicas u otros criterios precisos y está diseñado para ser utilizado generalmente como una guía, una regla o una definición.

2.6.1 En el Desarrollo de aplicaciones

Los estándares para el desarrollo de aplicaciones, proporcionan un marco de referencia común para los procesos del ciclo de vida del software, incluye tareas y actividades que se deben realizar en cada una de las etapas del ciclo de vida de desarrollo del software.

Cabe aclarar, que este bloque corresponde únicamente a la concepción del Ciclo de Vida de desarrollo de Software (CVDS), es decir no se incluyen las consideraciones de seguridad a lo largo del ciclo de vida. En el capítulo 3 se retomaran los estándares utilizados bajo la concepción de CVDS Seguro.

El estándar establecido por la ISO/IEC para el desarrollo de aplicaciones es el estándar ISO/IEC 12207: Proceso de Ciclo de Vida de Software, a continuación se presenta un breve resumen del estándar.

ISO/IEC 12207

La norma ISO/IEC 12207 "Software Life Cycle Processes" **[28],** es el estándar para los procesos de ciclo de vida del software, el cual establece un marco de referencia común para los procesos del ciclo de vida para el software, incluye procesos y actividades que se aplican desde la definición de requisitos, pasando por la adquisición y configuración de los servicios del sistema, hasta la finalización de su uso. Este estándar tiene como objetivo principal proporcionar una estructura común para que compradores, proveedores, desarrolladores, personal de mantenimiento, operadores, administradores y personal involucrados en el desarrollo de software usen un lenguaje común. Este lenguaje común se establece en forma de procesos bien definidos.

La estructura del estándar ha sido concebida de manera flexible y modular de manera que pueda ser adaptada a las necesidades de cualquiera que lo use. Para conseguirlo, el estándar se basa en dos principios fundamentales: Modularidad y responsabilidad. Con la modularidad se pretende conseguir procesos con un mínimo acoplamiento y una máxima cohesión. En cuanto a la responsabilidad, se busca establecer un responsable para cada proceso, facilitando la aplicación del estándar en proyectos en los que pueden existir distintas personas u organizaciones involucradas.

Los procesos se clasifican en tres tipos: Principales, de soporte y de la organización, esta clasificación se puede apreciar en la figura 5 **[28].**

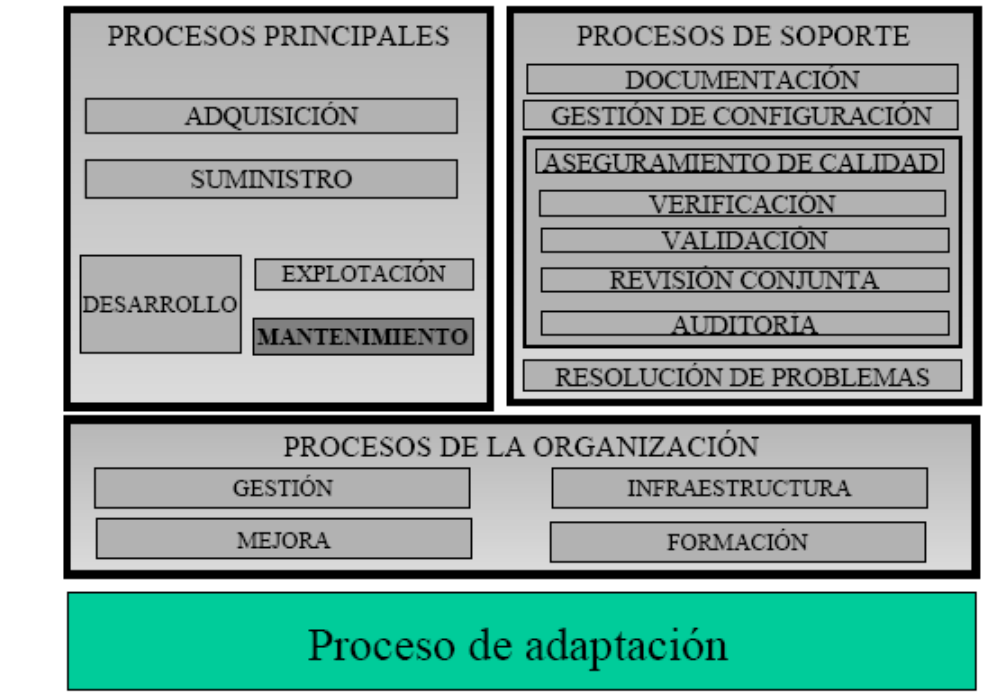


Fig 5. Proceso del Ciclo de vida de software según ISO/IEC 12207.

Como puede apreciarse en la figura 5, la norma ISO/IEC 12207, dentro de los procesos de la organización, se considera también el proceso de adaptación cuyo objetivo es realizar la adaptación básica de la norma ISO a distintos proyectos de software, teniendo en cuenta las variaciones en las políticas y procedimientos propios de cada una de las organizaciones que requiera implementar la norma dentro de sus procesos de desarrollo.

Proceso Principales

ISO/IEC 12207 define cinco procesos principales, de cuya ejecución se encargan las denominadas partes principales. En la norma se considera "parte principal" la que inicia o realiza uno de los cinco procesos principales, por lo cual las partes principales son: el adquiriente, el suministrador, el desarrollador, el operador y el personal de mantenimiento del software.

1. **Proceso de adquisición:** Comienza definiendo la necesidad de adquirir un sistema o un producto software y continúa con la preparación y publicación de la solicitud de propuestas, la selección de un proveedor y la gestión de los procesos de adquisición hasta la aceptación del producto.

2. **Proceso de suministro:** Puede iniciarse bien por una decisión de preparar una propuesta para responder a una petición de un adquiriente, bien por la firma de un contrato con el adquiriente para proporcionar el producto software. El proceso continúa con la identificación de los procedimientos y recursos necesarios para gestionar y asegurar el proyecto, incluyendo el desarrollo de los planes del proyecto y la ejecución de los planes hasta la entrega del producto software.

3. **Proceso de desarrollo:** Contiene las actividades para el análisis de requisitos, diseño, codificación, integración, pruebas, e instalación y aceptación relativas al software.

4. **Proceso de operación:** Abarca la operación del software y el soporte a usuarios. Debido a que la operación del software se integra en la operación del sistema, las actividades y tareas del proceso de operación se refieren al sistema.

5. **Proceso de mantenimiento:** Se activa cuando el software sufre modificaciones de código o de documentación asociada debido a un error, una deficiencia, un problema o la necesidad de mejora/adaptación.

Procesos de soporte

La norma contiene ocho procesos de soporte, los cuales pueden ser empleados por los procesos de adquisición, suministro, desarrollo, operación, mantenimiento o cualquier otro proceso de soporte. Estos procesos se emplean en varios puntos del ciclo de vida y pueden ser realizados por la organización que los emplea, por una organización independiente (como un servicio), o por un cliente como elemento planificado o acordado del proyecto.

1. **Proceso de documentación:** Registra la información producida por un proceso o actividad del ciclo de vida. Este proceso contiene el conjunto de actividades que planifican, diseñan, desarrollan, producen, editan, distribuyen y mantienen los documentos necesarios para todos los interesados tales como directores, ingenieros y usuarios del sistema.

2. **Proceso de gestión de configuración:** Consta además de la implementación del propio proceso (en la que se incluye la elaboración del plan de gestión de configuración), de las actividades de identificación, control, evaluación de la configuración, gestión y entregas de liberaciones.

3. **Proceso de aseguramiento de la calidad:** Proporciona el aseguramiento adecuado de que los procesos y productos de soporte del ciclo de vida del proyecto cumplen con los requisitos especificados y que se ajustan a los planes establecidos.

4. **Proceso de verificación:** Determina si los requisitos de un sistema o software están completos y correctos, así también que los productos de software en cada fase de desarrollo cumplen los requisitos o condiciones impuestos sobre ellos en las fases previas, responde a la pregunta ¿Estamos construyendo adecuadamente el producto? La verificación puede integrarse en el proceso que la emplee.

5. **Proceso de validación:** Determina si los requisitos y el software construido cumplen con su uso proyectado, la pregunta a la que responde es ¿Estamos construyendo el producto correcto? Al igual que el anterior, este proceso puede ejecutarlo una organización independiente del proveedor, desarrollador, operador o personal de mantenimiento.

6. **Proceso de revisión conjunta:** Define las actividades, que emplea cualquiera de las partes, para evaluar el estado y los productos de las actividades.

7. **Proceso de auditoría:** Permite determinar el cumplimiento de los requisitos, planes y contrato según sea apropiado.

8. **Proceso de resolución de problemas:** Analiza y resuelve los problemas que se descubren durante el ciclo de vida del software. Proporciona los medios oportunos, responsables y documentados para asegurar que todos los problemas descubiertos se analizan y resuelven.

Procesos Organizacionales

Los procesos organizacionales apoyan al establecimiento, implementación y mejoran la organización, consiguiendo una organización más eficiente.

1. **Proceso de gestión:** Contiene las actividades y tareas genéricas que puede emplear cualquier parte en la dirección de sus respectivos procesos; comprende la iniciación y definición del alcance, planificación, ejecución y control, revisión y evaluación, y cierre.

2. **Proceso de infraestructura:** Establece la infraestructura necesaria para cualquier otro proceso, que puede incluir hardware, software,

herramientas, técnicas, normas e instalaciones para desarrollo, operación o mantenimiento.

3. **Proceso de mejora:** Establece, valora, mide, controla y mejora los procesos del ciclo de vida del software.

4. **Proceso de formación:** Proporciona y mantiene un personal formado.

5. **Proceso de adaptación:** Permite realizar la adaptación básica de la norma ISO a distintos proyectos de software, teniendo en cuenta las variaciones en las políticas y procedimientos organizacionales, los métodos y estrategias de adquisición, el tamaño y complejidad de los proyectos, los requisitos de sistema y métodos de desarrollo, etc. etc.

2.6.2 En la Seguridad y Auditoría Informática

Una auditoría se realiza con base en un patrón o conjunto de directrices o buenas prácticas sugeridas.

Existen mejores prácticas y estándares orientados a servir como base para auditorías de informática, entre ellos encontramos el ISO 27002, COBIT e ISO/IEC 15408.

Por otra parte el NIST, presenta en la publicación FIPS PUB 199 y 200, el estándar para clasificar la seguridad de los SI y lo requerimientos mínimos de seguridad de un SI. De manera complementaria, al FIPS PUB 200 se presenta el NIST SP 800-53 el cual presenta los controles de seguridad recomendados.

De igual manera, existen mejores prácticas utilizadas para la evaluación de seguridad, entre las más comunes se encuentra el OSSTMM y la guía de pruebas OWASP.

A continuación se presenta una breve descripción de los estándares y mejores prácticas considerados para la seguridad y auditoría informática.

ISO 27002.

Se ha conformado como un código internacional de buenas prácticas de seguridad de la información. Puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad.

Para ampliar la información acerca de este estándar, se recomienda consultar el apéndice B: ISO 17799/ISO 27002.

COBIT.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT)**[29]**, brindan un conjunto de las mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información(ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI).

COBIT presenta un marco de trabajo de dominios y procesos, así como las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos y están enfocadas fuertemente en el control y menos en la ejecución.

COBIT ofrece a directivos, auditores y a usuarios de TI un conjunto de medidas de aceptación general, indicadores, procesos y mejores prácticas para asistirlos a maximizar los beneficios procedentes de la utilización de TI y el desarrollo adecuado gobierno de TI y control en una empresa. COBIT 4.1 se conforma de 34 procesos de alto nivel, los cuales cubren 210 objetivos de control clasificados en 4 dominios: Planear y Organizar, Adquirir e implantar, Entrega y da soporte, y Monitorear y Evaluar. Dentro de los objetivos definidos por COBIT con respecto a la seguridad de los SI, se encuentra definido el objetivo de control de alto Nivel "DS5: Garantizar la Seguridad de los Sistemas" (contenido en el dominio de "Entrega y da soporte").

El objetivo de control de alto nivel DS5 "Garantizar la seguridad de los Sistemas", incluye los siguientes objetivos de control específicos:

- DS5.1 Administración de la seguridad de TI
- DS5.2 Plan de seguridad de TI
- DS5.3 Administración de identidad
- DS5.4 Administración de cuentas del usuario
- DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
- DS5.6 Definición de incidente de seguridad
- DS5.7 Protección de la tecnología de seguridad
- DS5.8 Administración de llaves criptográficas
- DS5.9 Prevención, detección y corrección de software malicioso
- DS5.10 Seguridad de la red
- DS5.11 Intercambio de datos sensitivos

Para ampliar la información acerca del objetivo de control de alto nivel DS5, se recomienda consultar el apéndice C: COBIT, DS5: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.

ISO/IEC 15408.

El estándar ISO/IEC 15408 **[30]** (common criteria) define un criterio estándar para la evaluación de las propiedades y características de seguridad de determinado producto o sistema IT.

El estándar proporciona un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto en base al conjunto de requisitos de seguridad y garantía, que satisface respecto a esta norma obteniendo de esa forma una certificación oficial de nivel de seguridad que satisface.

Los requisitos de seguridad presentados en el estándar, definen un comportamiento deseado en materia de seguridad de un determinado producto o sistema IT y se agrupa en clases, las clases contenidas son:

FAU- Auditoría

FCO- Comunicaciones

FCS- Soporte criptográfico

FDP- Protección de datos de usuario

FIA- Identificación y autenticación de usuario

FMT- Gestión de la seguridad

FPR- Privacidad

FPT- Protección de las funciones de seguridad del objetivo a evaluar

FRU- Utilización de recursos

FTA- Acceso al objetivo de evaluación

FTP- Canales seguros

Para ampliar la información acerca de este estándar, se recomienda consultar el apéndice D: CRITERIOS COMUNES DE EVALUACIÓN ISO/IEC 15408.

FIPS PUB 199

Describe las normas para la clasificación de seguridad de la información federal y los Sistemas de Información (SI), en esta publicación se detalla la forma en que las agencias federales de los EUA pueden clasificar su información y los SI.

La publicación FIPS 199 requiere que la organización clasifique sus sistemas de información como de bajo impacto, impacto moderado o alto impacto para los objetivos de seguridad de la confidencialidad, integridad y disponibilidad.

Los valores del impacto potencial asignado a los objetivos de seguridad correspondientes, son los valores más altos de entre las categorías de seguridad que se han determinado para cada tipo de información residente en estos sistemas de Información.

El formato generalizado para expresar la categoría de seguridad (CS) de un SI es:

$$CS_{SI} = \{(\text{confidencialidad, impacto}), (\text{integridad, impacto}), (\text{disponibilidad, impacto})\}$$

Los valores aceptables para el impacto potencial son bajo, moderado o alto.

FIPS PUB 200

Denominado "Minimum Security Requirements for Federal Information and Information Systems" fue publicado en Marzo del 2006 y define los requerimientos mínimos de seguridad para la información y SI federales de los EUA.

El NIST define un requerimiento de seguridad **[12]**, como los requerimientos percibidos en un SI que se derivan de las leyes, decretos, directivas, políticas, normas, instrucciones, regulaciones o procedimientos, o la misión de la organización/casos de negocio necesarios para garantizar la confidencialidad, integridad y disponibilidad de los información que es procesada, almacenada o transmitida.

Los requisitos mínimos de seguridad cubren diecisiete áreas relacionadas con la seguridad con respecto a la protección de la confidencialidad, integridad y disponibilidad de los SI y la información procesada, almacenada y transmitida por estos sistemas.

Las diecisiete áreas representan una amplia base, de un programa equilibrado de seguridad de la información que se ocupa de la gestión, operación y aspectos

técnicos de la protección de la información y los SI. Estas áreas relacionadas con la seguridad son:

1. Control de acceso (AC)
2. Sensibilización y Formación (AT)
3. Auditoría y Rendición de Cuentas (AU)
4. Certificación, Acreditación y evaluaciones de Seguridad (CA)
5. Gestión de la Configuración (CM)
6. Planes de Contingencia (CP)
7. Identificación y autenticación (IA)
8. Respuesta a Incidentes (IR)
9. Mantenimiento (MA)
10. Protección de Medios (MP)
11. Protección física y Ambiental (PE)
12. Planificación (PL)
13. Personal de Seguridad (PS)
14. Evaluación de Riesgos (RA)
15. Adquisición de sistema y servicios (SA)
16. Protección de Sistemas y Comunicaciones (SC)
17. Integridad de Sistema y la información (SI)

Para ampliar la información correspondiente a cada una de las áreas sugeridas por el FIPS PUB 200, se recomienda consulta el apéndice F: FIPS PUB 200.

NIST SP 800-53.

La publicación especial SP 800-53 **[31]** del NIST "Recommended Security Controls for Federal Information Systems and Organizations", es un documento que agrupa los controles de seguridad recomendados para los Sistemas de información y organizaciones federales de los Estados Unidos de América.

Los controles de seguridad descritos en 800-53 tienen una organización bien definida y estructurada. Para facilidad de selección del Control de Seguridad y las especificaciones de sus procesos se organizan en 17 familias:

1. Control de acceso;
2. Concientización y capacitación;
3. Auditoría y rendición de cuentas,
4. Certificación, acreditación y evaluaciones de seguridad,
5. Gestión de configuración,
6. Planificación de contingencia,
7. Identificación y autenticación,
8. Respuesta a incidentes,
9. Mantenimiento,
10. Protección de Medios,

11. Protección física y ambiental,
12. La planificación,
13. Personal de seguridad,
14. Evaluación del riesgo,
15. Adquisición de sistemas y servicios,
16. Protección del sistema y comunicaciones,
17. Integridad del sistema y la información.

Para ayudar a las organizaciones en la selección adecuada de los controles de seguridad para un SI, se introduce el concepto de los controles de referencia. Los controles de referencia son el punto de partida para el proceso de selección de los controles de seguridad descritos en SP800-53 y son elegidos en base a la categoría de seguridad y nivel de impacto de los asociados del sistema de información determinado de conformidad con FIPS 199 y FIPS 200 respectivamente. La medida de referencia de control de seguridad es el conjunto mínimo de controles de seguridad para el SI.

Para ampliar la información de la publicación FIPS 199, consultar el apéndice E: FIPS PUB 199. Para ampliar la información de la publicación FIPS 200, consultar el apéndice F: FIPS PUB 200.

OSSTMM: Manual de Metodología Abierta de Evaluación de Seguridad.

El manual de metodología abierta de evaluación de seguridad **[32]**, es un documento de metodología Abierta de evaluación de seguridad emitido por ISECOM. Esta guía proporciona un conjunto de reglas y lineamientos para determinar cuándo, qué y cuáles eventos deben ser evaluados. Esta metodología cubre únicamente la prueba de seguridad externa, es decir, evalúa la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado. El objetivo de este manual es crear un método aceptado para la realización de pruebas de seguridad en profundidad. Las secciones consideradas en este manual son:

1. Seguridad de la Información
2. Seguridad de los Procesos
3. Seguridad en las tecnologías de Internet
4. Seguridad en las Comunicaciones
5. Seguridad Inalámbrica
6. Seguridad Física

Guía de Pruebas OWASP.

La guía de Pruebas OWASP **[33]**, es una metodología Abierta, la cual cubre los procedimientos y herramientas para probar la seguridad en las aplicaciones Web. La versión 3, fue emitida por la organización OWASP en el año 2008. Esta guía incluye las "mejores prácticas" de pruebas de penetración para ser aplicadas tanto a nivel de empresa como a nivel de proyecto de desarrollos de software orientados al entorno Web. La guía de pruebas OWASP V3.0, se conforma de un total de 10 categorías de pruebas y 66 controles.

Las categorías de pruebas de seguridad presentadas por el OWASP V3.0 son:

1. Recopilación de la información
2. Pruebas de gestión de la configuración
3. Pruebas de la lógica de negocio
4. Pruebas de autenticación
5. Pruebas de autorización
6. Pruebas de gestión de sesiones
7. Pruebas de validación de datos
8. Pruebas de denegación de Servicio
9. Pruebas de Servicios Web
10. Pruebas de AJAX

2.6.3 Calidad en los Sistemas de Información

La definición de calidad propuesta por la norma ISO / IEC 8402 **[34]** es:

"La totalidad de rasgos y características de un producto o un servicio que le confieren su aptitud para satisfacer necesidades implícitas o explícitas".

Hablar de calidad del software, implica la necesidad de contar con parámetros que permitan establecer los niveles mínimos que un producto de este tipo debe alcanzar para que se considere de calidad **[35]**.

La calidad del software no sólo se puede especificar como software sin errores. La especificación de la calidad del software debe ser más precisa y detallada. La formalización de la calidad del software puede llevarse a cabo mediante la adopción de un modelo de calidad. Para conveniencia de esta tesis se utilizará el modelo propuesto por la norma ISO 9126.

Modelo de calidad establecido por ISO 9126.

La norma ISO 9126**[36]**, es un estándar internacional para la evaluación de la calidad de productos de software, en el cual se establecen las características de calidad consideradas para el software. El estándar fue publicado en 1992 con el nombre de "Information technology –Software product evaluation: Quality characteristics and guidelines for their use". La norma ISO 9126 define un modelo de calidad que es aplicable a todo tipo de software, en él se definen seis características de calidad del producto. Las características de calidad definidas en el modelo ISO 9126 y la pregunta central que atiende cada una de estas características se pueden apreciar en la figura 6. Establece que cualquier componente de la calidad del software puede ser descrito en términos de características básicas, las cuales son: funcional, confiable, utilizable, eficiente, susceptible a mantenimiento y portable.

Cada una de las características de esta Norma, se detalla a través de un conjunto de sub-características y a su vez se componen de atributos que permiten profundizar en la evaluación de la calidad de productos de software. El proceso de evaluación se divide en tres etapas **[36-A]**:

A) Definición de requisitos de calidad: Se toma como entrada un conjunto de necesidades expresadas o implícitas, documentación técnica y la propia norma ISO y se produce una especificación de requisitos de calidad.

B) Preparación de la evaluación: Implica la selección de las métricas apropiadas, definición de los niveles de evaluación y criterios de evaluación. Las métricas, en la norma ISO 9126, suelen dar lugar a medidas cuantificables asignadas a escalas. La definición de los niveles de evaluación determina qué rangos de valores en estas escalas cuentan como satisfactorio o insatisfactorio. Del mismo modo, la definición de los criterios de evaluación consiste en la preparación de un procedimiento para resumir los resultados de la evaluación para un entorno específico.

C) Procedimiento de evaluación: se conforma de pasos: medición, calificación y evaluación. En la medición, las métricas seleccionadas se aplican a los productos de software y se evalúa sobre las escalas de las métricas obtenidas. Subsecuentemente, para cada valor medido, se determina el nivel de calificación. La evaluación es el paso final, donde se resume un conjunto de niveles previamente calificados. El resultado es un resumen de la calidad del producto de software. La calidad final se compara entonces con otros aspectos tales como el tiempo y costo, y la decisión final se toma con base a criterios de gestión.

Sin embargo, a pesar de la existencia de estos modelos de mejora de la calidad del producto software, la medición de la misma no está cerrada ya que la implantación o puesta en práctica de dichos modelos es difícil de llevar a la práctica.

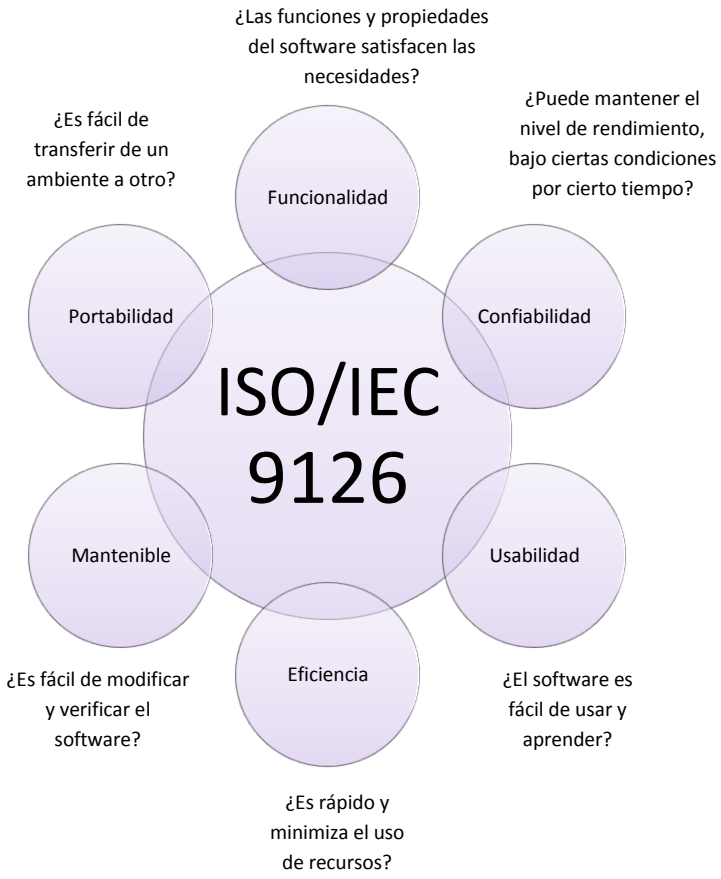


Fig 6. Las seis características de calidad de un software definidas por el ISO 9126.

Las sub-características aprobados por la ISO 9126**[34]**,**[35]**, Se presentan en las tablas 3 y 4:

Características y Sub-características definidas por el modelo ISO 9126	
Características	**Sub-características**
Funcionalidad En este grupo se conjunta una serie de atributos que permiten calificar si un producto de software maneja en forma adecuada el conjunto de funciones que satisfacen las necesidades para las cuales fue diseñado.	**Adecuación** Se enfoca a evaluar si el software cuenta con un conjunto de funciones apropiadas para efectuar las tareas que fueron especificadas en su definición.
	Exactitud Este atributo permite evaluar si el software presenta resultados o efectos acordes a las necesidades para las cuales fue creado.
	Interoperabilidad Permite evaluar la habilidad del software de interactuar con otros sistemas previamente especificados.
	Cumplimiento Evalúa si el software se adhiere a estándares, convenciones o regulaciones en leyes y prescripciones similares.
	Seguridad Se refiere a la habilidad de prevenir el acceso no autorizado, ya sea accidental o premeditado, a los programas y datos.
Confiabilidad Aquí se agrupan un conjunto de atributos que se refieren a la capacidad del software de mantener su nivel de ejecución bajo condiciones normales en un periodo de tiempo establecido.	**Madurez** Permite medir la frecuencia de falla por errores en el software.
	Tolerancia a fallos Se refiere a la habilidad de mantener un nivel específico de funcionamiento en caso de fallas del software o de la vulneración de su interfaz específica.
	Recuperación Se refiere a la capacidad de restablecer el nivel de operación y recuperar los datos que hayan sido afectados directamente por una falla, así como el tiempo y esfuerzo necesario para lograrlo.
Usabilidad Consiste de un conjunto de atributos que permiten evaluar el esfuerzo necesario que deberá invertir el usuario para utilizar el sistema.	**Comprensibilidad** Se refiere al esfuerzo requerido por los usuarios para reconocer la estructura lógica del sistema y los conceptos relativos a la aplicación del software.
	Facilidad de aprender Establece atributos del software relativos al esfuerzo que los usuarios deben hacer para aprender a usar la aplicación.
	Operabilidad Agrupa los conceptos que evalúan la operación y el control del sistema

Tabla 3.- Características y Sub-características de calidad definidas por el modelo ISO 9126.

Características y Sub-características definidas por el modelo ISO 9126	
Características	**Sub-característica**
Eficiencia Esta característica permite evaluar la relación entre el nivel de funcionamiento del software y la cantidad de recursos usados.	**Comportamiento respecto al tiempo** Atributos del software relativos a los tiempos de respuesta y de procesamiento de los datos.
	Comportamiento con respecto a recursos Atributos del software relativos a la cantidad de recursos usados y la duración de su uso en la realización de sus funciones.
Mantenible Se refiere a los atributos que permiten medir el esfuerzo necesario para realizar modificaciones al software, ya sea por la corrección de errores o por el incremento de funcionalidad.	**Capacidad de análisis** Relativo al esfuerzo necesario para diagnosticar las deficiencias o causas de fallas, o para identificar las partes que deberán ser modificadas.
	Capacidad de modificación Mide el esfuerzo necesario para modificar aspectos del software, remover fallas o adaptar el software para que funcione en un ambiente diferente.
	Estabilidad Permite evaluar los riesgos de efectos inesperados debidos a las modificaciones realizadas al software.
	Facilidad de prueba Se refiere al esfuerzo necesario para validar el software una vez que fue modificado.
Portabilidad En este caso, se refiere a la habilidad del software de ser transferido de un ambiente a otro.	**Adaptabilidad** Evalúa la oportunidad para adaptar el software a diferentes ambientes sin necesidad de aplicarle modificaciones.
	Facilidad de instalación Es el esfuerzo necesario para instalar el software en un ambiente determinado.
	Conformidad Permite evaluar si el software se adhiere a estándares o convenciones relativas a portabilidad
	Capacidad de sustitución Se refiere a la oportunidad y el esfuerzo usado en sustituir el software por otro producto con funciones similares.

Tabla 4.- Características y Sub-características de calidad definidas por el modelo ISO 9126(2).

2.7 Comentarios del Capítulo

En la medida en que las funciones y procesos en las organizaciones se han automatizado, los SI se han tornado aceleradamente más especializados, dando origen a un sin número de SI que aportan valor a la organizaciones. Como consecuencia de este crecimiento en el número de SI, el problema de SI inseguros se ha convertido en uno de los retos técnicos más importante de nuestros tiempos.

Así, los SI seguros son aquellos que garantizan la confidencialidad, integridad y disponibilidad de los recursos del sistema y de la Información que maneja, mediante la aplicación de controles de seguridad, derivados del previo establecimiento de los requerimientos mínimos de seguridad que plantea la misión, visión y objetivos de la organización.

Partiendo de la hipótesis planteada en esta tesis, existen 2 maneras de dotar seguridad a un SI, la primera es incluir seguridad en cada una de las fases del ciclo de vida de desarrollo de software, mediante la adopción de metodologías de CVDS Seguro y, la segunda, mediante el uso de un modelo de auditoría de seguridad de SI, el cual garantice que las aplicaciones desarrolladas cuenten con los controles necesarios que reduzcan las típicas vulnerabilidades de las aplicaciones.

Los estándares y mejores prácticas utilizadas en la industria de TI y presentados en este capítulo, proporcionan una guía de proceder en las tareas de planeación, adquisición, diseño, desarrollo, implementación, evaluación y operación de los SI, entre otras. En este capítulo los estándares y mejores prácticas se agruparon en tres grandes bloques: 1) en el desarrollo de aplicaciones, 2) en la seguridad y auditoría informática y 3) en la calidad del software.

Los estándares y mejores prácticas en el desarrollo de aplicaciones dependen en gran parte de la adopción de diferentes metodologías de CVDS por parte de los equipos de desarrollo y de las organizaciones para las que se desarrollan los SI. En este capítulo se presentó el estándar ISO/IEC 12207, el cual muestra un proceso de Ciclo de Vida de Desarrollo de Software. En este estándar aún no se dan las consideraciones necesarias de las tareas y actividades necesarias para incluir seguridad en cada una de las etapas del ciclo de vida. Por ello, en el siguiente capítulo se abordará el Ciclo de Vida Desarrollo de Software Seguro (CVDS Seguro).

Los estándares y mejores prácticas en la seguridad y auditoría informática presentados en este capítulo, serán abordados en el capítulo 4 para determinar los requerimientos mínimos de seguridad de los SI.

El estándar de calidad del software presentado en este capítulo, será abordado en el capítulo 4 para determinar los requerimientos mínimos funcionales de los SI.

Las consideraciones presentadas en este capítulo, correspondiente a los POE serán utilizados en el capítulo 5 para definir los POE que apoyen la implementación del modelo de auditoría de seguridad de los SI propuesta en esta tesis.

CAPÍTULO 3: CICLO DE VIDA DE DESARROLLO SEGURO

Resumen

Este capítulo pretende concientizar al lector de la importancia de que los sistemas de información nazcan seguros. Es decir, pasar de un punto en el que la seguridad es sólo la parte final del proceso de implantación del sistema de información a otro en el que la seguridad se considera como parte integral de un sistema, donde cada etapa del ciclo de vida incluye las consideraciones necesarias para dotar a la aplicación de una seguridad desde su nacimiento.

Los puntos a tocar en este capítulo son:

- El ambiente de operación considerado en el que actualmente se diseñan, desarrollan, prueban y ponen en operación los SI.
- Retos a los que se enfrentan las organizaciones al integrar un Ciclo de Vida de desarrollo de Software Seguro.
- Metodología de Desarrollo seguro de sistemas de información de Microsoft
- Estándar y mejores prácticas en el desarrollo de aplicaciones (NIST SP 800-64)

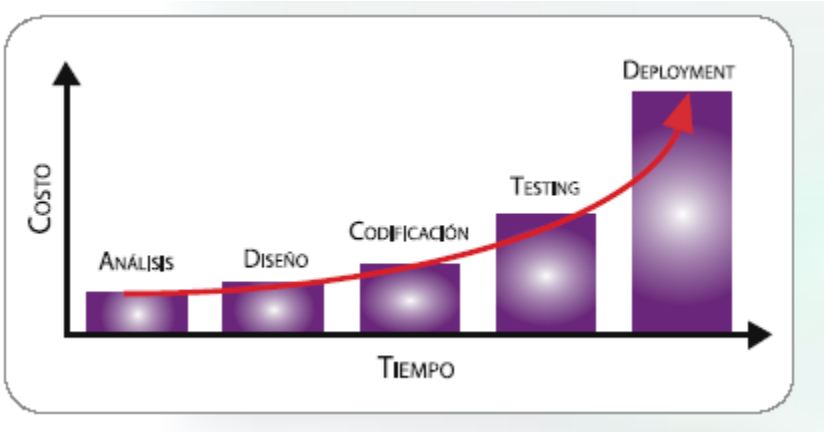
3.1 Ambiente de Operación considerado

Como se describió en el capítulo 1, la mayor parte de las organizaciones adquiere un SI para apoyar los procesos de su negocio. Como todo software, los SI pueden contener fallas de seguridad, y a diferencia del software comercial, estos SI no disponen generalmente de las actualizaciones liberadas de manera continua por parte del fabricante para cubrir las vulnerabilidades detectadas. Por lo general, el tratamiento de las vulnerabilidades en los SI de una organización se da hasta el momento que el SI ya ha sido vulnerado, es decir surge como una medida reactiva.

En la actualidad la mayoría de las organizaciones, aún no considera en sus procesos organizacionales del Ciclo de Vida de Desarrollo de Software (CVDS) las consideraciones de seguridad de los SI desarrollados. Es una práctica muy común por parte de las organizaciones, la puesta en producción de SI sin la participación del área de Seguridad de la Información. En el mejor de los casos, el área de seguridad realiza una evaluación de seguridad una vez que el SI ya está desarrollado; en este punto, la mayoría de los errores y vulnerabilidades encontradas requieren de su corrección por parte del equipo de desarrollo y en algunas ocasiones un rediseño del SI, lo cual implica un costo adicional en tiempo y esfuerzo.

Está comprobado que cuánto más temprano se encuentre una falla de seguridad en las fases del CVDS, más rápida y económica será su mitigación. ¿Cuál es el rumbo a seguir? Las buenas prácticas indican la conveniencia de incluir seguridad de la información desde el principio y a lo largo de todas las etapas del CVDS **[37]**.

La relación de costos relacionados con la incorporación de medidas de seguridad en un SI en las diferentes fases del CVDS se detallan en la figura 7 **[37]**. Estos datos se derivan de los costos reales necesarios para realizar los cambios y correcciones necesarias a los SI en diferentes puntos del CVDS.



Fuente: MILANO, Pablo."Seguridad en el ciclo de vida de desarrollo de software", http://www.prensariotila.com/pdf/TutorialCybsec_0710.pdf.

Fig 7 Costo de la integración de medidas de seguridad en diferentes fases del ciclo de vida del desarrollo de software.

La pregunta obligada es, ¿Cómo implementar seguridad a lo largo del CVDS? Mediante la adopción e implementación de un modelo de Ciclo de Vida de Desarrollo Seguro (CVDS), donde el personal de seguridad de la información se encuentre involucrado y participe en las distintas etapas de desarrollo, supervisando la realización de las mismas.

3.2 Retos en la adopción e implementación de un CVDS Seguro

La mejor forma de integrar seguridad a los SI, es tomando acciones a lo largo del Ciclo de vida mediante la adopción de un CVDS Seguro, donde en cada fase del ciclo se realicen las tareas necesarias que doten de seguridad al SI desarrollado. En cada una de estas fases debe existir la participación activa por parte del área de seguridad, la cual validará y verificará la adecuada realización de las tareas de seguridad.

Desgraciadamente, en la actualidad la estructura y cultura organizacional por parte de la mayoría de las organizaciones no permite la implementación de este modelo de desarrollo. Los principales retos a los que la adopción de un CVDS dentro de una organización se enfrenta son los siguientes:

- Erradicar la idea errónea por parte de la alta gerencia, propietarios del SI, usuarios, equipos de diseño y desarrollo de que dotar de seguridad a un SI

es un proceso independiente al Ciclo de Vida de Desarrollo del SI y generalmente se lleva en las últimas fases del ciclo de vida.

- Poco o nulo compromiso por parte de la alta gerencia con respecto a las consideraciones de seguridad de los SI organizacionales.
- Erradicar el pensamiento erróneo por parte de la alta gerencia, propietarios del SI, usuarios, e integrantes de los equipos de diseño y desarrollo, de que el área de seguridad sólo entorpece el trabajo y ejecución habitual de sus actividades diarias.
- Escasa o nula sensibilización y capacitación en seguridad de la gerencia y equipo de liderazgo de la organización, lo que deriva en la incomprensión del incremento en tiempo, recursos y esfuerzos derivado de las acciones planeadas al incluir seguridad en los SI.
- Escaso o nulo entrenamiento en seguridad de los profesionales de TI.
- Desconocimiento por parte de los equipos de diseño y desarrollo de las consideraciones y uso de las mejores prácticas de seguridad como parte de sus procesos en el desarrollo de SI.
- Poca colaboración entre las áreas de seguridad y las áreas de diseño y desarrollo.
- La inversión inicial para realizar el cambio en la forma de trabajo por las áreas de diseño y desarrollo es alta, considerando que se tiene que trabajar e invertir esfuerzo en la reorganización de la estructura de trabajo y en la capacitación de sus equipos.
- Se requiere tiempo para que una organización absorba cambios, y más cuando estos se reflejan en sus procesos internos y cultura organizacional.

3.3 Metodologías de Desarrollo Seguro de Sistemas de Información

En un Ciclo de Vida de Desarrollo Seguro (CVDS Seguro), la seguridad se aborda desde la primera etapa del ciclo de desarrollo y a lo largo de todas las etapas. En cada etapa, se realizan diversas actividades que en su conjunto aumentan la seguridad de la aplicación. Incluir seguridad tempranamente en el CVDS suele resultar menos costoso y más eficiente que agregarla a un sistema en operación. Es importante que el personal de seguridad de la información participe en las distintas etapas de desarrollo.

Las organizaciones han empezado a darle la importancia debida a la seguridad en las aplicaciones. Existen modelos de desarrollo seguro, los cuales están disponibles al público. La idea es que estos modelos puedan ser aceptados y utilizados, y posteriormente enriquecidos con las aportaciones y sugerencias y experiencia de los profesionales que han implementado estos modelos dentro de las organizaciones.

3.3.1 Microsoft Security Development LifeCycle (SDL)

Esta metodología incorpora varias actividades y materiales relacionados con la seguridad a cada una de las fases del proceso de desarrollo de software. Estas actividades y materiales incluyen el desarrollo de modelos de amenazas durante el diseño de software, el uso de herramientas de exploración del código de análisis estático durante la implementación y la realización de revisiones del código y pruebas de seguridad durante una "campaña de seguridad". Antes del lanzamiento de software sometido al SDL, un equipo independiente del grupo de desarrollo debe realizar una revisión final de seguridad. En comparación con el software que no se ha sometido al SDL, el software que ha seguido este proceso ha presentado una reducción considerable en el número de detección externa de vulnerabilidades de seguridad.

Esta metodología supone que hay un grupo central en la organización que controla el desarrollo y la evolución de las prácticas recomendadas de seguridad y las mejoras de los procesos, actúa como fuente de conocimientos para toda la organización y realiza la revisión final de seguridad antes del lanzamiento del software. Según la experiencia de Microsoft, la existencia de tal organización es vital para implementar adecuadamente el SDL, así como para mejorar la seguridad del software. Sin embargo, algunas organizaciones delegan en un consultor externo esta función de "equipo de seguridad central". Describe la integración de un conjunto de pasos destinados a aumentar la seguridad del software durante el proceso de desarrollo que suelen utilizar grandes

organizaciones. El objetivo de dichas mejoras de procesos es reducir el número y la gravedad de las deficiencias de seguridad. Recomienda que el equipo de seguridad pertenezca a la organización donde se desarrollo el software, debido a que el equipo de seguridad debe estar disponible para recurrir a él con frecuencia durante el diseño y el desarrollo del software, y es preciso confiarle información técnica y empresarial confidencial.

Puede considerarse al grupo central como un auditor de seguridad interno dentro de la metodología de Microsoft.

Las fases de SDL definidas por Microsoft son las siguientes:

- entrenamiento,
- análisis de requerimientos,
- diseño,
- implementación,
- verificación,
- liberación y
- respuesta.

En la figura 8 **[38]** se muestran las etapas y actividades clave consideradas por el SDL de Microsoft.

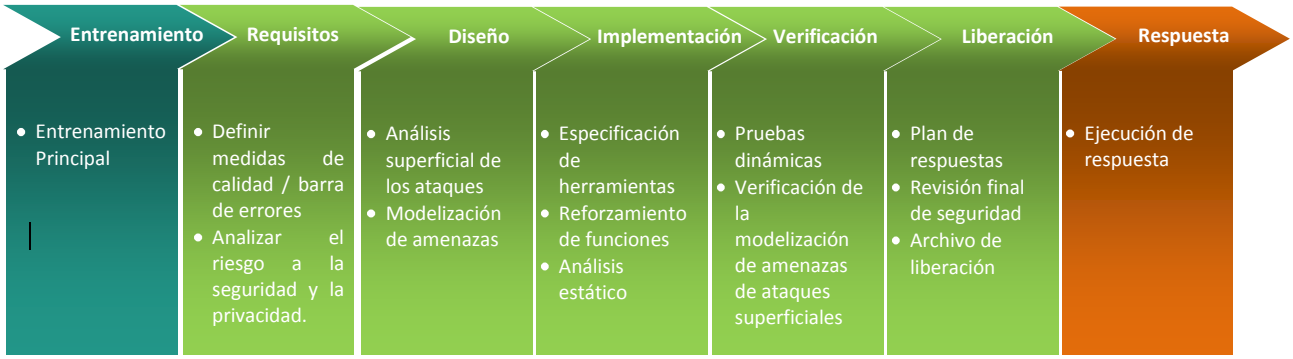


Fig 8 Ciclo de Vida de Desarrollo Seguro de Microsoft.

Entrenamiento: Considera actividades de capacitación, las cuales permiten aprender acerca de las bases de seguridad, uso de técnicas especificas y actualización de las amenazas recientes en el ámbito de seguridad.

Análisis de Requisitos: Se llevan a cabo actividades para integrar las características de seguridad y las medidas de control con los programas que probablemente se utilizarán con el software que están desarrollando. Esta fase es considerada como la mejor para integrar la seguridad a los procesos de desarrollo e identificar los objetivos de seguridad.

Diseño: Se debe identificar la estructura y los requisitos globales del software y se establece el uso de las mejores prácticas a utilizar. Desde el punto de vista de la seguridad, los elementos clave de la fase de diseño son: definir la arquitectura de seguridad y las directrices de diseño, documentar los elementos de la interfaz de ataque del software y realizar un modelado de las amenazas.

Implementación: Se prueba e integra el software. Los pasos destinados a eliminar los errores de seguridad o a impedir que se incluyan desde el principio son de gran utilidad, ya que reducen la probabilidad de que las deficiencias de seguridad lleguen a la versión final que se lanzará a los clientes. Las tareas que se aplican en la fase son: uso de: normas de codificación y de pruebas, herramientas de comprobación de seguridad, herramientas de exploración del código de análisis estático y realizar revisiones del código.

Verificación: Se realizan revisiones del código de seguridad aparte de las realizadas en la fase de implementación, así como la realización de pruebas centradas en la seguridad.

Liberación: El software debe someterse a una revisión final de seguridad, la cual definirá si desde el punto de vista de la seguridad el software está preparado para su lanzamiento a los clientes. Esta revisión se lleva a cabo mediante una revisión independiente del software que realiza el equipo de seguridad central de la organización. Adicional a ello, se lleva a cabo la creación del plan de respuesta a incidentes.

Respuesta: El equipo de desarrollo debe estar disponible para responder a cualquier posible vulnerabilidad de seguridad que surja. Una tarea importante de esta etapa es la difusión a los equipos de desarrollo y de seguridad de los procesos adaptados en los SI para que errores detectados y corregidos en los productos no se repitan en el futuro. Además, desarrollar un plan de respuesta que incluye los preparativos para posibles problemas posteriores a la liberación.

3.3.2 NIST SP 800-64

Fue emitido por el Instituto Nacional de Estándares y Tecnologías de EUA y aborda el tema de las consideraciones de seguridad en el ciclo de vida de desarrollo de SI. Presenta una guía para la incorporación de la seguridad en todas las fases del proceso de CVDS, desde su inicio hasta su disposición. Esta guía provee apoyo a las organizaciones para seleccionar y adquirir controles de seguridad rentables, explicando la forma de incluir requerimientos de seguridad en un SI en las fases adecuadas del CVDS. Las 5 fases básicas del CVDS son definidas por el NIST SP800-18, Guía para el desarrollo de planes de seguridad para sistemas de TI y son:

- Iniciación
- Adquisición/Desarrollo
- Implementación
- Operación/Mantenimiento
- Disposición

El NIST 800-64 describe los pasos que pueden ayudar a integrar la seguridad de TI dentro del ciclo de vida de desarrollo de software (CVDS). Relaciona en cada fase del CVDS con los requerimientos técnicos y de seguridad. La tabla 5 **[39]** muestra cómo incorpora la seguridad dentro del CVDS:

	Comienzo	Adquisición / Desarrollo	Implementación	Operaciones / Mantenimiento	Disposición

CVDS	• Determinación de necesidades
	  ○ Percepción de una necesidad.
	  ○ Vinculación de las necesidades con la misión y objetivos de rendimiento.
	  ○ Evaluación de Alternativas de los Bienes de Capital
	  ○ Preparación para el Análisis de Inversión y Presupuesto
		• Declaración funcional de la necesidad
		• Investigación de mercado
		• Estudio de factibilidad
		• Análisis de requerimientos
		• Análisis de alternativas
		• Análisis costo-beneficio
		• Estudio del cambio de software
		• Análisis de costos
		• Planeación de la administración del riesgo
		• Planeación de adquisiciones
			• Instalación
			• Inspección
			• Pruebas de Aceptación
			• Entrenamiento inicial al usuario
			• Documentación
				• Medición del Rendimiento
				• Modificaciones Contractuales
				• Operaciones
				• Mantenimiento
					• Oportunidad de Disposición
					• Intercambio y venta
					• Selección interna de la Organización
					• Transferencia y Donación
					• Cierre de Contrato

Consideraciones de Seguridad	• Clasificación de la Seguridad • Evaluación preliminar del riesgo	• Evaluación del Riesgo • Análisis de requerimientos funcionales de seguridad • Análisis de requerimientos de garantías de seguridad • Consideraciones de costos y generación de informes • Planeación de la seguridad • Desarrollo de controles de seguridad • Desarrollo de Pruebas y evaluación de Seguridad • Otros componentes de planeación	• Inspección y aceptación • Integración de los controles de seguridad • Certificación de seguridad • Acreditación de seguridad	• Administración de la configuración y controles • Monitoreo continuo	• Preservación de la Información • Limpieza de medios • Eliminación de hardware y software

Tabla 5.- Consideraciones de seguridad a lo largo del ciclo de vida de desarrollo de software propuesto por el NIST SP 800-64.

Cada una de estas cinco fases incluye un conjunto mínimo de medidas de seguridad necesarias para incorporar de manera efectiva la seguridad en un sistema durante su desarrollo.

Iniciación

En la primera fase del ciclo de vida, el cual contempla las tareas de Categorización de Seguridad y una evaluación preliminar del Riesgo.

- **La categorización de Seguridad:** define tres niveles de impacto potencial (bajo, moderado o alto) sobre la organización o los individuos en caso de existir una violación de seguridad (pérdida de confidencialidad, integridad o disponibilidad). El estándar de categorización de la seguridad apoya a las organizaciones en la selección apropiada de los controles de seguridad para sus SI.

- **Evaluación Preliminar de Riesgo:** Esta actividad da lugar a la descripción inicial de las necesidades básicas de seguridad del sistema. Una evaluación preliminar del riesgo debe definir el entorno de amenazas en los que el SI deberá funcionar.

Adquisición/Desarrollo

Durante la fase de adquisición y desarrollo se consideran las tareas de:

- **Evaluación del riesgo:** análisis que identifica los requisitos de protección para el sistema a través de un proceso de evaluación de riesgos formal. Este análisis se basa en la evaluación inicial de riesgos realizada durante la fase de iniciación, pero es más profundo y específico.

- **Análisis de requerimientos funcionales de seguridad:** análisis de las necesidades que pueden incluir los siguientes componentes: (1) de entorno de seguridad del sistema (información de la empresa, política de seguridad y arquitectura de seguridad de la empresa) y (2) requerimientos de seguridad funcional

- **Análisis de requerimientos de las garantías de seguridad:** el análisis de requerimientos se ocupan de las actividades de desarrollo requeridas y el aseguramiento de la evidencia necesaria para producir el nivel de confianza deseado en que la seguridad de la información funcionará correctamente y con eficacia.

- **Consideraciones de costos y generación de informes:** determina la cantidad del costo de desarrollo que puede atribuirse a la seguridad de la información sobre el ciclo de vida del sistema. Estos costos incluyen hardware, software, personal, y capacitación.

- **Planeación de la seguridad:** asegura que los controles de seguridad acordados y planificados estén completamente documentadas. El plan de seguridad también ofrece una descripción del SI, así como archivos adjuntos o referencias a los documentos importantes que apoyan el programa de la organización de seguridad de la información. Por ejemplo, el plan de gestión de la configuración, plan de contingencia, plan de respuesta a incidentes, la conciencia de seguridad y un plan de formación, las normas de la conducta, la evaluación del riesgo, autorizaciones y acreditaciones, y un plan de acción y metas.

- **Desarrollo de controles de seguridad:** garantiza que los controles de seguridad descritos en los correspondientes planes de seguridad, son diseñados, desarrollados e implementados. Para los SI actualmente en operación, los planes de seguridad para estos sistemas pueden derivar el desarrollo de controles de seguridad adicionales para complementar los controles ya existentes o la modificación de los controles seleccionados que se consideran menos eficaces.

- **Desarrollo de pruebas y evaluación de seguridad:** garantiza que los controles de seguridad desarrollados para un nuevo SI funcionan correctamente y son eficaces.

- **Otros componentes de planeación:** asegura que todos los componentes necesarios del proceso de desarrollo son considerados cuando se incorpora la seguridad en el ciclo de vida. Estos componentes incluyen la selección del tipo de contrato correspondiente, la participación de todos los grupos funcionales necesarios dentro de una organización, la participación por el certificador y acreditador, y el desarrollo y ejecución de los planes de contratación y procesos necesarios.

Implementación

Durante la fase de implementación se consideran las tareas de:

- **Inspección y aceptación:** asegura que la organización valida y verifica que la funcionalidad descrita en las especificaciones se incluye en el producto final.

- **Integración de los controles de seguridad:** asegura que los controles de seguridad son integrados en el centro de operación donde el SI será implementado para operar. La configuración de los controles de seguridad se habilitará de acuerdo con las instrucciones del fabricante y las guías de implementación de seguridad disponibles.

- **Certificación de seguridad:** se asegura de que los controles se apliquen efectivamente a través de técnicas de verificación y procedimientos establecidos. De igual manera, da a los funcionarios de la organización la confianza de que las medidas que se han adoptado protegen el SI de la organización. Una certificación de Seguridad también descubre y describe las vulnerabilidades conocidas en el SI.

- **Acreditación de Seguridad:** proporciona la autorización de seguridad necesaria de un SI para procesar, almacenar, o transmitir la información que se requiere. Esta autorización se concede por un oficial de alto nivel de la organización y se basa en la verificación de la efectividad de los controles de seguridad a un nivel acordado de garantía y a un nivel de riesgo residual identificado para los activos u operaciones de la organización.

Operación/Mantenimiento

Durante la fase de Operación y Mantenimiento se consideran las siguientes tareas:

- **Administración y control de la configuración:** garantiza la adecuada consideración de los impactos potenciales de seguridad, debido a cambios específicos en un SI o de su entorno. La administración de la configuración y los procedimientos de configuración de control son fundamentales para establecer una base inicial de hardware, software y componentes de firmware para el SI y, posteriormente, controlar y mantener un inventario exacto de los cambios en el sistema.

- **Monitoreo continuo:** asegura que los controles siguen siendo eficaces en su aplicación a través de pruebas y evaluaciones periódicas. El monitoreo de controles de seguridad (es decir, verificar la eficacia permanente de los controles en el tiempo) y la comunicación del estado de seguridad del sistema de información para funcionarios de la organización son actividades esenciales de un programa de seguridad de la información global.

Disposición

Durante la fase de disposición se consideran las siguientes tareas:

- **Preservación de la Información:** garantiza que la información se conserva, según sea necesario, para ajustarse a los requisitos legales vigentes y para adaptarse a futuros cambios de tecnología que puede hacer que el método de recuperación sea obsoleto.

- **Limpieza de medios:** asegura que los datos se han eliminado, borrado, y sobre escritos conforme sea necesario.

- **Eliminación de hardware y software:** asegura que el hardware y el software son eliminados de la manera indicada por el funcionario de seguridad de la información del sistema.

3.4 Comentarios del Capítulo

La forma ideal de integrar seguridad a los SI, es tomando acciones a lo largo del Ciclo de vida mediante la adopción de un CVDS Seguro. En cada una de estas fases debe existir la participación activa por parte del área de seguridad, la cual validará y verificará la adecuada realización de las tareas de seguridad.

Desgraciadamente, en la actualidad existen muchos retos en la estructura, madurez y cultura organizacional, esto impide la correcta implementación de un modelo de desarrollo de software seguro. Los cambios se deben hacer gradualmente y requieren de un trabajo conjunto de las organizaciones, profesionistas y la academia, donde se cambie la manera de requerir, analizar, diseñar, desarrollar, probar e implementar los SI por parte de todos los elementos de la organización. Pasará todavía algún tiempo para que las organizaciones integren totalmente el CVDS Seguro en sus procesos de desarrollo de SI.

Por ello, se destaca la importancia de buscar una solución alternativa para dotar de seguridad a los SI en lo que se logra implementar los procesos internos de CVDS Seguro. La pregunta obligada es ¿De qué otras alternativas disponemos para ello? Tenemos 2 alternativas:

- **Tomar medidas reactivas:** Seguir trabajando como hasta ahora y mantener los SI expuestos a posibles amenazas y en el momento en que se detecte que el SI ha sido comprometido, tomar las acciones reactivas necesarias para corregir la vulnerabilidad explotada y poner de nuevo en operación el SI.

- **Tomar medidas preventivas:** Sea cual sea el modelo de desarrollo del SI, adoptar una auditoría de seguridad de SI, para evaluar el grado en que el SI cumple con los requerimientos mínimos de seguridad y determinar el grado de exposición del SI; de tal manera que la auditoría de seguridad arroje las vulnerabilidades encontradas en el SI y se tomen las medidas correctivas necesarias antes de poner en operación el SI.

Bajo este escenario, la alternativa para dotar de seguridad los SI en lo que se logra implementar un CVDS Seguro en la organización, e incluso como complemento de la adopción de un CVDS Seguro, es la adopción de una auditoría de seguridad de SI, para ello se propone una metodología de auditoría de seguridad de SI en los capítulos siguientes.

CAPÍTULO 4: REQUERIMIENTOS DE UNA AUDITORÍA DE SEGURIDAD PARA SISTEMAS DE INFORMACIÓN

Resumen

En este capítulo se presentan las definiciones correspondientes a los requerimientos mínimos funcionales y de seguridad que los SI deben contar. Los requerimientos funcionales se enfocan a que el SI cumpla con el objetivo para el que fue diseñado, mientras que los requerimientos de seguridad se enfocan a que el SI cuente con las funciones mínimas de seguridad para dar soporte a las operaciones provistas por SI. De igual manera, se introducen las consideraciones necesarias para evaluar el grado de cumplimiento de los Requerimientos Funcionales y de Seguridad de los SI; es decir validar la existencia y suficiencia de funciones, medidas y controles implementados en el SI para dar respuesta a los requerimientos funcionales y de seguridad descritos. Finalmente se concluye el capítulo con los errores de software más comunes en los SI.

4.1 Requerimientos mínimos funcionales y de seguridad de un SI

Un requerimiento o también llamado requisito, es una descripción de las necesidades o deseos que debe cumplir un SI. El objetivo de documentar un requerimiento es identificar lo que en realidad se necesita. Se debe expresar de manera que pueda ser fácilmente entendido por el cliente y el equipo de desarrollo. De igual manera, la definición de requisitos provee un común entendimiento del SI entre el dueño del SI y el equipo de desarrollo. Se recomienda aquí definir al menos los siguientes puntos:

- **Panorama general:** ¿Cómo encaja el SI en el sistema global? ¿Con qué otros sistemas debe interactuar?
- **Metas:** ¿Qué se espera lograr con la implementación del SI?
- **Funciones del sistema:** ¿Qué es lo que debe hacer el SI?
- **Atributos del sistema:** ¿Cuáles son las características que debe contar el SI?

Comúnmente, suele agruparse los requerimientos de un SI, en funcionales y no funcionales, para fines didácticos, en este capítulo agruparemos a los requisitos funcionales y no funcionales en los Requerimientos funcionales del SI

Un SI debe cumplir no sólo con los requerimientos funcionales del SI, además de ellos, debe cubrir un conjunto de requisitos mínimos de seguridad, los cuales garanticen que el SI cubre con las necesidades funcionales para las que fue diseñado y a su vez implementa un conjunto de controles de seguridad que dan soporte a la funcionalidad del SI.

4.1.1 Requerimientos mínimos funcionales de un SI

Requerimientos Funcionales

Ian Sommerville en el libro "Ingeniería de software" **[10]**, define un requerimiento funcional como toda característica requerida del sistema que expresa una capacidad de acción del mismo. Es decir, la funcionalidad que debe realizar el sistema; generalmente expresada en una declaración en forma verbal.

Un requerimiento funcional es la declaración de los servicios que debe proporcionar el SI. Especifica la manera en que el SI debe reaccionar a determinadas entradas, la forma en que el SI debe comportarse en situaciones particulares. De igual manera, un requerimiento funcional puede declarar explícitamente lo que él SI no debe hacer.

Las funciones pueden clasificarse en tres categorías: evidentes, ocultas y superfluas. Las evidentes deben realizarse, y el usuario debe saber que se han realizado. Las ocultas también deben realizarse, y puede que no sean visibles para el usuario. Muchas de estas funciones se omiten (erróneamente) durante el proceso de obtención de requerimientos. Las superfluas son opcionales, y su inclusión no repercute significativamente en el costo ni en otras funciones.

Requerimientos no funcionales

Ian Sommerville**[10]**, define un requerimiento no funcional como un conjunto de restricciones de los servicios o funciones ofrecidas por el sistema (fiabilidad, tiempo de respuestas, capacidad de almacenamiento, etc.). En general, se refiera a todas aquellas características no funcionales que debe cubrir un SI, las cuales se aplican al sistema en su totalidad. Estos requisitos surgen de las necesidades específicas del usuario u organización, como son las políticas de la organización, necesidad de interoperabilidad, etc. De la definición anterior, se podría incluir en este rubro a los atributos de calidad que debe cubrir un SI, pero por practicidad y manejo en esta tesis se utilizará en un siguiente rubro correspondiente a los requerimientos de calidad de un SI.

Requerimientos de calidad

Los requerimientos de calidad varían de un SI a otro según el modelo de calidad que se esté utilizando. Para el caso de estudio de esta tesis, se define un requerimiento de calidad como todas aquellas características mínimas que un SI debe cubrir para que se considere de calidad. Para determinar las características mínimas que un SI debe alcanzar, se utilizará el modelo de calidad definido por el ISO 9126 (para ampliar información ver el apartado 2.6.3 de esta tesis), en general las características de calidad que cualquier SI debería cubrir son las mostradas en la figura 9.

Fig 9. Características de calidad de un Sistema de Información.

Como se puede apreciar en la figura 9 el modelo de calidad ISO 9126, incluye una característica de calidad relacionada a la funcionalidad. No se debe confundir los requerimientos funcionales con la funcionalidad incluida dentro de las características de calidad del ISO 9126, ya que los requerimientos funcionales hablan específicamente de las funciones y tareas que el SI debe realizar, mientras que la funcionalidad como atributo de calidad se refiere a que el producto final (SI), implementado para cubrir los requerimientos funcionales, es congruente con las sub-características funcionales de adecuación, exactitud, interoperabilidad, cumplimiento y seguridad.

4.1.2 Requerimientos mínimos de seguridad de un SI

No existe una regulación nacional en México acerca de los requerimientos mínimos de seguridad de la Información y los SI, por lo que en este trabajo se ha optado por utilizar la propuesta por el NIST en la Publicación FIPS PUB 199 para clasificar la seguridad de la información y el FIPS PUB 200 para determinar los Requerimientos Mínimos de Seguridad de los SI.

El NIST define un requerimiento de seguridad **[12]**, como los requerimientos percibidos en un SI que se derivan de las leyes, decretos, directivas, políticas, normas, instrucciones, regulaciones o procedimientos, o la misión de la organización/casos de negocio necesarios para garantizar la confidencialidad, integridad y disponibilidad de los información que es procesada, almacenada o transmitida.

Los requisitos mínimos de seguridad descritos por el FIPS PUB 200, cubren diecisiete áreas relacionadas con la seguridad con respecto a la protección de la confidencialidad, integridad y disponibilidad de los SI y la información procesada, almacenada y transmitida por estos sistemas. Las diecisiete áreas representan una amplia base, de un programa equilibrado de seguridad de la información que se ocupa de la gestión, operación y aspectos técnicos de la protección de la información y los SI. Estas áreas relacionadas definidas por el **FIPS PUB 200**, fueron mencionadas en el apartado 2.6.2 de esta tesis. Para ampliar la información correspondiente a cada una de las áreas sugeridas por el FIPS PUB 200, se recomienda consulta el apéndice F: FIPS PUB 200.

Para el cumplimiento de los requerimientos de seguridad, las organizaciones deben seleccionar e implementar los controles de seguridad apropiados para el SI conforme a la clasificación de la seguridad previamente realizada de la información y el SI auditado. Para ampliar la información de la clasificación de la información y de los SI revisar el apéndice E: FIPS PUB 199.

Se eligieron los requerimientos mínimos de seguridad para los SI presentados en el estándar FIPS PUB 200, debido a que el NIST presenta como complemento a este, el estándar NIST SP 800-53 para la selección e implementación de controles de seguridad. El NIST SP 800-53 agrupa los controles de seguridad recomendados para la información y SI que pueden implementarse para cubrir los requerimientos mínimos de seguridad para los SI.

De igual manera, se hizo una comparativa entre los estándares y mejores prácticas FIPS PUB 200, ISO/IEC 15408, ISO/IEC 27002, COBIT, OSSTMM y la guía de pruebas OWASP, y se encontró que los requisitos mínimos de seguridad

presentados por el estándar FIPS PUB 200 coinciden con los aspectos presentados por los demás estándares.

En las siguientes tablas, se muestra la correspondencia de los requisitos mínimos de seguridad propuestos en esta tesis (**FIPS PUB 200**) y los aspectos considerados en los estándares y mejores prácticas de seguridad y auditoría informática presentados en el capítulo 2.6.2. En las tablas 6 y 7 se muestra la correspondencia entre los requerimientos de seguridad propuestos por el FIPS PUB 200 y los estándares ISO/IEC 27002, ISO/IEC 15408 y COBIT en su objetivo de control de alto nivel DS5 "Garantizar la seguridad de los Sistemas". En la tabla 8 se muestra la correspondencia entre los requerimientos de seguridad propuestos por el FIPS PUB 200 y el manual de metodología abierta de evaluación de seguridad OSSTMM y la guía de pruebas OWASP.

Estándares y Mejores Prácticas			
Dominios sugeridos	**FIPS PUB 200**	**ISO/IEC 27002**	**ISO/IEC 15408**
	1. Control de acceso (AC)	11.- Control de Acceso	FPR- Privacidad FTA- Acceso al objetivo de evaluación
	2. Sensibilización y Formación (AT)		
	3. Auditoría y Rendición de Cuentas (AU)		FAU- Auditoría
	4. Certificación, Acreditación y evaluaciones de Seguridad (CA)		
	5. Gestión de la Configuración (CM)	10.- Gestión de Comunicaciones y operaciones	
	6. Planes de Contingencia (CP)	14.- Gestión de la continuidad del negocio	
	7. Identificación y autenticación (IA)		FIA- Identificación y autenticación de usuario
	8. Respuesta a Incidentes (IR)	13.- Gestión de incidentes en la seguridad de la información	
	9. Mantenimiento (MA)	12.- Adquisición, desarrollo y mantenimiento de los SI	
	10. Protección de Medios (MP)		
	11. Protección física y Ambiental (PE)	9.- Seguridad Física y ambiental	
	12. Planificación (PL)		FCS- Soporte criptográfico FMT- Gestión de la seguridad FRU- Utilización de recursos
	13. Personal de Seguridad (PS)		
	14. Evaluación de Riesgos (RA)		
	15. Adquisición de sistema y servicios (SA)	12.- Adquisición, desarrollo y mantenimiento de los SI	FTP- Canales seguros FRU- Utilización de recursos
	16. Protección de Sistemas y Comunicaciones (SC)	10.- Gestión de Comunicaciones y operaciones	FCO- Comunicaciones FCS- Soporte criptográfico FPT- Protección de las funciones de seguridad
	17. Integridad de Sistema y la información (SI)		FDP- Protección de datos de usuario

Tabla 6.- Correspondencia entre Requerimientos mínimos de Seguridad propuestos por el FIPS PUB 200.

Estándares y Mejores Prácticas		
Dominios sugeridos	**FIPS PUB 200**	**COBIT** **DS5: Garantizar la Seguridad de Sistemas**
	1. Control de acceso (AC)	DS5.3 Administración de identidad
	2. Sensibilización y Formación (AT)	
	3. Auditoría y Rendición de Cuentas (AU)	
	4. Certificación, Acreditación y evaluaciones de Seguridad (CA)	
	5. Gestión de la Configuración (CM)	DS5.8 Administración de llaves criptográficas
	6. Planes de Contingencia (CP)	
	7. Identificación y autenticación (IA)	
	8. Respuesta a Incidentes (IR)	DS5.6 Definición de incidente de seguridad
	9. Mantenimiento (MA)	
	10. Protección de Medios (MP)	DS5.7 Protección de la tecnología de seguridad
	11. Protección física y Ambiental (PE)	
	12. Planificación (PL)	DS5.1 Administración de la seguridad de TI DS5.2 Plan de seguridad de TI DS5.8 Administración de llaves criptográficas DS5.4 Administración de cuentas del usuario DS5.8 Administración de llaves criptográficas
	13. Personal de Seguridad (PS)	
	14. Evaluación de Riesgos (RA)	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
	15. Adquisición de sistema y servicios (SA)	
	16. Protección de Sistemas y Comunicaciones (SC)	DS5.9 Prevención, detección y corrección de software malicioso DS5.10 Seguridad de la red
	17. Integridad de Sistema y la información (SI)	DS5.11 Intercambio de datos sensitivos DS5.5 Pruebas, vigilancia y monitoreo de la seguridad

Tabla 7.- Correspondencia entre Requerimientos mínimos de Seguridad propuestos por el FIPS PUB 200(2).

Mejores Prácticas para la evaluación de la seguridad.			
Dominios sugeridos	**FIPS PUB 200**	**OSSTMM**	**Guía de Pruebas OWASP**
	1. Control de acceso (AC)		5. Pruebas de autorización
	2. Sensibilización y Formación (AT)		
	3. Auditoría y Rendición de Cuentas (AU)		
	4. Certificación, Acreditación y evaluaciones de Seguridad (CA)		
	5. Gestión de la Configuración (CM)		2. Pruebas de gestión de la configuración
	6. Planes de Contingencia (CP)		
	7. Identificación y autenticación (IA)		4. Pruebas de autenticación
	8. Respuesta a Incidentes (IR)		
	9. Mantenimiento (MA)		
	10. Protección de Medios (MP)		
	11. Protección física y Ambiental (PE)	6. Seguridad Física	
	12. Planificación (PL)		
	13. Personal de Seguridad (PS)		
	14. Evaluación de Riesgos (RA)		
	15. Adquisición de sistema y servicios (SA)		
	16. Protección de Sistemas y Comunicaciones (SC)	2. Seguridad de los Procesos 3. Seguridad en las comunicaciones 5. Seguridad Inalámbrica	
	17. Integridad de Sistema y la información (SI)	1. Seguridad de la Información	7. Pruebas de validación de datos

Tabla 8.- Correspondencia entre Requerimientos mínimos de Seguridad propuestos por el FIPS PUB 200(3).

4.2 Cumplimiento de los Requerimientos mínimos Funcionales y de Seguridad de un SI

La decisión de operación se limita a 3 posibilidades:

- El SI cumple con los requerimientos mínimos, por lo que **se autoriza la operación** del SI,
- El SI no cumple con los requisitos mínimos funcionales y de seguridad, por lo que **no se autoriza la operación** del SI y el SI es regresado al equipo de desarrollo para corregir las vulnerabilidades encontradas y dar seguimiento a las recomendaciones realizadas por el equipo auditor,
- El SI no cumple con los requisitos mínimos funcionales y de seguridad, pero es una prioridad para la organización que el SI sea puesto en producción, por lo que se emite una **autorización condicionada**, es decir que el SI puede ser puesto en operación bajo ciertas condiciones y limitaciones.

Cumplimiento de los Requerimientos de Seguridad

Para el cumplimiento de los requerimientos de seguridad, las organizaciones deben seleccionar e implementar los controles de seguridad apropiados para el SI conforme a la clasificación de la seguridad previamente realizada de la información y el SI auditado. Para ampliar la información de la clasificación de la información y de los SI revisar el apéndice E: FIPS PUB 199.

Para validar el cumplimiento de los controles de seguridad, se deberán ejecutar un conjunto de actividades por parte del auditor para determinar el grado de efectividad con el que un control de seguridad se implementa, funcionando según lo previsto, y produciendo los resultados deseados respecto al cumplimiento de los requerimientos de seguridad definidos para el SI.

La severidad y extensión de esta evaluación del cumplimiento dependerá de la clasificación de la Información y del SI auditado, así como los objetivos planteados por la auditoría.

4.3 Selección de controles de seguridad

La clasificación de la información y del SI serán un factor determinante en la selección y aplicación de los controles de seguridad en el SI. Esta clasificación de la información y de los SI se deberá determinar conforme a los procedimientos internos de cada organización; de no contar con los procedimientos internos de clasificación de la información se sugiere utilizar los definidos por el NIST en la Publicación FIPS PUB 199, donde clasifica la información y los SI de acuerdo al nivel de impacto de los objetivos de seguridad (integridad, confidencialidad y disponibilidad) en las operaciones, activos e individuos. Para ampliar la información con respecto al FIPS PUB 199 se recomienda revisar el apéndice E: FIPS PUB 199.

Tras el proceso de clasificación de seguridad de la información y los SI, la organización deberá seleccionar un conjunto apropiado de controles de seguridad para sus SI que satisfagan los requerimientos mínimos de seguridad establecidos correspondientes a la clasificación de seguridad del SI.

Algunos de los controles que se pueden considerar como guías para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones se encuentran contenidos en los estándares y mejores prácticas como ISO 27002, COBIT, NIST SP 800-53 entre otros. De igual manera, la propia organización podría proponer y desarrollar el conjunto de controles específicos y adecuados para los SI de la propia organización.

Es importante mencionar que aunque los controles seleccionados por cualquier estándar son importantes y deben de ser considerados, se debe determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo de la organización.

4.4 Errores de Programación más Peligrosos en los SI

Otro aspecto importante a evaluar en una auditoría de seguridad de SI, es la revisión de que el SI auditado está libre de los errores de programación más comunes y peligrosos que pueden conducir a graves deficiencias de software. Existen varias fuentes de las publicaciones de las vulnerabilidades más comunes en los SI. Para esta tesis, se propone la lista emitida anualmente por el Instituto SANS, la cual presenta la descripción detallada de los 25 principales errores de programación, junto a una guía recomendada para mitigarlos y evitarlos.

El sitio Web CWE[7], publica anualmente una lista de los errores de programación más comunes que pueden conducir a graves vulnerabilidades de software **[40]**; el último artículo presentado lleva por título '2010 CWE/SANS Top 25 Most Dangerous Programming Errors'. También en esta lista se presentan las descripciones detalladas de los 25 principales errores de programación, junto con una guía recomendada para mitigarlos y evitarlos. La lista es el resultado de la colaboración entre SANS, MITRE, y expertos destacados de software de seguridad en los EE.UU. y Europa. MITRE mantiene el sitio web CWE (Common Weakness Enumeration), con el apoyo del Departamento de Seguridad Interna Nacional de la División de Seguridad Cibernética de los EUA. El sitio también contiene información sobre más de 800 errores de programación adicionales, errores de diseño, arquitectura y los errores que pueden llevar a vulnerabilidades explotables. Esta lista es una herramienta para la educación y sensibilización que apoya a los programadores a prevenir los tipos de vulnerabilidades que afectan a la industria del software.

El Top 25 está organizado en tres categorías de alto nivel que contienen entradas CWE múltiples:

- Interacción insegura entre componentes
- Gestión riesgosa de los recursos
- Defensas Insuficientes

A continuación se describe cada una de las categorías y se enlistan los errores más comunes conforme al Top 25 correspondientes a cada categoría. La posición que corresponde dentro del top 25 de cada CWE se encuentra denotada por RNK-XX, donde XX es la posición que ocupa en el ranking.

[7] http://cwe.mitre.org/

Interacción insegura entre componentes

Las vulnerabilidades en esta categoría se relacionan con formas poco seguras en la cuales se envían y reciben los datos entre componentes, módulos, programas, procesos, hilos (ejecución simultanea de procesos) o sistemas aislados.

1. CWE-79 (Failure to Preserve Web Page Structure, 'Cross-site Scripting'): Error al preservar la Estructura de la página Web. (RNK-01).
2. CWE-89 (Failure to Preserve SQL Query Structure, 'SQL Injection'): Error al preservar la estructura de las consultas SQL. (RNK-02).
3. CWE-352 (Cross-Site Request Forgery, 'CSRF'): Falsificación de petición en sitios cruzados. (RNK-04).
4. CWE-434 (Unrestricted Upload of File with Dangerous Type): Carga de archivos no restringida con posible contenido malicioso. (RNK-08).
5. CWE-78 (Improper Sanitization of Special Elements used in an OS Command, 'OS Command Injection'): Incorrecta validación y discriminación de elementos especiales utilizados en comandos del sistema operativo. (RNK-09).
6. CWE-209 (Information Exposure Through an Error Message): Revelación de información a través de Mensajes de error. (RNK-16).
7. CWE-601 (URL Redirection to Untrusted Site 'Open Redirect'): Redireccionamiento URL a Sitios no confiables. (RNK-23).
8. CWE-362 (Race Condition): Condición de Competencia. (RNK-25).

Gestión Riesgosa de Recursos

Las vulnerabilidades en esta categoría se relacionan con las formas en las que el software maneja inapropiadamente la creación, uso, transferencia o destrucción de recursos importantes del sistema.

1. CWE-120 (Buffer Copy without Checking Size of Input 'Classic Buffer Overflow'): Copiado del Buffer sin validación del tamaño de entrada. (RNK-03).

2. CWE-22 (Improper Limitation of a Pathname to a Restricted Directory 'Path Traversal'): Limitación inapropiada de una ruta a un directorio restringido. (RNK-07).
3. CWE-805 (Buffer Access with Incorrect Length Value): Acceso de Buffer con un valor de longitud incorrecto. (RNK-12).
4. CWE-754 (Improper Check for Unusual or Exceptional Conditions): Validación Inapropiada para condiciones excepcionales o inusuales. (RNK-13).
5. CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion'): Control inapropiado de un nombre archivo para las sentencias Include/Require en programas PHP. (RNK-14).
6. CWE-129 (Improper Validation of Array Index): Validación inapropiada de los índices de un arreglo. (RNK-15).
7. CWE-190 (Integer Overflow or Wraparound): Desbordamiento de enteros o Wraproud. (RNK-17).
8. CWE-131 (Incorrect Calculation of Buffer Size): Calculo incorrecto del tamaño de Buffer. (RNK-18).
9. CWE-494 (Download of Code Without Integrity Check): Descarga de código sin validación de integridad. (RNK-20).
10. CWE-770 (Allocation of Resources Without Limits or Throttling): Reservación de recursos de manera ilimitada. (RNK-22).

Defensas Inconsistentes

Las vulnerabilidades en esta categoría se relacionadas con las técnicas de defensa que a menudo son violadas, utilizados incorrectamente o simplemente ignoradas.

1. CWE-285 (Improper Access Control (Authorization)): Control de acceso inadecuado (autorización). (RNK-05)
2. CWE-807 (Reliance on Untrusted Inputs in a Security Decision): Dependencia en entradas no confiables en una decisión de seguridad. (RNK-06).

3. CWE-311 (Missing Encryption of Sensitive Data): Falta de cifrado en datos sensibles. (RNK-10).
4. CWE-798 (Use of Hard-coded Credentials): Uso de "código duro" en las credenciales de autenticación. (RNK-11).
5. CWE-306 (Missing Authentication for Critical Function): Ausencia de autenticación para funciones críticas. (RNK-19).
6. CWE-732 (Incorrect Permission Assignment for Critical Resource): Incorrecta asignación de permisos para los recursos críticos. (RNK-21).
7. CWE-327 (Use of a Broken or Risky Cryptographic Algorithm): Uso de un Algoritmo criptográfico descifrado. (RNK-24).

En la actualidad, los SI se han convertido en el blanco preferido por los atacantes, debido a que el mayor número de vulnerabilidades encontradas en estos SI, son vulnerabilidades ya conocidas, documentadas y ampliamente difundidas, para muestra de ello, se encuentra el "Top 25" presentado en este apartado.

La mayoría de las veces las vulnerabilidades encontradas en los SI resultan de un mismo origen, el desconocimiento de las implicaciones y prácticas de seguridad por parte de los equipos que diseñan y desarrollan estos SI. Las publicaciones de vulnerabilidades más comunes, deberían ser tomadas como una herramienta de capacitación y sensibilización para los equipos de diseño y desarrollo, de manera que les permita prevenir las diferentes vulnerabilidades que afectan en la actualidad a la industria del software.

Un aspecto importante a considerar en cualquier proceso de perfeccionamiento en los SI, p.ej. el modelo de auditoría en seguridad propuesta en este trabajo de tesis, debería ser la revisión de que el SI auditado está libre de los errores de programación más comunes que pudieran ser utilizados para vulnerar la seguridad de las aplicaciones y comprometer la información que estas manejan.

En el modelo de auditoría propuesto en esta tesis, se propone utilizar como base de la revisión de que el SI está libre de vulnerabilidades, la lista emitida anualmente por el Instituto SANS: "CWE/SANS Top 25 Most Dangerous Programming Errors". Cabe aclarar que la utilización de cualquier lista de vulnerabilidades, deberá estar sujeta a una constante revaloración, actualización y readaptación en caso de ser necesario.

4.5 Cumplimiento documental del SI.

Otro aspecto importante a considerar en la auditoría de seguridad de SI, es el cumplimiento documental del SI.

Para uso de esta tesis, se define al cumplimiento documental como el conjunto de procedimientos, diseños, manuales, formatos y documentación de un SI, requeridos por la organización.

Este cumplimiento documental debe ser definido con anterioridad por la organización y las áreas relacionadas a los SI, como pueden ser: las áreas de diseño y desarrollo, las áreas de seguridad, las áreas de calidad, las áreas de mantenimiento, las áreas de auditoría, entre otras.

Entre los elementos que contemplan el cumplimiento documental se encuentran:

- Procedimientos de Operación
- Diseños funcionales
- Diseños técnicos
- Análisis de factibilidad
- Manual de Usuario
- Manual de Operación
- Plan de Instalación
- Clasificación de la información y SI
- Autorización de Operación
- Informes de Seguimiento
- Etc.

Es tarea de la organización y de las áreas correspondientes establecer los elementos que conforman el cumplimiento documental de un SI. Una vez establecido el cumplimiento documental para los SI organizacionales, es de vital importancia difundir este conocimiento a toda la organización.

4.6 Marco regulatorio del SI.

Un aspecto considerado en la auditoría de seguridad de SI, es el cumplimiento con el marco regulatorio del SI. El objetivo del cumplimiento regulatorio del SI es evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y a cualquier requerimiento de seguridad **[41]**. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país (es decir, flujo de datos entre fronteras). Se debe definir explícitamente, documentar y actualizar todos los requerimientos normativos relevantes para el SI. De igual manera, la organización debe definir y documentar los controles y responsabilidades individuales específicas para satisfacer estos requerimientos normativos. El cumplimiento normativo que todo SI debe considerar y al cual debe alinearse corresponde a:

1. Regulación internacional,
2. Regulación nacional,
3. Regulación por sector,
4. Regulación Institucional y
5. Regulación de validez oficial[8]

[8] En esta tesis, se agrupa bajo este término la regulación para procesos de acreditación y certificación

4.7 Comentarios del capítulo

4.7.1 Requerimientos mínimos de una auditoría de Seguridad de SI.

Los aspectos a evaluar en la auditoría de seguridad propuesta en esta tesis son:

- Cumplimiento de los **requerimientos mínimos funcionales**, estos se conforman de:

    1. Requerimientos funcionales: Se define a los requisitos funcionales, como las necesidades explicitas por parte de los dueños del SI acerca de la funcionalidad que el SI debe de cubrir, funciones que en su conjunto apoyan los procesos del negocio para los que fueron diseñados.

    2. Requerimientos no funcionales: Se define un requisito no funcional, como los atributos que le indican al sistema como realizar su trabajo. De igual manera se debe incluir las restricciones del SI.

    3. Requerimientos de calidad: Se define un requisito de calidad, como todas aquellas características de calidad que un SI debe cubrir, teniendo como base el modelo de calidad del ISO 9126.

- Cumplimiento de los **requerimientos mínimos de seguridad** de un SI, estos se conforman por los requerimientos relacionados con la protección de la confidencialidad, integridad y disponibilidad de los SI y la información procesada, almacenada y transmitida por estos sistemas. En esta tesis, se proponen los requerimientos mínimos definidos en el **FIPS PUB 200**, presentados en el apartado 2.6.2 y explicados en el apéndice F: FIPS PUB 200 de esta tesis.

- Revisión de que el **SI auditado está libre de los errores de programación más comunes y peligrosos que pueden conducir a graves deficiencias de software**. Se propone la lista emitida anualmente por el Instituto SANS: "CWE/SANS Top 25 Most Dangerous Programming Errors", esta lista presenta la descripción detallada de los 25 principales errores de programación, junto a una guía recomendada para mitigarlos y evitarlos.

- **Cumplimiento documental establecido por la organización**, el cual consiste de un conjunto de procedimientos, diseños, manuales, formatos y documentación de un SI, requeridos por la organización.

- **Cumplimiento regulatorio del SI**, cuyo objetivo es evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. Dentro de esta tesis se ha considerado el cumplimiento regulatorio presentado en el apartado 4.6.

Consideraciones de aplicación de los Requerimientos mínimos de un SI

Los elementos a evaluar por una auditoría de SI se pueden ver como un punto de inicio para desarrollar los lineamientos específicos de cada organización. No todos los controles y lineamientos pueden ser aplicables a la organización. Es más, se pueden requerir controles y lineamientos adicionales no incluidos en la definición anterior. Se requiere de un proceso de personalización de requerimientos y controles aplicables a la organización.

Es responsabilidad de la organización y las áreas correspondientes, definir el conjunto de requerimientos mínimos de seguridad con base en la determinación de la categoría de seguridad de los SI. Es decir, establecer el conjunto de requerimientos mínimos de seguridad para cada clasificación de seguridad de los SI. El procedimiento para determinar la categoría de seguridad de los SI debe ser previamente establecido y acatado por la organización, de no contar con este procedimiento se sugiere el propuesto por el FIPS PUB 199, que es el que se considera en esta tesis.

4.7.2 Evaluación del cumplimiento de los requerimientos mínimos de un SI

Una vez establecidos los requerimientos mínimos de un SI, será tarea del equipo auditor realizar el conjunto de actividades realizadas por el equipo de auditores para evaluar exhaustivamente el nivel de cumplimiento del SI con respecto a los requerimientos mínimos previstos para el SI, y con ello determinar el nivel de exposición del SI auditado(Riesgo del SI).

La profundidad de la evaluación del cumplimiento dependerá de la clasificación de seguridad de la información y del SI auditado.

Los criterios de evaluación del cumplimiento de los requerimientos mínimos deberán ser establecidos por la organización y deberán ser acatados por el equipo auditor.

4.7.3 Decisión de Operación de un SI, conforme al cumplimiento de los requerimientos mínimos del SI.

La decisión de operación de un SI[9], es la autorización formal de operación del SI auditado, conforme al cumplimiento de los requerimientos mínimos del SI y el nivel de riesgo del SI auditado.

La organización deberá determinar los criterios bajo los cuales se determinará la decisión de operación del SI, la cual considere la evaluación del cumplimiento de los requerimientos mínimos del SI y el nivel de riesgo del SI.

Las decisiones de operación de un SI consideradas en esta tesis son[10]:

- **Autorización para operar:** el SI cumple con los requerimientos mínimos y el nivel de riesgo del SI es aceptable, es decir, El SI está autorizado para operar sin ningún tipo de restricciones o limitaciones en su funcionamiento.
- **No autorizado para operar:** el SI no cumple con los requisitos mínimos y el nivel de riesgo del SI es inaceptable, por lo tanto no se autoriza la operación del SI y el este es regresado al equipo de desarrollo para corregir las vulnerabilidades encontradas y dar seguimiento a las recomendaciones realizadas por el equipo auditor,
- **Autorización condicionada:** el SI no cumple con los requisitos mínimos y el nivel de riesgo del SI es inaceptable, pero es una prioridad para la organización que el SI sea puesto en producción, por lo que se emite una autorización condicionada, es decir que el SI puede ser puesto en operación bajo ciertas condiciones y limitaciones, incluidas las medidas correctivas que deban adoptarse por el propietario del SI y un plazo de tiempo requerido para la realización de esas acciones.

[9] El NIST define en el estándar "NIST SP 800-37. Guía para la Certificación y Acreditación de los SI Federales de los EUA", el concepto de decisión de acreditación, este concepto ha sido adaptado a esta tesis bajo el concepto de decisión de operación de un SI.

[10] Las decisiones de operación establecidas en esta tesis, han sido adaptadas de la decisión de acreditación definidas por el NIST en el estándar "NIST SP-800-37. Guía para la Certificación y acreditación de los SI Federales de los EUA".

CAPÍTULO 5: DISEÑO Y DOCUMENTACIÓN DE UN MODELO DE AUDITORÍA EN SEGURIDAD PARA SISTEMAS DE INFORMACIÓN

Resumen

En este capítulo se plantea el diseño y documentación de un modelo de auditoría en seguridad para sistemas de información (SI), el cual estará orientado a revisar la existencia y suficiencia de los requerimientos mínimos de un SI. Adicionalmente, se incluye una aproximación de la aplicación del modelo de auditoría en los SI organizacionales. Para implementar el modelo de auditoría de seguridad propuesto, se establece una metodología para auditar la seguridad de un SI y para apoyar su implementación, se documentan los Procedimientos Operativos Estándar (POE) desarrollados para aplicar la metodología de auditoría de seguridad propuesta. De igual manera, se presenta un conjunto de recomendaciones generales propuestas para implementar este modelo de auditoría. Finalmente, se concluye el capítulo con la aplicación de la metodología propuesta en la auditoría de seguridad para SI.

5.1 Diseño y documentación de un modelo de auditoría en seguridad para SI.

Tomando las consideraciones planteadas a lo largo del desarrollo de esta tesis, se propone el modelo de auditoría de seguridad de SI contenido en la figura 10.

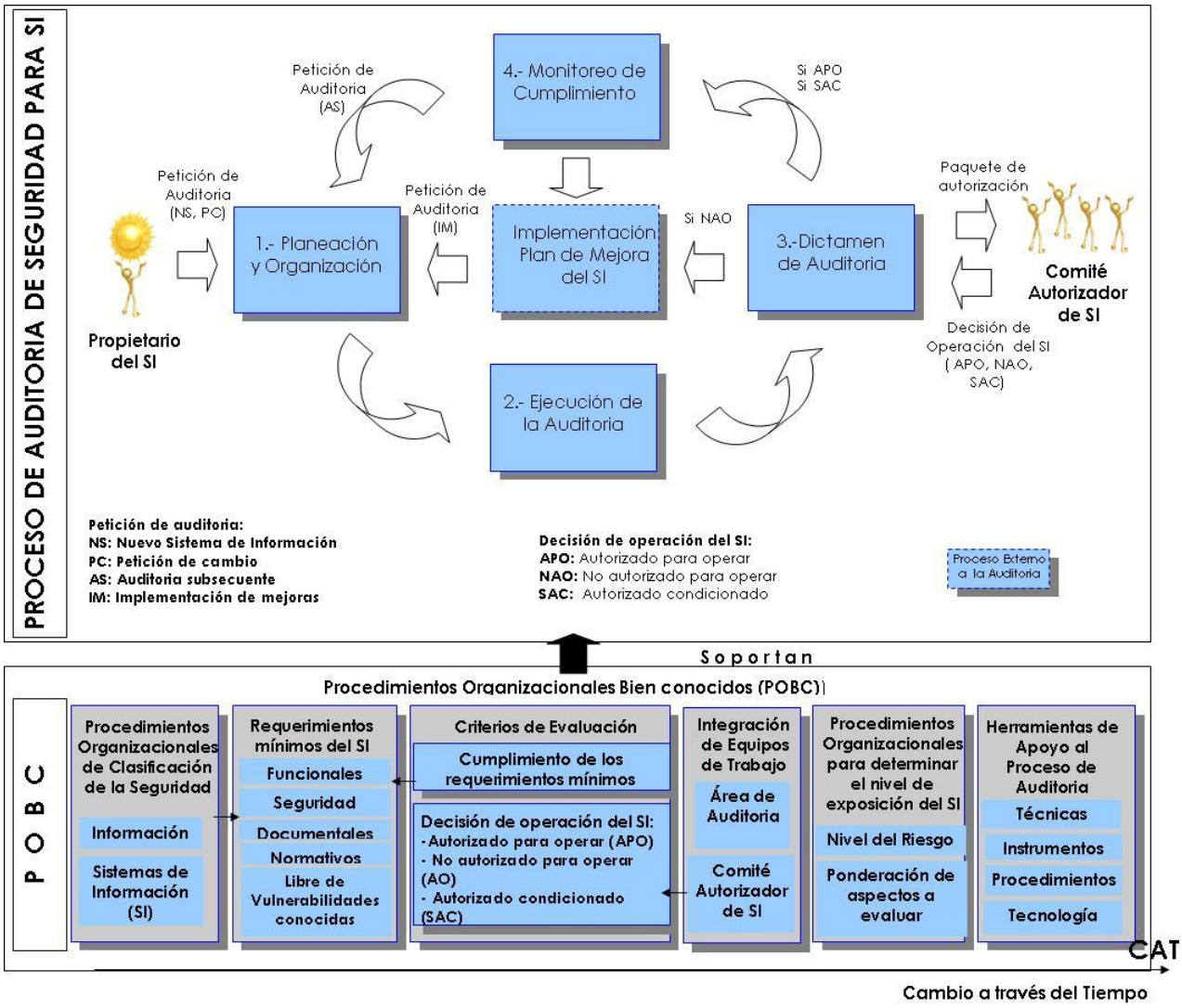


Fig 10. Modelo propuesto de auditoría en seguridad para Sistemas de Información.

5.2 Descripción del Modelo de auditoría en Seguridad para SI

El modelo de auditoría de seguridad de SI que se propone considera que la auditoría es un proceso interno encada organización, el cual puede tener especificidades durante su ejecución y aplicación. No obstante, en este apartado se presenta una aproximación de una posible aplicación del modelo propuesto, donde se definen responsables, entradas y salidas.

El modelo propuesto se divide en 2 grandes bloques:

1. Los Procedimientos Organizacionales Bien Conocidos (POBC) y
2. El proceso de Auditoría de Seguridad.

Procedimientos Organizacionales Bien Conocidos

POBC

Los POBC, son aquellos procedimientos y definiciones formales establecidas por la organización y con carácter de directiva, los cuales apoyan al proceso de auditoría de seguridad de SI; por lo que antes de realizar cualquier auditoría de seguridad de SI, es necesario que la organización defina los POBC que respalden el proceso de auditoría de sus SI.

Establecer los POBC en una organización conlleva a la estandarización de los aspectos considerados en las auditorías de seguridad de SI en la organización, lo que permite realizar un proceso más objetivo que los proporcionados por las auditorías tradicionales. Emplear los POBC proporciona una estandarización en el proceso de auditoría y permite la comparación de resultados de auditoría de seguridad entre SI similares.

Los POBC, pueden considerarse como un repositorio de procedimientos y lineamientos organizacionales considerados en el proceso de auditoría, de ahí el nombre de procedimientos organizacionales bien conocidos. Los POBC son importantes debido a que son la base del proceso de auditoría.

Los elementos que integran al POBC, se pueden apreciar en la figura 11.

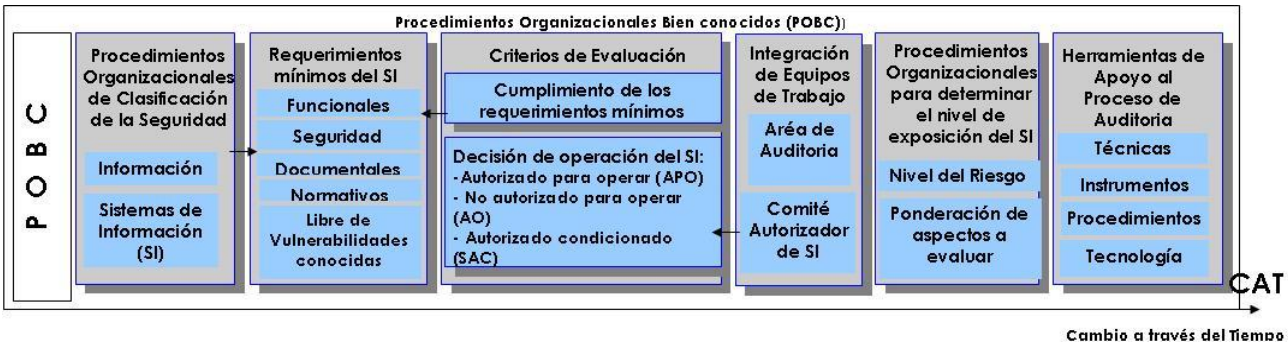


Fig 11. Elementos que conforman los Procedimientos Organizacionales Bien conocidos (POBC).

Componentes de los POBC

Los POBC definidos en el modelo propuesto se conforman por:

1. Procedimientos organizacionales para **clasificar la seguridad de la Información y los SI**: La organización deberá determinar los procedimiento organizacional aplicables para clasificar la seguridad de la información y de los SI auditados. Si la organización no cuenta con estos procedimientos, un punto de partida pueden ser los recomendados por el NIST documentado en el FIPS PUB 199(Para ampliar información revisar el apartado 2.6.2 de esta tesis).
2. Determinación de los **requerimientos mínimos del SI:** La organización deberá determinar los requerimientos mínimos de un SI que serán evaluados en la auditoría de seguridad del SI, conforme a la clasificación de seguridad de la información y los SI organizacionales. Los requerimientos mínimos deben considerar los aspectos funcionales, de seguridad, cumplimiento documental, marco normativo y revisión de que el SI está libre de las vulnerabilidades conocidas. Si la organización no cuenta con estos requerimientos mínimos del SI, un punto de partida pueden ser los recomendados en el capítulo 4 de esta tesis.
3. Establecimiento de los **criterios de evaluación organizacionales:** La organización deberá establecer los criterios de evaluación que el equipo de auditores utilizará para determinar el nivel de cumplimiento de los requerimientos mínimos de los SI auditados, así como determinar los criterios de evaluación que el comité autorizador deberá considerar en la toma de decisión de operación del SI (un punto de partida pueden ser los establecidos en el capítulo 4 de esta tesis).

Es decir, los criterios de evaluación organizacionales, definen formalmente la forma en que el equipo de auditores evaluará el grado de cumplimiento del SI, para ello se considera:

- Preparación de la evaluación: Implica la selección de las métricas apropiadas, definición de los niveles de evaluación y criterios de evaluación. Las métricas suelen dar lugar a medidas cuantificables asignadas a escalas. La definición de los niveles de evaluación determina qué rangos de valores en estas escalas cuentan como satisfactorio o insatisfactorio. La definición de los criterios de evaluación consiste en la preparación de un procedimiento para resumir los resultados de la evaluación para un entorno específico.
- Procedimiento de evaluación: se conforma de pasos: medición, calificación y evaluación. En la medición, las métricas seleccionadas se aplican a los SI y se evalúa sobre las escalas de las métricas obtenidas. Subsecuentemente, para cada valor medido, se determina el nivel de calificación. La evaluación es el paso final, donde se resume un conjunto de niveles previamente calificados. El resultado es un resumen del cumplimiento de los Requerimientos mínimos del SI.

4. Los POBC suponen la **integración de equipos de trabajo**: La organización deberá definir y documentar formalmente los procedimientos para integrar de los equipos de trabajo y definir las responsabilidades, funciones y limitaciones de los equipos de trabajo:
    - El **área de auditoría**, será conformada por un equipo de auditores y especialistas con un perfil altamente técnico y con conocimiento de la estructura organizacional. Es tarea de la organización definir los procedimientos y perfiles para conformar el área y equipo de auditoría de seguridad de SI, se propone que los perfiles del equipo de auditoría consideren amplios conocimientos en las áreas de informática, SI, entornos de desarrollo, seguridad y auditoría para adaptar la metodología al entorno en especifico en que se desarrolla. Finalmente, deberá existir independencia entre áreas, una de las premisas de la auditoría es que no se puede ser juez y parte; por lo que el equipo auditor debe ser diferente al equipo desarrollador.
    - Un **comité autorizador del SI**, para el modelo de auditoría propuesto, la figura del comité autorizador del SI, es de vital importancia ya que

en este reside la decisión de operación[11] del SI. El comité autorizador del SI, deberá ser un órgano conformado como mínimo por el líder de la auditoría, los responsables del área de seguridad de la información y un representante ejecutivo de la organización el cual pueda dar respaldo a la decisión tomada con respecto a la autorización de operación del SI. Es tarea de la organización determinar la conformación, responsabilidades y obligaciones del comité autorizador del SI.

5. Establecimiento de los procedimientos organizacionales para **determinar el nivel de exposición de los SI**: Es tarea de la organización determinar y documentar formalmente los procedimientos que serán interpretados como directivas para determinar el nivel de exposición de los SI, entre ellos se encuentran los procedimientos para determinar el nivel de riesgo del SI y la ponderación de aspectos a evaluar en el SI auditado.
6. Establecimiento de las **herramientas de apoyo al proceso de auditoría:** La organización deberá seleccionar, desarrollar cuando sea necesario y documentar formalmente, las herramientas de apoyo al proceso de auditoría. Las herramientas consideradas incluyen el uso de diversas técnicas, instrumentos y procedimientos manuales u automatizados, y tecnología aplicable. Se sugiere que en lugar de desarrollar herramientas únicas o especializadas y procedimientos para evaluar los controles de seguridad en el SI, se pueden consultar los métodos y procedimientos estandarizados[12] para evaluar los controles de seguridad, estos métodos y procedimientos pueden ser sumados a los definidos en este punto.

Lo único constante es el cambio: CAT

Una variable importante en el modelo propuesto es la consideración del Cambio a través del Tiempo (**CAT)**. Esta consideración supone que el ambiente de operación de los SI organizacionales no es constante y como tal, los POBC se encuentran en continua valoración, redefinición y adaptación de cualquiera de sus componentes, para responder a los cambios del entorno y ser reflejados dentro del proceso organizacional de auditoría de seguridad de los SI.

[11] Autorización formal de operación del SI auditado, conforme al cumplimiento de los requerimientos mínimos del SI y el nivel de riesgo del SI auditado.

[12] por ejemplo para los SI basados en WEB, el Manual de Metodología Abierta de Evaluación de Seguridad OSSTMM y la guía de evaluación del OWASP pueden ser de gran utilidad.

La tarea constante de adaptación de los POBC derivado del CAT es responsabilidad de la organización, quien deberá definir la periodicidad de revaloración y redefinición de los POBC. En el mismo sentido, se deberán definir las condiciones extraordinarias por las que se requerirá revalorar y redefinir de manera anticipada los POBC, como es el caso de la entrada en vigor de nuevas normas y estándares a los que la organización se tuviese que alinear.

Proceso de auditoría de Seguridad de SI

El proceso de auditoría de seguridad de SI se compone de 4 procesos principales, estos son:

1. Planeación y Organización
2. Ejecución de la Auditoría
3. Dictamen de Auditoría
4. Monitoreo de Cumplimiento

El proceso de auditoría de seguridad empieza con la petición de auditoría por parte del propietario del SI, el origen de la auditoría se puede deber a 4 motivos:

a) **Creación del SI**, con el fin de obtener la autorización de operación del SI auditado.
b) **Petición de cambio** a un SI que ya se encuentra operando, con el fin de obtener la autorización de operación del SI modificado, validando que los cambios realizados en el SI no aportan nuevas vulnerabilidades al SI.
c) **Implementación de mejoras**, es solicitada por el propietario del SI, una vez que este ha implementado las actividades contempladas en el plan de mejora[13], con el fin de obtener la autorización formal para que el SI auditado sea puesto en operación[14].
d) **Auditorías subsecuentes** de manera programada, para validar que los controles implementados en el SI son eficientes a través del tiempo.

[13] El plan de mejoras, es un documento generado por el líder de la auditoría en colaboración con el propietario del SI, en el cual se describen las medidas previstas para reducir el número de vulnerabilidades y corregir los aspectos negativos encontrados en la auditoría del SI.

[14] esta petición se origina debido a que previamente, se han realizado auditorías de seguridad al SI, pero los resultados indican que el SI no es apto para ser puesto en operación, por lo que el equipo auditor emite un plan de mejoras al propietario del SI para reducir las vulnerabilidades encontradas en este.

Planeación y Organización de la Auditoría: engloba las tareas de planeación, organización y preparación de recursos; así como las actividades y procedimientos necesarios para obtener la información del SI que servirá de base para ejecutar la auditoría. En esta fase se pretende identificar las razones por las que se realizará la auditoría y se definirá el objetivo que se persigue. De igual manera, se prepararán los documentos e instrumentos que servirán de apoyo en la ejecución de la auditoría. Finalmente este proceso culmina con la elaboración documental de los planes y programas de la auditoría. Una tarea importante del equipo auditor en esta etapa, es la determinación de los requerimientos mínimos aplicables al SI auditado, recordando que estos son establecidos en los POBC y se determinan conforme a la clasificación de la información y del SI auditado.

Ejecución de la auditoría: se refiere al conjunto de actividades realizadas por el equipo de auditores para evaluar exhaustivamente el nivel de cumplimiento del SI con respecto a los requerimientos mínimos previstos y, con ello, determinar el nivel de exposición del SI auditado. El objetivo de esta etapa es recopilar la evidencia de auditoría necesaria, mediante la aplicación de instrumentos y herramientas diseñadas para la auditoría(definidas en los POBC), la cual permita determinar el nivel de riesgo del SI auditado (conforme a los POBC) y con ello proponer las medidas correctivas al SI.

Dictamen de la auditoría: se refiere al conjunto de actividades realizadas para la confección y elaboración del informe y dictamen final. En este proceso se contempla la elaboración del plan de mejora del SI, el cual define una serie de tareas y actividades para eliminar o reducir el número de vulnerabilidades y aspectos negativos encontradas en la auditoría del SI. Este proceso concluye con la entrega del informe de auditoría a los propietarios del SI y al equipo de desarrollo a cargo del SI. Una de las tareas más importantes de este proceso es la toma de decisión de operación del SI por parte del comité autorizador de SI. Esta decisión se toma con base en la evidencia obtenida y la determinación del nivel de riesgo del SI, los cuales se obtienen del proceso de ejecución de auditoría.

Las posibles decisiones de operación, conforme a los POBC, que pueden ser otorgadas a un SI son:

1. Autorizado para operar (APO)
2. No autorizado para operar (NAO)
3. Autorizado condicionado (SAC)

Si la decisión de autorización del SI es "autorizado para operar" (APO) o "autorizado condicionado" (SAC) el siguiente proceso, dentro del modelo de

auditoría, es el Monitoreo de cumplimiento.

Si la decisión de autorización del SI es "no autorizado para opera" (NAO), el propietario del SI tendrá que realizar las actividades contenidas en el Plan de Mejora del SI en la forma y tiempo acordados mediante el proceso de Implementación de mejoras del SI[15]. Una vez que se implementen las acciones del Plan de Mejora del SI, el propietario del SI deberá solicitar una nueva auditoría de seguridad que evalúe el cumplimiento de las recomendaciones hechas en el plan de mejora de SI (Implementación de Mejoras).

El comité autorizador determinará la decisión de operación del SI auditado conforme a los criterios de evaluación definidos en los POBC, basándose en el análisis de los hallazgos obtenidos y el nivel de riesgo del SI auditado.

Monitoreo del Cumplimiento: se refiere a las actividades de seguimiento y monitoreo de las actividades definidas en el Plan de mejora para el SI auditado. En este proceso se incluye:

1. Programación de las **auditorías subsecuentes** del SI, considerando que el medio de operación del SI no es constante.
2. Definición de las actividades y responsabilidades de **monitoreo continuo a los controles** de seguridad implementados en el SI para determinar su nivel de eficaces a lo largo del tiempo.
3. El **seguimiento** al proceso **de Implementación de mejoras** a cargo del propietario del SI.

[15] El proceso de Implementación de mejoras del SI, es un proceso externo a la auditoría de seguridad del SI. Es responsabilidad del propietario del SI, definir las tareas y recursos requeridos para dar solución a las acciones planteadas en el Plan de Mejora del SI.

5.3 Aproximación del Proceso de auditoría de seguridad de SI

A continuación se describe una aproximación de la ejecución de cada una de las etapas del proceso de auditoría de seguridad de SI que sugiere el modelo propuesto. Cada una de estas aproximaciones considera las entradas, salidas, flujo del proceso y responsables de cada actividad.

En la figura 12, se describe la aproximación de la etapa 1 del modelo propuesto: **planeación y organización de la auditoría**. El actor que inicia el proceso con una petición de auditoría es el propietario del SI.

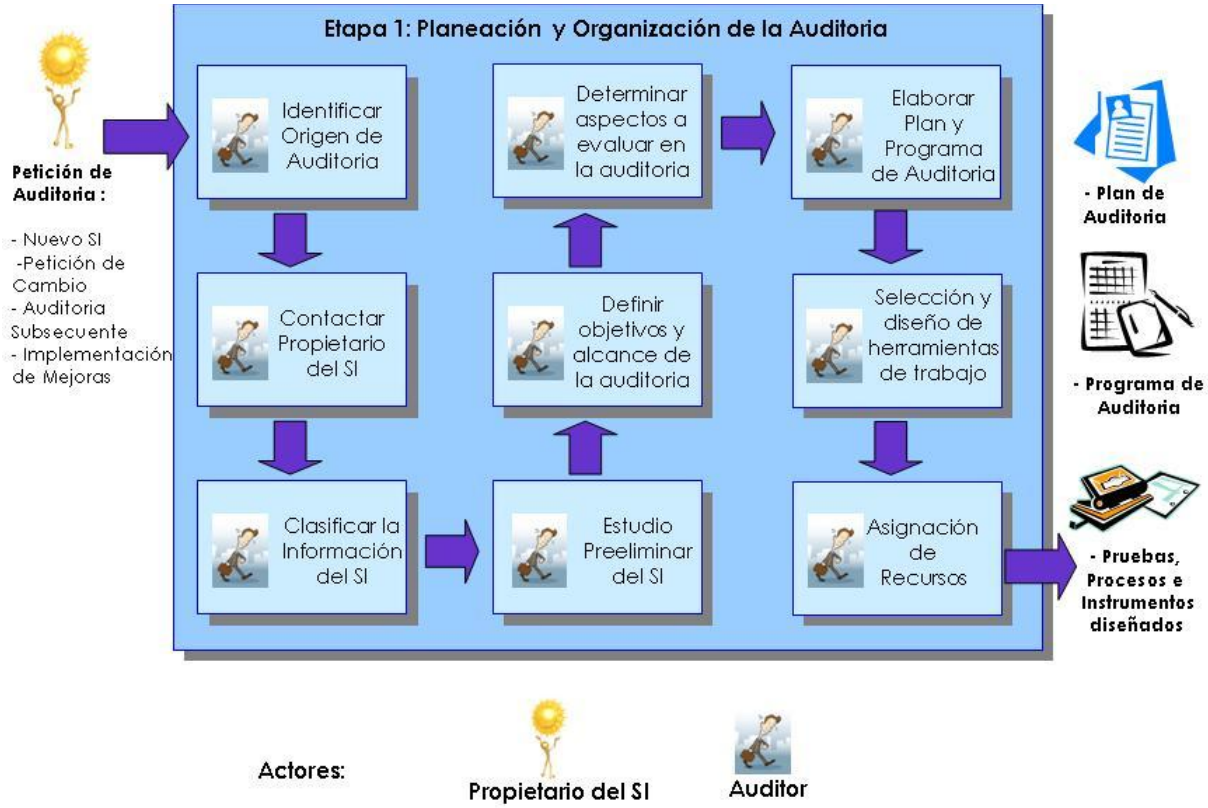


Fig 12. Aproximación de la etapa 1 del modelo propuesto de auditoría de seguridad de Sistemas de Información.

En la figura 13, se describe la aproximación de la etapa 2 del modelo propuesto, las entradas a la etapa de **ejecución de la auditoría** son los planes y programas de auditoría y las pruebas, procesos e instrumentos diseñados en la etapa 1.

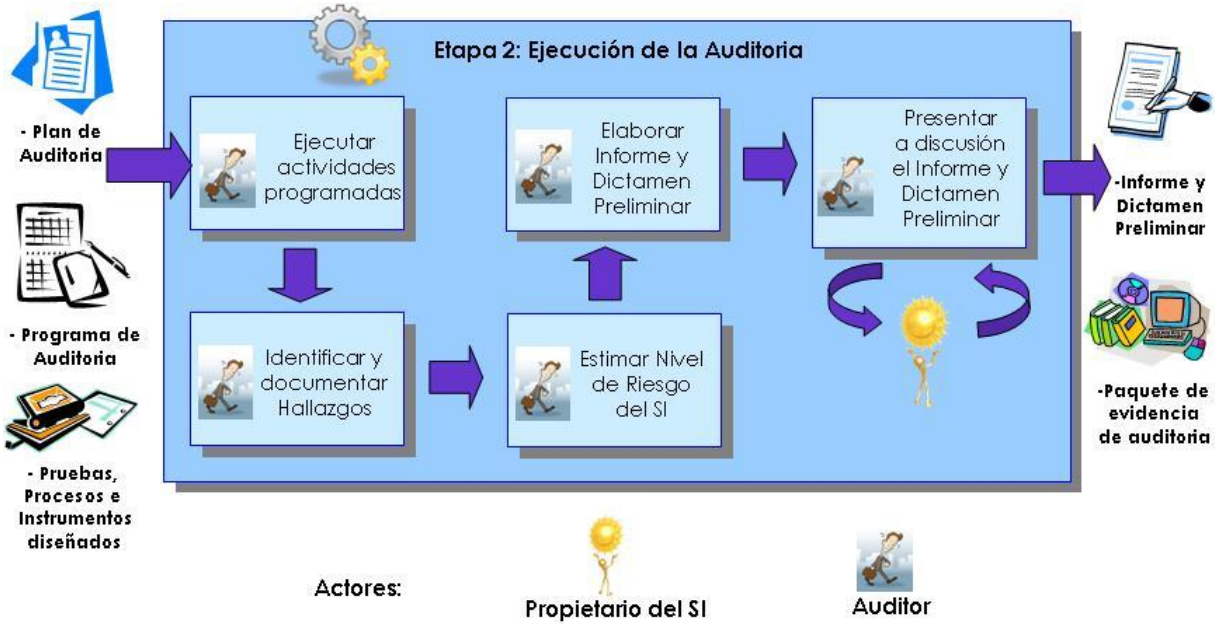


Fig 13. Aproximación de la etapa 2 del modelo propuesto de auditoría de seguridad de Sistemas de Información.

En la figura 14, se describe la aproximación de la etapa 3 del modelo propuesto. Las entradas a la etapa de **dictamen de la auditoría** son el Informe y dictamen preliminar y el paquete de evidencia de auditorías generadas en la etapa 2. Como se puede apreciar en la figura, existen 2 posibles rumbos que puede tomar la auditoría de seguridad propuesta:

- Si al presentar el informe y dictamen final de auditoría, la decisión es "No autorizado para opera", el propietario de auditoría de seguridad tendrá que empezar el proceso (externo a la auditoría) de "Implementar el Plan de Mejora del SI". En este proceso, el equipo de desarrollo implementará en tiempo y forma las actividades definidas dentro del plan de mejora. Una vez concluida la implementación del plan de mejora, el propietario del SI deberá solicitar nuevamente una auditoría del SI cuyo origen es la implementación de mejoras.

- Si al presentar el informe y dictamen final de auditoría, la decisión es "Autorizado para operar" o "Autorizado condicionado", la siguiente etapa de la auditoría de seguridad es el monitoreo del cumplimiento del SI.

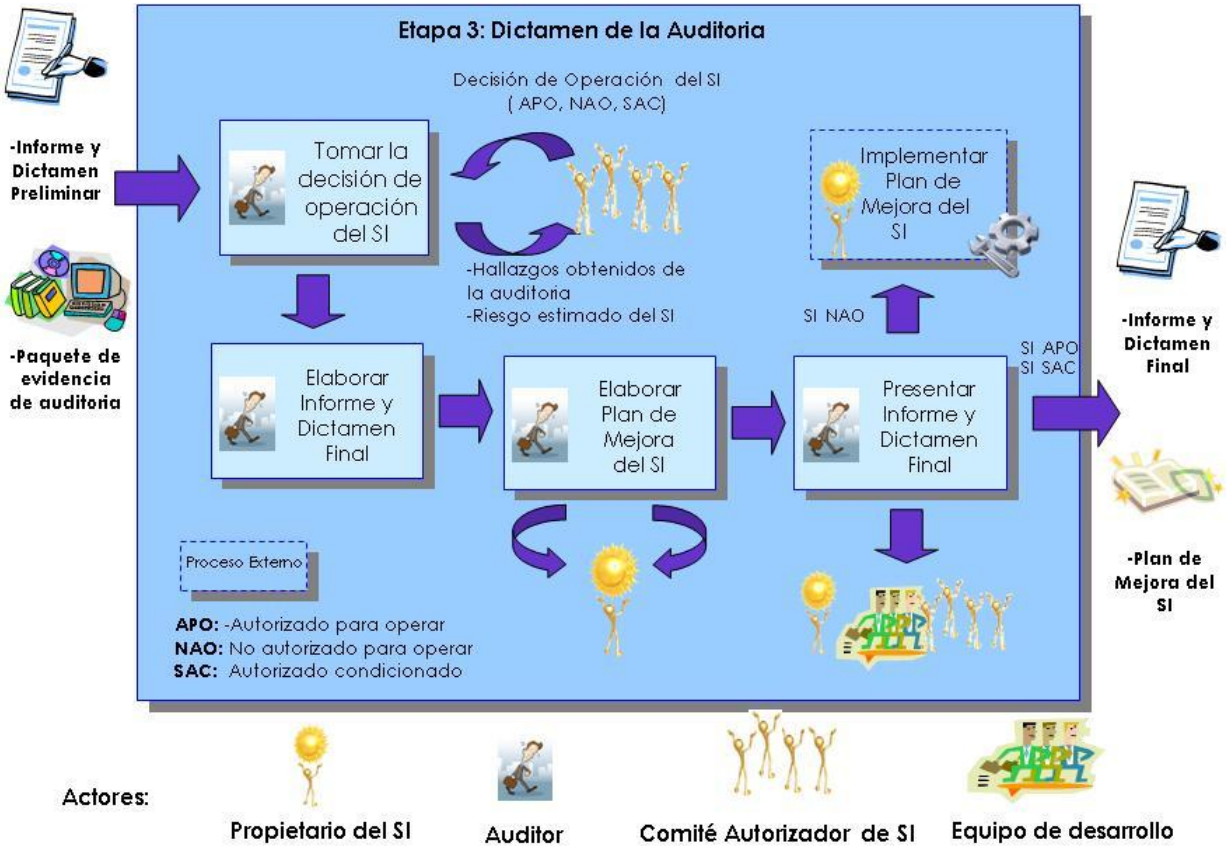


Fig 14. Aproximación de la etapa 3 del modelo propuesto de auditoría de seguridad de Sistemas de Información.

En la figura 15, se describe la aproximación de la etapa 4 del modelo propuesto. Las entradas a la etapa de **Monitorear cumplimiento del SI** son el informe y dictamen de auditoría, y el plan de mejora del SI generados en etapa 3.

En esta etapa el equipo auditor en conjunto con el propietario del SI, establecen y documentan los lineamientos, responsables y periodicidad de las actividades del seguimiento de la implementación del plan de mejora, programación de auditorías subsecuentes y el monitoreo continuo del cumplimiento de los controles de seguridad. Las actividades de la etapa 4 se llevan de manera paralela y concluyen con una petición de auditoría con el origen "Auditoría Subsecuente".

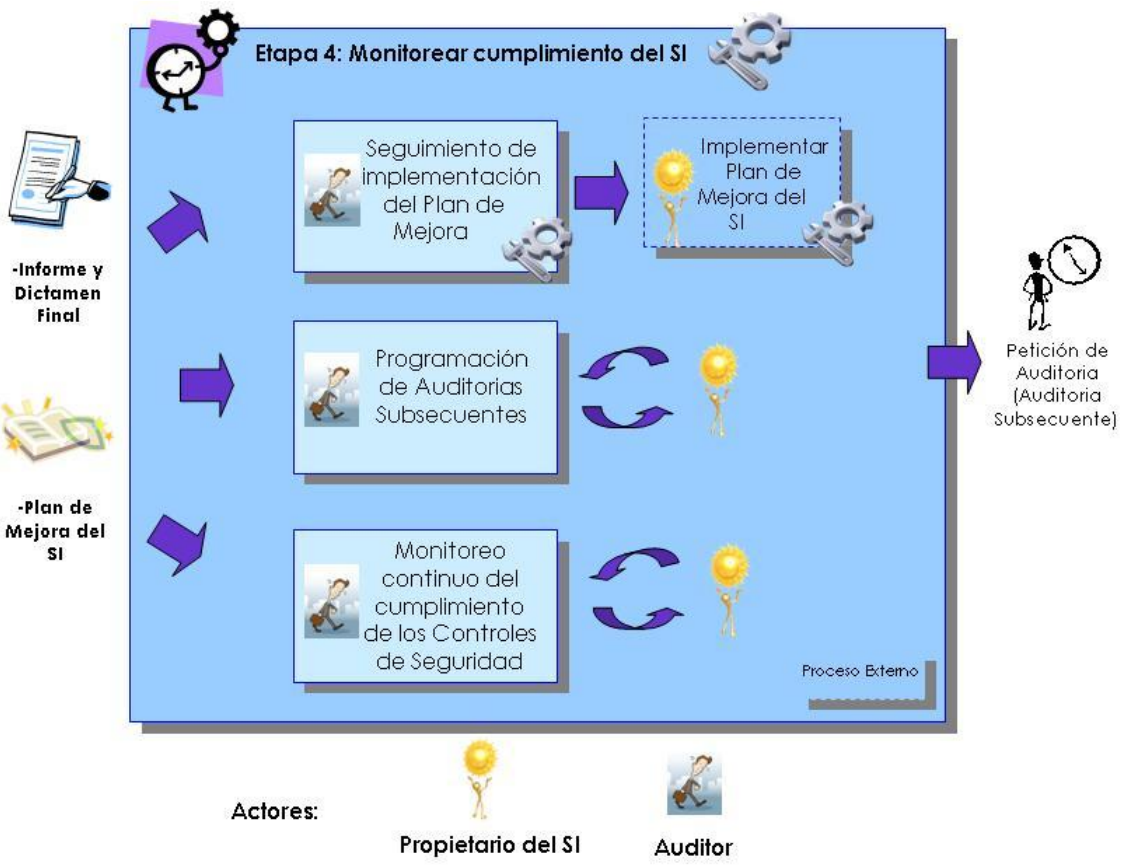


Fig 15. Aproximación de la etapa 4 del modelo propuesto de auditoría de seguridad de Sistemas de Información.

Para apoyar la correcta implementación del modelo propuesto se ha desarrollado una metodología. En los siguientes apartados se presenta el diseño y definición de la metodología resultante.

5.4 Aplicación del Método científico en la metodología propuesta

Para la elaboración de una metodología de auditoría de seguridad de SI se hace necesario aplicar, en estricto sentido, el método científico considerando todas las etapas del proceso de auditoría.

Así, se deben considerar en el contexto de la auditoría de seguridad de SI los siguientes pasos que definen al método científico:

Paso 1: Identificar e investigar sobre el problema. Ocurre en la etapa de *Planeación y programación de la auditoría*, cuando el equipo auditor se da a la tarea de realiza el estudio preliminar del SI a auditar. Se consideran los componentes del sistema, dependencias, responsables, posibles vulnerabilidades y cualquier otro aspecto que considere importante para la ejecución de la auditoría.

Paso 2: Formular una hipótesis. Ocurre en la etapa de *planeación y programación de la auditoría*, cuando el equipo auditor determina cuales son los requerimientos mínimos que debería cubrir el SI auditado para autorizar su operación.

Paso 3: Probar la hipótesis de manera empírica[16] y conceptual. Una vez que se haya generado la hipótesis, se hayan determinado los requerimientos mínimos del SI a evaluar y se hayan generado los planes y programas de auditoría, se deberá, empírica y conceptualmente, probar la hipótesis a través de la *ejecución de la auditoría.*

En la ejecución de la auditoría, el equipo auditor se enfocará a revisar el cumplimiento de: 1) requerimientos mínimos funcionales del SI, 2) requerimientos mínimos de seguridad conforme a la categoría de seguridad del SI, 3) Cumplimiento documental del SI, 4) Marco Normativo del SI y finalmente 5) Revisión de que el SI auditado está libre de los errores de programación más comunes.

Paso 4: Evaluar la hipótesis con respecto a los resultados probados. Una vez revisado el cumplimiento de los requerimientos mínimos del SI, el equipo auditor identificará los hallazgos obtenidos de la auditoría del SI auditado y elaborará un informe y *dictamen de auditoría*. De igual manera, conforme a los hallazgos obtenidos, el equipo auditor determinará el nivel del riesgo del SI auditado.

Paso 5: Si la hipótesis se confirma, evaluar su Impacto. Consiste en aquellas actividades contundentes (sentencias o toma de decisiones que se deben

[16] Conocimiento Empírico: Conocimiento que fundamente sus conocimientos exclusivamente en la experiencia.

respetar) que se generan una vez que la ejecución de la auditoría se ha completado.

En el proceso de auditoría, estas actividades son producto de los resultados de la decisión de autorización del SI, informe y dictamen de auditoría, los cuales confirman o rechazan la hipótesis planteada.

Las tareas que el propietario del SI deberá realizar para *monitorear el cumplimiento del SI y/o implementar el plan de mejora del SI* están en función de la decisión de autorización del SI auditado.

Construcción de la metodología propuesta.

La construcción de la metodología aquí propuesta considera los siguientes aspectos:

- Aplicar los pasos anteriores del método científico a cada una de las fases que constituyen la metodología propuesta.
- Diseñar de procedimientos operativos estandarizados (POE) definidos en el capítulo 2, uno para cada etapa de la metodología.
- Clasificar la seguridad de la información y los SI (FIPS PUB 199) definidos en el capítulo 2.
- Determinar los requerimientos mínimos de un SI, definidos en el capítulo 4.
- Determinar la decisión de operación del SI (basado en NIST SP 800-37) definida en el capítulo 4

5.5 Metodología de Auditoría de Seguridad de SI para el modelo propuesto.

5.5.1 Antecedentes.

La metodología propuesta se basa, principalmente, en la recopilación y adaptación a la seguridad de las aplicaciones de estándares y mejores prácticas, internacionalmente aceptados en el área de seguridad y Tecnologías de la Información (ISO 9126, FIPS PUB 200, FIPS PUB 199, NIST SP 800-37).

Esta metodología se ha diseñado con base en la aplicación de los procedimientos operativos estándar POE. Inicialmente, se diseñaron 4 POEs, correspondiente a cada una de las etapas de la metodología para auditar la seguridad de los SI; pero la estructura de la metodología permite descomponer cada uno de los 4 POEs en POE más específicos para ser utilizados a la conveniencia del auditor.

5.5.2 Características de la Metodología Propuesta.

Una metodología de auditoría en seguridad para SI permite, a los auditores y evaluadores de seguridad, obtener un informe/dictamen integral, ordenado, claro y confiable que refleja el nivel de seguridad del SI evaluado. Un aspecto importante de la metodología propuesta es que parte de un mínimo de requisitos de seguridad que deben cumplirse en un SI. De igual manera, a través de esta metodología se establece un protocolo mediante el cual la evidencia de auditoría (papeles de trabajo) se obtiene, reúne y maneja con alta calidad, contribuyendo con esto a la estandarización de los procesos y obtención de resultados repetibles. De esta manera, la evidencia tendrá las condiciones de custodia y calidad adecuadas para que pueda ser revisada e interpretada por expertos ajenos al equipo de auditores.

Trabajar sin una metodología puede arrojar resultados subjetivos y poco confiables. El éxito y profundidad de la auditoría dependerá de la experiencia, conocimiento, estilo y preferencias del grupo de auditores a cargo de evaluar los aspectos de seguridad de los SI.

A continuación, se enumeran algunas de las características que presenta la metodología propuesta:

1. **Congruente con lineamentos y metodologías internacionales.** Las áreas y aspectos específicos a evaluar, según se recomienda en la metodología, así como los controles de seguridad sugeridos, fueron tomados y adaptados a la seguridad de los SI según los siguientes lineamientos:
    a. Estándar internacional utilizado para la evaluación de software: ISO 9126, del cual se determinó una parte de los requerimientos funcionales del SI.
    b. Clasificación de seguridad de la Información y SI: FIPS PUB 199
    c. Requerimientos Mínimos de Seguridad para Información y SI: FIPS PUB 200, del cual se tomaron los requerimientos mínimos de seguridad para los SI.
    d. Guía para la certificación y acreditación de SI federales de EUA: NIST SP 800-37.

De esta manera, la metodología está construida con base en organizaciones internacionales, especializadas en el área de auditoría, TI y evaluaciones de seguridad.

2. **Es de aplicación general.** No se enfoca a un entorno de desarrollo específico. Por lo que la metodología puede ser totalmente adaptable a los diferentes tipos de SI y organizaciones a evaluar.
3. **Basada en POEs.** Los POEs aseguran la calidad de las actividades realizadas y los documentos e informes que se pueden generar. Involucran y especifican la aplicación de mejores prácticas internacionales en materia de seguridad. Los POEs se conforman por un conjunto de tareas que tienen el carácter de directiva y se definen para asegurar y mantener la calidad de los procesos que ocurren en un sistema. Así mismo permite la reproducibilidad de las pruebas realizadas dentro de la auditoría de seguridad.
4. **Adaptable al cambio.** El entorno de operación no es constante, las amenazas a los SI y el número de hallazgos de vulnerabilidad crecen día con día. Esta metodología permite adecuar la evaluación del SI al entorno de operación del SI a lo largo del tiempo (CAT). Esta adaptación se hace mediante la evaluación y redefinición de los POBC que soportan el proceso de auditoría de seguridad de SI. Los requisitos mínimos de seguridad **del SI se derivan de la Clasificación de Seguridad del SI.** Se establecen los requisitos mínimos a evaluar del SI conforme a su clasificación de seguridad. Se pueden exigir más requerimientos de seguridad que deben cubrir los SI auditados; estos requerimientos serán resultado de los objetivos concretos y particularidades del SI.

6. **Sugiere el uso de diversas herramientas para automatizar procesos.** Las tareas que se recomiendan dentro de esta metodología pueden realizarse manual o automáticamente mediante el uso de diversas herramientas de apoyo.
7. **Sugiere la mejora continua.** Evidencía las deficiencias encontradas en el SI evaluado y sugiere acciones para mitigarlas o eliminarlas. De igual manera, establece un compromiso con los propietarios del SI y el equipo desarrollador para dar solución en un tiempo establecido a las deficiencias encontradas, para luego ejecutar una nueva auditoría.
8. **La decisión de puesta en operación del SI es flexible.** El resultado de la auditoría de seguridad del SI en evaluación tiene 3 posibilidades: la primera es que el SI cumple con los requerimientos mínimos de seguridad, lo que conlleva a la autorización para poner en operación el SI. La segunda posibilidad es que el SI no cumpla con los requisitos mínimos de seguridad, por lo que él Sistema no estará autorizado para operar y debe regresarse al equipo de desarrollo para que corrijan los hallazgos de vulnerabilidad y den seguimiento a las recomendaciones realizadas por el equipo auditor. La tercera posibilidad es una autorización condicionada, es decir que el sistema puede ser puesto en operación bajo ciertas condiciones que deberán estar expresadas sin ambigüedad en el dictamen y deberán ser cumplidas en el tiempo establecido.
9. **El proceso de auditoría es soportado por los POBC.** La organización define un conjunto de procedimientos organizacionales bien conocidos, los cuales sirven de soporte al proceso de auditoría de seguridad de los SI.

5.5.3 Alcance.

Existen diversas propuestas de metodologías para guiar el proceso de evaluación de seguridad de SI (ver apartado 5.3 de esta tesis). Sin embargo, no se ha llegado a ninguna conclusión sobre cuál es la más apropiada, cada una de ellas tiene una orientación especifica y la mayoría se enfoca a los aspectos de seguridad, sin tomar en cuenta los requerimientos funcionales. A pesar de que, cada marco de trabajo podría funcionar bien en el contexto de su área de especialización, no manejan la evaluación del SI de manera integral; es decir, en la metodología propuesta se establece que la auditoría debe considerar tanto el aspecto funcional como de seguridad. La metodología propuesta ha sido desarrollada para apoyar a los auditores de seguridad al análisis, revisión, evaluación y propuesta de perfeccionamiento de los SI. Este modelo intenta superar las principales deficiencias de los modelos de TI y evaluación de seguridad de SI existentes discutidos en las secciones anteriores, logrando integrar las mejores prácticas y aspectos propuestos en cada uno de ellos.

En esta metodología de auditoría de seguridad se verifica la seguridad de los SI conforme al grado en que se garantiza los aspectos de confidencialidad, integridad, y disponibilidad de la información y la infraestructura que le da soporte. De igual manera, se verifica la funcionalidad de los SI conforme a la funcionalidad de negocio, confiabilidad, usabilidad, eficiencia, mejora continua y portabilidad.

Esta metodología ha quedado conformada de cuatro apartados, los cuales se muestran a continuación: Objetivo, Limitaciones, Requisitos y Etapas Propuestas.

5.5.4 Objetivo.

El objetivo de la metodología es establecer un marco de trabajo válido, estándar y aceptado. La metodología establecerá procedimientos que permitan realizar una auditoría de seguridad de los SI. Estos procedimientos estarán basados en las mejores prácticas definidas por distintos organismos internacionales reconocidas en el área de TI, seguridad y auditoría.

Los objetivos específicos de esta metodología de auditoría de seguridad de los SI son: revisar el nivel de cumplimiento de los requerimientos funcionales y de seguridad del SI, verificar el cumplimiento del marco normativo al que se debe someter el SI, determinar el nivel de riesgo al que el SI se encuentra expuesto, elaborar un informe que contenga los resultados obtenidos de la auditoría de seguridad, el dictamen de auditoría y el plan de mejora para el SI.

5.5.5 Limitaciones.

La metodología presenta las siguientes limitaciones:

El alcance de la metodología está limitado a la seguridad en los SI, no se considera el aspecto de seguridad perimetral, tal cual se definió en el alcance de esta tesis.

Esta metodología está orientada a los SI en general, sin importar la plataforma, ni el entorno de desarrollo utilizado, por lo que será trabajo del auditor adecuar la metodología al entorno especifico que se requiera.

5.5.6 Requisitos.

Acerca del Personal.

Debido a que la metodología está diseñada para SI en general, el **equipo de trabajo debe contar con un perfil especializado**, debe contar con amplios conocimientos en el área de informática, entornos de desarrollo, seguridad y auditoría para adaptar la metodología al entorno en específico en que se desarrolla.

Se recomienda que el personal que llevará a cabo la auditoría de seguridad tenga como mínimo experiencia en algún entorno de desarrollo, lo que permitirá tener nociones básicas de la manera en que se encuentra integrado el SI y la lógica de programación.

Los equipos de trabajo de auditoría de seguridad, deben estar en **constante capacitación y actualización**, debido a que día con día surgen nuevas amenazas y brechas de seguridad que deben ser contempladas dentro de la evaluación de la seguridad de los SI.

Debe existir **independencia entre áreas**, una de las premisas de la auditoría es que no se puede ser juez y parte; por lo que el equipo auditor debe ser diferente al equipo desarrollador. Este punto garantiza que los resultados no han sido manipulados para favorecer al SI evaluado.

Esta metodología supone la conformación y actuación de un **comité autorizador del SI**, el cual deberá ser conformado como mínimo por el líder de la auditoría, los responsables del área de seguridad de la información y un representante ejecutivo de la organización con las facultades suficientes para respaldar la decisión tomada. La función de este comité autorizador es la evaluación de los hallazgos de vulnerabilidad en el sistema y el nivel de riesgo que se tiene, para que de esta forma se defina la decisión de operación para el SI evaluado.

Acerca de las Herramientas.

El equipo de trabajo, debe estar al tanto de las herramientas que existen en el mercado para apoyar el trabajo de auditoría de seguridad y que podrían utilizarse en el trabajo diario.

Esta metodología no sugiere una herramienta específica, sólo hace mención que la mayoría de las revisiones de seguridad pueden automatizarse con el apoyo de herramientas tecnológicas. El uso y adopción de una herramienta es decisión y responsabilidad del equipo auditor.

5.5.7 Etapas de la Metodología Propuesta

Debido a que cada sistema tiene su propio grado de complejidad y características de diseño que lo hacen distinto de otros, la definición de un enfoque de procedimiento definitivo es una tarea complicada de realizar. A pesar de ello, varias propuestas hacen referencia a los mismos aspectos de evaluación en los SI como los presentados en el punto 4.7. Aunque cada modelo resalta el grado de importancia en diferentes aspectos, en este trabajo se consideran 5 grupos fundamentales: los requerimientos funcionales, los requerimientos de seguridad, el cumplimiento documental, el marco regulatorio y la búsqueda de vulnerabilidades conocidas en los SI.

La metodología aquí propuesta está definida para ser empleada en aquellas organizaciones e instituciones que deseen tener cierto grado de certeza en el cumplimiento de los requisitos mínimos funcionales y de seguridad de sus SI antes de ser puestos en operación.

Con el propósito de interpretar adecuadamente la aplicación de esta metodología a continuación se presentan, en forma genérica, todas aquellas etapas y actividades que deben ser consideradas. Inicialmente se ha dividido en 4 grandes apartados, las etapas principales que servirán de guía para la realización de una auditoría de seguridad de SI.

Etapa 1: Planeación y Organización de la Auditoría

1.1. Identificar el Origen de la Auditoría
1.2. Establecer contacto directo con los dueños o líderes a cargo del SI a auditar.
1.3. Clasificar la información del SI con base en criterios de seguridad.
1.4. Estudiar el SI objeto de la auditoría.
1.5. Definir objetivos y alcance de la auditoría a realizar.
1.6. Determinar los aspectos del objeto auditado que serán evaluados, verificados y analizados durante el proceso de auditoría.
1.7. Elaborar el Plan y Programa de auditoría.
1.8. Identificar y seleccionar los métodos, herramientas, instrumentos, criterios de evaluación, metodologías de riesgo y procedimientos necesarios para ejecutar la auditoría.
1.9. Asignar recursos humanos, financieros y materiales para la realización de la auditoría.
1.10. POE propuesto para la etapa 1.

Etapa 2: Ejecución de la auditoría.

2.1. Ejecutar las actividades programadas para la auditoría de acuerdo al calendario establecido.
2.2. Identificar y elaborar los documentos que reportarán los hallazgos obtenidos de la auditoría
2.3. Estimar el Riesgo del SI con los hallazgos obtenidos de la auditoría
2.4. Elaborar el informe y dictamen preliminar de auditoría
2.5. Presentar el informe y dictamen preliminar de auditoría con las áreas involucradas para su discusión
2.6. POE propuesto para la etapa 2.

Etapa 3: Dictamen de la auditoría.

3.1. Tomar la decisión de operación del SI
3.2. Elaboración del informe y dictamen final de auditoría
3.3. Elaborar el Plan de Mejora del SI
3.4. Presentar el informe y dictamen final de auditoría
3.5. POE Propuesto para la etapa 3.

Etapa 4: Monitorear cumplimiento del SI

4.1. Seguimiento a las acciones establecidas en el Plan de Mejora
4.2. Programar auditorías subsecuentes.
4.3. Monitorear continuamente el cumplimiento de la atención de observaciones hechas en el plan de mejora.
4.4. POE Propuesto para la etapa 4.

A continuación se detalla cada una de las etapas propuestas en la metodología y las actividades que conlleva cada una de ellas:

Etapa 1: Planeación y Organización de la Auditoría

Se define, planea, organiza y preparan los recursos, actividades y procedimientos necesario para obtener la información del SI que servirá de base para ejecutar la auditoría de seguridad. En esta etapa se deben identificar claramente las razones por las que se realizará la auditoría y la determinación del objetivo de la misma. De igual manera se preparan los documentos que servirán de apoyo para su ejecución, culminando con la elaboración documental del plan, programa y calendario de ejecución de la auditoría.

1.1 Identificar el Origen de la Auditoría: En esta fase se define la razón que origina la auditoría de seguridad (nuevo SI, petición de cambio, implementación de mejoras, auditoría subsecuente), de esta determinación dependerá el rumbo, tareas y enfoque que se le dará a la auditoría de seguridad.

En esta fase, es de suma importancia determinar la forma de adquisición del SI a auditar, ya que con ello se determina si la auditoría a realizar será desde un entorno interno (SI desarrollados a la medida) o desde un entorno externo (SI comerciales).

Cuando la auditoría se realiza desde un entorno interno, la amplitud y exhaustividad de la evaluación es mayor que la realizada en un entorno externo, ya que se tiene mayor acceso a la información relacionada con la infraestructura, relaciones, procedimientos, documentación, relaciones, etc.

1.2 Establecer contacto directo con los dueños o lideres a cargo del SI a auditar: Es imprescindible que el auditor establezca contacto directo con los propietarios del SI y los líderes a cargo del SI a evaluar. El propósito de este primer contacto es que el auditor obtenga una visión más amplia del SI a auditar, relaciones, dependencias, restricciones y la importancia del SI en el proceso productivo de la organización. En realidad, lo que se busca es que el auditor pueda vislumbrar el panorama al cual se enfrenta, para que de ello diseñe su estrategia para el desarrollo de auditoría.

Si en el punto anterior de esta metodología se determinó que la auditoría a realizar es externa no es necesario establecer el contacto directo con los propietarios del SI. La estrategia para obtener información acerca del SI consistirá en recolectar la mayor cantidad de información que el propietario del SI hace disponible a los usuarios finales. De la misma manera, cuando se evalúe un SI comercial, esta se debe realizar de manera previa a la adquisición e implementación del SI.

1.3 Clasificar la información del SI con base en criterios de seguridad: En esta fase se realiza la clasificación de la información que maneja el SI. Una vez obtenida la clasificación de la información se obtiene la clasificación del SI. Esta etapa es de vital importancia, ya que con base en esta clasificación se determinarán los requerimientos mínimos de seguridad a evaluar en el SI.

Cada organización debe definir sus procedimientos para clasificar la seguridad de la información y del SI, un buen punto de partida es utilizar los propuestos por FIPS PUB 199. Para más información ver apéndice E.

1.4 Estudiar el SI objeto de la auditoría: En esta fase se realiza el trabajo de investigación y recopilación de información propia del SI a auditar. En este estudio se determinan los aspectos esenciales del SI (misión, objetivo y funciones del sistema), se define la arquitectura del SI, se determina el ambiente de operación y entorno de desarrollo e implementación del SI y finalmente se determina el marco regulatorio al cual se debe apegar el SI.

Para los SI que son auditados desde un ambiente externo, no será necesario recopilar información correspondiente al marco regulatorio, ni los aspectos relacionados con la funcionalidad del SI; ya que se considera que estos aspectos han sido considerados por la empresa que los desarrolló antes de ser puestos a disposición de los usuarios finales.

1.5 Definir objetivos y alcance de la auditoría a realizar: En esta fase se definen los objetivos generales y particulares del trabajo de auditoría a realizar, así como el alcance de la auditoría.

El alcance de la auditoría dependerá de la forma de adquisición del SI a evaluar, se consideran 2 opciones:

- SI comerciales y
- SI desarrollados a la medida.

Para el caso de auditoría de SI comerciales, la evaluación no se realizará desde un entorno interno, sino como usuarios de la aplicación. Es decir, el alcance de la auditoría será delimitado a los aspectos que se encuentran documentados y de libre distribución por los dueños del SI (ya que el acceso a procedimientos, manuales, diseños y cierta documentación especializada se encuentra restringida a los usuarios finales).

1.6 Determinar los aspectos del objeto auditado que serán evaluados, verificados y analizados durante el proceso de auditoría: En esta fase se definen los aspectos a ser evaluados por la auditoría de seguridad del SI.

Al considerar los puntos a evaluar en la auditoría, es importante considerar dentro de esta fase la forma de adquisición del SI a auditar:

- Si el SI a audita es un SI desarrollado a la medida, se considera que la auditoría será realizada desde un entorno interno, por lo que se considerarán la evaluación del grado de cumplimiento de los siguientes aspectos:

- ❖ Cumplimiento documental,
- ❖ Requerimientos mínimos funcionales,
- ❖ Requerimientos mínimos de seguridad basados en la clasificación de seguridad del SI,
- ❖ Marco regulatorio y
- ❖ Revisión de que el SI auditado está libre de los errores de programación más comunes

- o Si el SI a auditar es una adquisición de un SI comercial, se considera que la auditoría será realizada desde un entorno externo, por lo que el alcance de la auditoría será más limitado que para un SI hecho a la medida, ya que se carece de información concerniente al funcionamiento, arquitectura, relaciones, diseño, comunicación y dependencias del SI. En este caso la evaluación del SI se limitará a los siguientes aspectos:

  - ❖ Cumplimiento documental,
  - ❖ Requerimientos mínimos de seguridad basados en la clasificación de seguridad del SI,
  - ❖ Revisión de que el SI auditado está libre de los errores de programación más comunes

La importancia de esta fase radica en que es el antecedente para el establecimiento de las herramientas, procedimientos y la manera en que se realizará la auditoría.

Una guía para determinar los requerimientos mínimos a evaluar en la auditoría de seguridad del SI se presenta en el capítulo 4.

1.7 Elaborar el Plan y Programa de auditoría: En esta fase se elaboran los documentos que contemplan los planes formales para la ejecución de la auditoría, así como los programas en donde se delimita perfectamente las etapas, eventos, actividades y los tiempos de ejecución para cumplir con el objetivo.

Los planes y programas de auditoría se convierten en guía para documentar los diferentes pasos de la auditoría que se realizará, el grado, tareas y los aspectos evaluados. Provee un rastro del proceso usado para realizar la auditoría así como también a quien se debe adjudicar la responsabilidad de su realización.

1.8 Identificar y seleccionar los métodos, herramientas, instrumentos, criterios de evaluación, metodologías de riesgo y procedimientos necesarios para la auditoría: En esta fase se determinan los documentos, plantillas, herramientas y medios con los cuales se llevará a cabo la auditoría de seguridad del SI, esto se logrará mediante la selección, diseño de los métodos, procedimientos, herramientas e instrumentos necesarios, de acuerdo con lo indicado en los planes y programas de auditoría establecidos. De igual manera, se establece dentro del marco de la auditoría, los criterios de evaluación que serán utilizados para determinar el nivel de cumplimiento de los requerimientos mínimos del SI auditado. Es decir, se define la forma en que el equipo auditor evaluará y determinará si los Requerimientos mínimos del SI son cumplidos.

En esta fase, es de vital importancia, evaluar y seleccionar la metodología de análisis de riesgos que será utilizada para estimar el riesgo del SI auditado y posteriormente determinar que se hará con el riesgo.

1.9 Asignar recursos humanos, financieros y materiales para la realización de la auditoría: En esta fase se realiza la asignación formal de los recursos (humanos, financieros, informáticos, tecnológicos, etc.) que son necesarios para llevar a cabo la auditoría de seguridad del SI.

1.10 POE propuesto para la etapa 1: Para la aplicación de la etapa de Planeación y Organización de la auditoría y las fases y actividades relacionadas a estas, se propone el uso del siguiente POE.

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 1 de 6

PROCEDIMIENTO OPERATIVO ESTANDAR

a) Objetivo. El objetivo de este POE es dar soporte a las actividades propias de la etapa de Planeación y Organización de la auditoría.

b) **Alcance.** Este procedimiento es utilizado para apoyar las actividades de definición, planeación, organización y preparación de los recursos, actividades y procedimientos necesario para obtener la información del SI que nos servirá de base para ejecutar la auditoría de seguridad.

c) **Responsable(s).**
Cargo: Líderes de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Equipo de Auditoría
Habilidad: Amplio conocimiento técnico en las áreas de seguridad, SI y auditoría, así como el conocimiento y utilización de múltiples herramientas de trabajo que apoyen sus actividades definidas en los planes y programas de auditoría.
Nombre:

d) **Definiciones**.
n/a

e) **Materiales: Hardware y Software**.
1. Editores de Texto
2. Plantillas de Instrumentos, pruebas y procedimientos diseñados para auditar el SI

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 2 de 6

g) **Procedimiento.**

1. Etapa 1: Planeación y Organización de la Auditoría
   - 1.1. Identificar el Origen de la Auditoría
     - 1.1.1. Definir el origen de la auditoría(nuevo SI, petición de cambio, implementación de mejoras, auditoría subsecuente)
     - 1.1.2. Determinar la forma de adquisición del SI:
       - 1.1.2.1. SI comercial, la auditoría se realizará bajo un entorno externo
       - 1.1.2.2. SI desarrollado a la medida, la auditoría será bajo un entorno interno
   - 1.2. Establecer contacto directo con los dueños o líderes a cargo del SI a auditar.
     - 1.2.1. Identificación preliminar del SI y sus componentes
     - 1.2.2. Identificación preliminar de las funciones del SI
     - 1.2.3. Recolectar documentación técnica y operativa del SI
     - 1.2.4. Identificar posibles problemáticas del SI
     - 1.2.5. Prever los objetivos iniciales de la auditoría
     - 1.2.6. Determinar preliminarmente el no. de recursos, personas y perfiles necesarios para la auditoría del SI
   - 1.3. Clasificar la información del SI con base en criterios de seguridad.
     - 1.3.1. Utilizar los procedimientos organizacionales para clasificar la seguridad de la información y del SI auditado. (se propone utilizar el FIPS PUB 199).
   - 1.4. Estudiar el SI objeto de la auditoría.
     La amplitud de este estudio dependerá del entorno bajo el que se realice la auditoría, para un entorno externo la amplitud será limitada.
     - 1.4.1. Determinar Aspectos Esenciales del SI.
       - 1.4.1.1. Definición de la Misión del SI
       - 1.4.1.2. Definición de los objetivos generales y específicos del SI
       - 1.4.1.3. Definición de la función general del SI
         - 1.4.1.3.1. Determinar la tarea principal del SI
         - 1.4.1.3.2. Determinar procedencias y precedencias del SI
         - 1.4.1.3.3. Identificar perfiles validos para hacer uso del SI
           - 1.4.1.3.3.1. Determinar la totalidad de perfiles validos para el SI
       - 1.4.1.4. Definición detallada del diseño e implementación del SI
         - 1.4.1.4.1. Definición de la totalidad de módulos que componen el SI
         - 1.4.1.4.2. Definición de procedencia y precedencia entre los módulos del SI
         - 1.4.1.4.3. Definición de la relación existente entre los módulos que componen el SI
         - 1.4.1.4.4. Definición de las dependencias del SI.
         - 1.4.1.4.5. Definición de los recursos utilizados por el SI

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 3 de 6

1.4.1.5. Tecnología utilizada para el desarrollo del SI
1.4.1.5.1. Determinar el lenguaje y herramientas utilizadas para el desarrollo del SI
1.4.1.5.2. Determinar la plataforma considerada por el SI
1.4.1.5.3. Determinar las Bases de datos, y manejadores del SI
1.4.1.5.4. Determinar cualquier otra tecnología u herramienta utilizada en el desarrollo e implementación del SI
1.4.2. Determinar el marco regulatorio del SI
(Si la auditoría se realiza desde un entorno externo, no será necesario determinar el marco regulatorio del SI, ya que se da por entendido que la empresa propietaria del SI ya ha considerado estas regulaciones antes de poner el SI a disposición de los usuarios finales)
1.4.2.1. Regulación Internacional
1.4.2.2. Regulación Nacional
1.4.2.3. Regulación por Sector
1.4.2.3.1. Sector Bancario, Farmacéutico, Gubernamental, etc.
1.4.2.4. Regulación Institucional
1.4.2.5. Regulaciones de validez oficial
1.4.2.5.1. Cumplimiento para procesos de certificación y acreditación
1.5. Definir objetivos y alcance de la auditoría a realizar.
1.5.1. Definición de objetivos generales
1.5.2. Definición de objetivos específicos
1.5.3. Determinación del alcance de la auditoría conforme a la forma de adquisición del SI a evaluar(SI comerciales, SI desarrollados a la medida)
1.6. Determinar los aspectos del objeto auditado que serán evaluados, verificados y analizados durante el proceso de auditoría.
1.6.1. Cumplimiento documental
1.6.1.1. Determinar los Procedimientos, diseños, manuales y formatos requeridos del SI.
1.6.1.1.1. Considerar que si la auditoría se realiza desde un entorno externo, el alcance de esta evaluación será limitado a la información disponible.
1.6.2. Requerimientos mínimos de seguridad conforme a la Clasificación de Seguridad del SI auditado (ver apartado 4.1.2 de esta tesis).
1.6.2.1. Considerar que si la auditoría se realiza desde un entorno externo, el alcance de esta evaluación será limitado a la información disponible.
1.6.3. Requerimientos mínimos funcionales (ver apartado 4.1.1 de esta tesis). (Si la auditoría se realiza desde un entorno externo, se considera que la funcionalidad ya ha sido probada y avalada por la empresa que lo desarrolla, puesto que ya está disponible para los usuarios finales)
1.6.3.1. Determinar si ya se realizo la evaluación de aspectos funcionales, con el propietario del SI, usuario final o con la persona que se encargara

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 4 de 6

de dar el visto bueno del SI. (ver apartado 4.2 de esta tesis)

1.6.3.1.1. Si la evaluación funcional ya se llevo a cabo, se debe presentar la evidencia del visto bueno del propietario del SI, usuario final o persona encargada, así como las pruebas funcionales realizadas al SI.

1.6.3.1.2. Si la evaluación funcional no se ha llevado a cabo, será entonces necesario agendar y realizar una evaluación funcional con la persona encargada de dar el visto bueno de la funcionalidad del SI. En esta etapa solamente se prevé la determinación de los puntos a considerar en esta evaluación, algunas sugerencias son las siguientes:

1.6.3.1.2.1. Determinar Requerimientos funcionales a evaluar
1.6.3.1.2.2. Determinar Requerimientos no funcionales a evaluar
1.6.3.1.2.3. Determinar Requerimientos de calidad a evaluar
1.6.3.1.2.4. Determinar cualquier otro requerimiento mínimo funcional a evaluar aplicable al SI diferente de los contenidos en este apartado.

1.6.4.De cumplimiento con el marco regulatorio del SI

1.6.4.1. Definir los requerimientos regulatorios para el SI (conforme a la información obtenida en el punto 1.4.2 de este POE)

1.6.4.1.1. Si la auditoría se realiza desde un entorno externo, se considera que el cumplimiento del marco regulatorio para el SI ya ha sido cubierto, puesto que el SI ya está disponible para los usuarios finales.

1.6.5. Búsqueda de vulnerabilidades conocidas más comunes y peligrosas en los SI(ver apartado 4.4 de esta tesis)

1.7. Elaborar el Plan y Programa de auditoría

1.7.1.Diseñar y Elaborar el plan de auditoría

1.7.1.1. Determinar actividades que se van a realizar
1.7.1.2. Conformar el grupo de auditoría
1.7.1.3. Determinar responsables de cada actividad
1.7.1.4. Estimar los recursos materiales, humanos, informáticos o de cualquier otra índole que se utilizarán en la auditoría
1.7.1.5. Determinar los tiempos requeridos para cada actividad
1.7.1.6. Determinar el tiempo necesario para realizar la auditoría

1.7.2.Diseñar y Elaborar los programas de auditoría

1.7.2.1. Determinar de manera precisa las fases y etapas de la auditoría
1.7.2.2. Identificar concretamente los eventos que se llevaran a cabo en cada fase y etapa de la auditoría
1.7.2.3. Delimitar claramente las actividades a realizar en la auditoría
1.7.2.4. Organizar y distribuir los recursos que serán utilizados en las diferentes actividades de la auditoría

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 5 de 6

1.7.2.5. Calcular la duración de las fases, etapas, actividades planeadas en la auditoría.
1.7.2.6. Determinar fechas de inicio y fin de las fases, etapas y actividades de auditoría.
1.7.3. Generar un calendario de ejecución, el cual especifique la secuencia de ejecución de cada una de las actividades de la auditoría.
1.8. Identificar y Seleccionar los métodos, herramientas, instrumentos, criterios de evaluación, metodologías de riesgo y procedimientos necesarios para ejecutar la auditoría
1.8.1. Determinar los criterios de evaluación que se utilizarán en la auditoria, para determinar el nivel de cumplimiento de los requerimientos mínimos del SI.
1.8.1.1. Establecer el procedimiento de ponderación de los puntos que serán evaluados para realizar la estimación del riesgo del SI auditado
1.8.2. Determinar las pruebas, instrumentos, procedimientos, métodos y herramientas que se utilizarán para ejecutar la auditoría
1.8.3. Determinar las herramientas manuales y automatizadas que se ocuparán de apoyo a la ejecución de la auditoría
1.8.4. Elaborar las pruebas, instrumentos (documentos y formatos) y herramientas necesarias para la auditoría
1.8.4.1. Diseñar los instrumentos y herramientas para evaluar el cumplimiento documental (definidos en el punto 1.6.1.1 de este POE)
1.8.4.1.1. Definir criterios de evaluación y aceptación del cumplimiento documental
1.8.4.2. Diseñar las pruebas, documentos y formatos para la evaluación de los requerimientos mínimos de seguridad (definidos en el punto 1.6.2 de este POE)
1.8.4.2.1. Diseño de Pruebas para la revisión de los requerimientos mínimos de seguridad especificados para el SI
1.8.4.2.2. Definir criterios de evaluación y aceptación en la revisión y validación de los requerimientos mínimos de seguridad especificados para el SI a evaluar.
1.8.4.3. Diseñar las pruebas, documentos y formatos para la evaluación de los requerimientos mínimos funcionales (definidos en el punto 1.6.3 de este POE)
1.8.4.3.1. Diseño de Pruebas para la revisión de los requerimientos mínimos funcionales especificados para el SI
1.8.4.3.2. Definir criterios de evaluación y aceptación en la revisión y validación de los requerimientos mínimos funcionales especificados para el SI a evaluar.
1.8.4.4. Diseñar los instrumentos y herramientas para la evaluación de los requerimientos regulatorios del SI (definidos en el punto 1.6.4 de este POE)

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 6 de 6

1.8.4.4.1. Definir criterios de evaluación y aceptación en la revisión y validación de los requerimientos regulatorios para el SI auditado

1.8.4.5. Diseñar las pruebas, documentos y formatos para la búsqueda de vulnerabilidades conocidas más comunes y peligrosas en los SI(definidos en el punto 1.6.5 de este POE)

1.8.4.5.1. Diseño de Pruebas para la búsqueda de vulnerabilidades conocidas más comunes en el SI auditado

1.8.4.5.2. Definir criterios de evaluación y aceptación en la búsqueda de vulnerabilidades conocidas más comunes en el SI auditado

1.8.5. Determinar los lineamientos y plantillas a utilizar para documentar las acciones realizadas durante la auditoría del SI.

1.8.6. Evaluar y seleccionar la metodología de análisis de riesgos que será utilizada para estimar el riesgo del SI auditado

1.9. Asignación de recursos humanos, financieros y materiales para la auditoría
Asignación de recursos humanos, informáticos, materiales y cualquier otro recurso definido dentro del plan y programa de auditoría.

Referencias.

- FIPS 199
- FIPS 200
- NIST SP 800-53
- ISO 9126
- Guía de Pruebas OWASP, OSSTMM

Etapa 2: Ejecución de la auditoría.

El equipo de auditores realiza la evaluación exhaustiva del nivel de cumplimiento de las funciones y controles implementados en el SI con respecto a los requerimientos funcionales y de seguridad definidos para el SI, de lo anterior se logra determinar el nivel de exposición de los SI. El objetivo de esta etapa es recopilar la documentación y evidencia de auditoría necesaria mediante la aplicación de instrumentos y herramientas diseñadas para la auditoría, dicha evidencia nos permitirá identificar el nivel de exposición del SI auditado y con ello proponer las medidas correctivas al SI.

2.1 Ejecutar las actividades programadas para la auditoría de acuerdo al calendario establecido: En esta fase cada integrante del equipo de auditoría debe de realizar las actividades que le corresponden conforme fueron diseñas y descritas en los planes, programas y calendarios de ejecución de la auditoría. El objetivo de estas actividades es obtener la evidencia necesaria para determinar el grado de cumplimiento del SI con los requerimientos mínimos del SI, conforme a los criterios de evaluación establecidos en el marco de la auditoria.

2.2 Identificar y elaborar los documentos que reportarán los hallazgos obtenidos de la auditoría: En esta fase se identifican las vulnerabilidades en el SI encontradas y se procede a elaborar los documentos de los hallazgos obtenidos en la auditoría de seguridad, en el los cuales se describen las situaciones encontradas, las causas que las originan y las posibles soluciones, así como los responsables de solucionar dichas desviaciones.

2.3 Estimar el Riesgo del SI con los hallazgos obtenidos de la auditoría: El propósito de esta fase es determinar si las vulnerabilidades conocidas en el SI representan un nivel aceptable de riesgo para las operaciones, activos e individuos de la organización. La estimación del riesgo se realiza con base en la metodología de riesgo evaluada y seleccionada en la etapa anterior.

2.4 Elaborar el informe y dictamen preliminar de auditoría: El propósito de esta fase es elaborar el informe y dictamen preliminar de la auditoría del SI. Los aspectos que el informe y dictamen preliminar de auditoría debe contener son:

- Los resultados de la evaluación (es decir, la determinación de la medida en que los controles y funciones implementadas en el SI se aplican correctamente, funcionando según lo previsto, y producir el resultado

deseado con respecto al cumplimiento de los requisitos funcionales y de seguridad para el sistema),

- Recomendaciones para corregir las deficiencias en los controles y funciones implementadas en SI necesarias para reducir o eliminar las vulnerabilidades identificadas en la auditoría. Se propone que estas recomendaciones hechas por parte del equipo auditor sea utilizando los estándares y mejores prácticas de TI, como son: COBIT, ISO 27002, NIST SP 800-53, etc.
- El dictamen de auditoría del SI, donde el equipo auditor declare formalmente el estado de seguridad del SI, basado en la evidencia obtenida y la estimación de riesgo del SI.

A la par de la elaboración del informe y dictamen de auditoría, se debe integrar el paquete de evidencia de auditoría obtenida de la ejecución de la auditoría del SI.

2.5 Presentar el informe y dictamen preliminar de auditoría con las áreas involucradas para su discusión: El propósito de esta fase es contactar al propietario del SI y el equipo de desarrollo para presentar el informe y dictamen preliminar de auditoría de seguridad del SI auditado donde se muestran los aspectos encontrados y el resultado de la auditoría. En caso de que el propietario del SI o el equipo de desarrollo no coincidan con los aspectos encontrados y señalados en los documentos, se deberá presentar las pruebas o argumentos validos que lo corroboren, para que el equipo de auditores realice las correcciones necesarias al informe y dictamen de auditoría.

2.5 POE propuesto para la etapa 2: Para la aplicación de la etapa de Ejecución de la auditoría y las fases y actividades relacionadas a estas, se propone el uso del siguiente POE.

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 2	Título: Ejecución de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 1 de 3

PROCEDIMIENTO OPERATIVO ESTANDAR

a) **Objetivo.** El objetivo de este POE es dar soporte a las actividades propias de la etapa de Ejecución de la auditoría.

b) Alcance. Este procedimiento es utilizado para apoyar las tareas de ejecución de la auditoría, mediante la ejecución de las actividades previstas en el plan y programa de auditoría generado en la etapa anterior.

c) **Responsable(s).**
Cargo: Líder de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Equipo de Auditoría
Habilidad: Amplio conocimiento técnico en las áreas de seguridad, SI y auditoría, así como el conocimiento y utilización de múltiples herramientas de trabajo que apoyen sus actividades definidas en los planes y programas de auditoría.
Nombre:

d) **Definiciones**.
n/a

e) **Materiales: Hardware y Software**.
1. Herramientas y tecnología de apoyo para la búsqueda de vulnerabilidades y pruebas de seguridad.
2. Instrumentos, pruebas y procedimientos diseñados para auditar el SI

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 2	Título: Ejecución de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 2 de 3

g) **Procedimiento.**

2. Etapa 2: Ejecución de la auditoría.

2.1. Ejecutar las actividades programadas para la auditoría de acuerdo al calendario establecido (generado en el punto 1.7.3 del POE 1).
- 2.1.1. Evaluar el cumplimiento documental
  - 2.1.1.1. Recopilación de los Procedimientos, diseños, manuales y documentación exigidos por la organización (determinados en el punto 1.6.1.1)
  - 2.1.1.2. Documentación de las actividades realizadas y la evidencia obtenida.
- 2.1.2. Evaluar el cumplimiento de los requerimientos mínimos de seguridad
  - 2.1.2.1. Ejecución de Pruebas para la revisión y validación de los requerimientos mínimos de seguridad especificados para el SI (diseñadas en el punto 1.8.4.2.1 del POE 1)
  - 2.1.2.2. Documentación de las actividades realizadas y la evidencia obtenida.
- 2.1.3. Evaluar el cumplimiento de los requerimientos mínimos funcionales
  - 2.1.3.1. Ejecución de Pruebas para la revisión y validación de los requerimientos mínimos funcionales especificados para el SI (diseñadas en el punto 1.8.4.3.1 del POE 1)
  - 2.1.3.2. Documentación de las actividades realizadas y la evidencia obtenida.
- 2.1.4. Evaluar el cumplimiento de los requerimientos regulatorios del SI
  - 2.1.4.1. Recopilación de los procedimientos, diseños, manuales y documentación exigidos por la organización (determinados en el punto 1.6.4.1 del POE 1)
  - 2.1.4.2. Documentación de las actividades realizadas y la evidencia obtenida.
- 2.1.5. Diseñar las pruebas, documentos y formatos para la búsqueda de vulnerabilidades conocidas más comunes y peligrosas en los SI
  - 2.1.5.1. Ejecución de Pruebas para la revisión y validación de la búsqueda de vulnerabilidades conocidas más comunes y peligrosas en los SI (definidos en el punto 1.8.4.5.1 del POE 1)
  - 2.1.5.2. Documentación de las actividades realizadas y la evidencia obtenida.

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 2	Título: Ejecución de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 3 de 3

2.2. Identificar y elaborar los documentos de los hallazgos obtenidos de la auditoría
- 2.2.1. Analizar la evidencia obtenida de la auditoría
- 2.2.2. Enlistar las vulnerabilidades encontradas en el SI
- 2.2.3. Determinar las causas que originaron las vulnerabilidades encontradas
- 2.2.4. Sugerir las posibles soluciones a las vulnerabilidades encontradas

2.3. Estimar el Riesgo del SI con los hallazgos obtenidos de la auditoría
- 2.3.1. Estimar el Riesgo Real del SI conforme a los hallazgos obtenidos de la auditoría y a la aplicación de la metodología de analisis de riesgos seleccionada (definida en el el punto 1.8.6 de este POE).
- 2.3.2. Documentar el nivel de Riesgo estimado para el SI

2.4. Elaborar el informe y dictamen preliminar de auditoría
- 2.4.1. Elaboración del informe y dictamen preliminar de auditoría
  - 2.4.1.1. Elaborar el documento correspondiente al informe y dictamen preliminar, incluir los resultados obtenidos en los puntos 2.2 y 2.3 de este POE, así como una presentación formal del trabajo de auditoría realizado.
    - 2.4.1.1.1. Incluir un resumen de los hallazgos obtenidos en el SI evaluado (generado en el punto 2.2 de este POE)
    - 2.4.1.1.2. Incluir la estimación del riesgo del SI calculado con base en los hallazgos obtenidos de la auditoría,
    - 2.4.1.1.3. Incluir el conjunto de recomendaciones para el SI utilizando estándares, mejores prácticas en TI y procedimientos organizacionales
    - 2.4.1.1.4. Incluir el dictamen preliminar y evaluación del riesgo del SI(opinión del equipo de auditoría con respecto a los resultados obtenidos).
  - 2.4.1.2. Integrar el paquete de evidencia de auditoría obtenida de la ejecución de la auditoría del SI.

2.5. Presentar el informe y dictamen preliminar de auditoría con las áreas involucradas para su discusión
- 2.5.1. Comunicar y lograr el común acuerdo respecto a los hallazgos encontrados en la auditoría
- 2.5.2. Documentar los resultados de la revisión del informe y dictamen preliminar.

Referencias.

- COBIT, ISO 2702, NIST SP 800-53.
- Documentación técnica y especializada para auditar la seguridad del SI.
  Guías y procedimientos internos para determinar el cálculo del riego del SI.

Etapa 3: Dictamen de la auditoría.

En esta etapa de la auditoría de seguridad el equipo de auditores realiza la confección y elaboración del informe y dictamen final de auditoría. Se determina la decisión de operación del SI, con base en la evidencia obtenida y la determinación del nivel de riesgo del SI obtenidos de la fase anterior. De igual manera se contempla la elaboración del plan de mejora del SI, el cual define una serie de tareas y actividades para eliminar o reducir el número de vulnerabilidades encontradas en la auditoría del SI. Esta etapa concluye con la entrega del informe de auditoría a los propietarios del SI y al equipo de desarrollo a cargo del SI.

3.1 Tomar la decisión de operación del SI: En esta fase el **Comité autorizador de SI**, determina con base en la evidencia y documentación obtenida, criterios de evaluación definidos, grado de cumplimiento de los requerimientos mínimos del SI y del valor estimado del Riesgo del SI, si este es apto para operar.

La decisión de operación se limita a 3 posibilidades:

- El SI auditado cumple con los requerimientos mínimos del SI, por lo que se **autoriza la operación** del SI,
- El SI auditado no cumple con los requisitos mínimos, por lo que **no se autoriza la operación** del SI y el SI es regresado al equipo de desarrollo para corregir las vulnerabilidades encontradas y dar seguimiento a las recomendaciones realizadas por el equipo auditor,
- El SI auditado no cumple con los requisitos mínimos del SI, pero es una prioridad para la organización que el SI sea puesto en producción, por lo que se emite una **autorización condicionada**, es decir que el SI puede ser puesto en operación bajo ciertas condiciones y limitaciones.

3.2 Elaboración del informe y dictamen final de auditoría: En esta fase se prepara el informe y dictamen final de auditoría de seguridad, para lo cual se hacen las correcciones y adaptaciones al informe y dictamen preliminar realizado en la etapa anterior.

El informe y dictamen final de auditoría se compone de los siguientes elementos:

- Los resultados de la evaluación (es decir, la determinación de la medida en que los controles y funciones implementadas en el SI se aplican correctamente, funcionando según lo previsto, y producen el resultado

deseado con respecto al cumplimiento de los requisitos funcionales y de seguridad para el sistema),
- Recomendaciones para corregir las deficiencias en los controles y funciones implementadas en SI necesarias para reducir o eliminar las vulnerabilidades identificadas en la auditoría.
- El dictamen de auditoría del SI, donde el equipo auditor declare formalmente el estado de seguridad del SI, basado en la evidencia obtenida y la estimación de riesgo del SI, el cual culmina con **la decisión de autorización del SI** tomada por el comité autorizador de SI.

De igual manera se prepara el documento oficial de autorización del SI auditado, el cual contiene el resultado de la decisión de autorización del SI auditado.

3.3 Elaborar el Plan de Mejora del SI: El equipo de auditoría deberá elaborar el Plan de mejora donde se describan las medidas a adoptar o previstas por el propietario y equipo de desarrollo a cargo del SI, para corregir las deficiencias en los controles funcionales y de seguridad implementados en el SI, en el que se determine la forma en que las vulnerabilidades serán abordadas (es decir, reducir, eliminar, o aceptar las vulnerabilidades).

El plan de mejora identifica las siguientes actividades:

- Tareas que necesitan llevarse a cabo,
- Recursos necesarios para llevar a cabo los actividades descritas en el plan,
- Fechas previstas de finalización de las actividades y Plan de mejora.

3.4 Presentar el informe y dictamen final de auditoría: En esta fase se presenta formalmente el informe y dictamen final de auditoría al propietario del SI, equipo de desarrollo y comité autorizador de SI. También se debe incluir el paquete de evidencia obtenida y el Plan de Mejora elaborado.

A partir de este punto pueden ocurrir 2 situaciones:

- Si la decisión de autorización del SI es "autorizado para operar" (APO) o "autorizado condicionado" (SAC), la siguiente etapa de la metodología de auditoría es la de Monitoreo de cumplimiento (etapa 4).

- Si la decisión de autorización del SI es "no autorizado para opera"(NAO) , el propietario del SI tendrá que realizar las actividades contenidas en el Plan de Mejora del SI en la forma y tiempo acordado. Una vez implementadas las acciones del Plan de Mejora del SI, el propietario del SI deberá solicitar nuevamente una auditoría de seguridad de su SI, el origen de esta

auditoría será "Implementación de mejoras".

Una tarea crucial de esta etapa y en general del modelo de auditoría, es resguardar y mantener disponible a otros usuarios autorizados los informes y planes de mejora elaborados, de tal manera que los usuarios autorizados puedan consultar los aspectos auditados en SI similares y no repetir errores y vulnerabilidades ya conocidas.

3.5 POE Propuesto para la etapa 3: Para la aplicación de la etapa de dictamen de la auditoría y las fases y actividades relacionadas a estas, se propone el uso del siguiente POE.

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 1 de 3

PROCEDIMIENTO OPERATIVO ESTANDAR

a) **Objetivo.** El objetivo de este POE es dar soporte a las actividades propias de la etapa de Dictamen de Auditoría.

b) **Alcance.** Este POE pretende proporcionar la documentación necesaria (evidencia obtenida y la determinación del nivel de riesgo del SI) al Comité autorizador de SI para que se tome la decisión de operación del SI auditado, se genere el informe y dictamen de auditoría y el plan de mejora.

c) **Responsable(s).**
Cargo: Líder de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Equipo de Auditoría
Habilidad: Amplio conocimiento técnico en las áreas de seguridad, SI y auditoría, así como el conocimiento y utilización de múltiples herramientas de trabajo que apoyen sus actividades definidas en los planes y programas de auditoría.
Nombre:

d) **Definiciones**.
Comité Autorizador de SI: Es un órgano conformado como mínimo por el líder de la auditoría, los responsables del área de seguridad de la información y un representante ejecutivo de la organización el cual pueda dar respaldo a la decisión tomada.

e) **Materiales: Hardware y Software**.
1. Editores de Texto.
2. Herramienta de planificación.
3. Plantillas de Informes y Plan de Mejora.

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 2 de 3

g) **Procedimiento.**

3. Etapa 3: Dictamen de la auditoría.

3.1. Tomar la decisión de operación del SI
- 3.1.1. Ubicar y convocar al comité Autorizador de SI
  - 3.1.1.1. Preparar paquete para autorizar SI
  - 3.1.1.2. Evidencia y documentación obtenida de la auditoría
- 3.1.2. Estimación del Riesgo del SI,
- 3.1.3. Consenso y toma de decisión de operación del SI auditado
  - 3.1.3.1. autorizado para operar (APO)
  - 3.1.3.2. -no autorizado para operar NAO)
  - 3.1.3.3. autorizado condicionado (SAC)
- 3.1.4. Documentar la decisión de operación del SI auditado

3.2. Elaboración del informe y dictamen final de auditoría
- 3.2.1. En caso de ser necesario, hacer las correcciones necesarias al informe y dictamen preliminar de auditoría
- 3.2.2. Agregar al informe y dictamen final de auditoría, la decisión de autorización del SI auditado.
- 3.2.3. Agregar al informe y dictamen final de auditoría, la evidencia obtenida como resultado de la auditoría.
  - 3.2.3.1. Incluir la evidencia de la ejecución de las pruebas, instrumentos y resultado de las herramientas utilizadas para realizar la auditoría.
  - 3.2.3.2. Incluir los POE desarrollados, los cuales fungen como evidencia de auditoría.

3.3. Elaborar un plan de mejora para el SI.
- 3.3.1. El líder de auditoría y el propietario del SI, deberán planificar las tareas necesarias para dar seguimiento a las recomendaciones hechas por el equipo auditor para eliminar o reducir las vulnerabilidades encontradas.
  - 3.3.1.1. Determinar las tareas a realizar
  - 3.3.1.2. Determinar a los responsables de cada tarea
  - 3.3.1.3. Determinar los recursos que serán necesarios para la ejecución de cada tarea
  - 3.3.1.4. Estimar fechas de realización para cada tarea
  - 3.3.1.5. Estimar fechas de inicio y fin del Plan de Mejora del SI

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 3 de 3

3.4. Presentar el informe y dictamen final de auditoría.
- 3.4.1. Entregar el informe y dictamen final de auditoría, el Plan de Mejora y el paquete de evidencia obtenida a los propietarios del SI, comité autorizador del SI y equipo de desarrollo
- 3.4.2. Resguardar la información generada del proceso de auditoría del SI auditado
  - 3.4.2.1. Determinar los usuarios autorizados que pueden tener acceso a esta información.

Referencias.

- ISO 27002, ISO 9126, NIST SP 800-53, COBIT
- Guía de Pruebas OWASP, OSSTMM
- Estándares, Mejores Prácticas y Procedimientos internos para proponer las acciones y controles necesarios en el Plan de Mejora del SI.

Etapa 4: Monitorear cumplimiento del SI

El monitoreo de cumplimiento se deriva de que el proceso de auditoría ha concluido con la decisión de operación del SI, y de aquí en adelante se deberá iniciar un nuevo proceso de mejora continua, en el cual las acciones realizadas contribuyan al continuo perfeccionamiento del SI.

El propósito de esta etapa es proporcionar la declaración formal y por escrito, de la supervisión y seguimiento de las actividades definidas en el Plan de mejora para el SI auditado. En esta etapa se incluye la programación de las auditorías subsecuentes del SI, considerando que el medio de operación del SI es cambiante. En el mismo sentido, se definen las actividades y responsabilidades del monitoreo continuo a los controles de seguridad implementados en el SI de manera que aseguren que los controles implementados son eficaces a lo largo del tiempo,

4.1 Seguimiento de las acciones establecidas en el Plan de Mejora: Esta fase se define y estructura el seguimiento a las acciones concretas descritas en el Plan de Mejora previstas para corregir las deficiencias en los controles de seguridad para reducir o eliminar las vulnerabilidades encontradas en la auditoría de seguridad del SI.

4.2 Programar auditorías subsecuentes: Debido a que el entorno de operación del SI no es constante, y a que las amenazas de los SI y sus deficiencias crecen día con día, es necesario realizar auditorías subsecuentes para determinar el nivel de exposición del SI a lo largo del tiempo. En el mismo sentido, se deberán definir las condiciones especiales bajo las cuales se requerirá una auditoría subsecuente para refrendar la decisión de operación del SI o la anulación de la decisión en el caso de que los controles de Seguridad implementados ya no sean eficaces.

4.3 Monitorear continuamente el cumplimiento de los Controles de Seguridad del SI: En esta fase se deberá definir las acciones necesarias para monitorear el nivel de cumplimiento de los controles y funciones implementados en el SI de manera que aseguren que los controles implementados son eficaces a lo largo del tiempo; y cuando ya no sean eficaces darán pauta a tomar acciones inmediatas como una nueva auditoría de seguridad para perfeccionar el SI.

4.4 POE Propuesto para la etapa 4: Para la aplicación de la etapa del monitorear cumplimiento del SI y las fases y actividades relacionadas a estas, se propone el uso del siguiente POE.

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 4	Título: Monitorear Cumplimiento del SI	
Revisión número:	Fecha de vigencia:	Hoja 1 de 3

PROCEDIMIENTO OPERATIVO ESTANDAR

a) **Objetivo.** El objetivo de este POE es dar soporte a las actividades propias de la etapa de monitoreo del cumplimento del SI auditado.

b) **Alcance.** Este POE pretende dar soporte al definición y documentación de actividades relacionas con el seguimiento de la implementación del plan de mejora, de igual manera apoya asentando formalmente las bases del monitoreo continuo del cumplimiento de los controles implementados por el SI y finalmente define, documentar y planifica las auditorías subsecuentes de seguridad al SI considerando que el ambiente de operación es cambiante.

c) **Responsable(s).**
Cargo: Líder de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Propietario del SI auditado
Habilidad: Coordinar las actividades y tareas destinadas a la adquisición, implementación y correcto funcionamiento del SI adquirido. Así como la gestión de los recursos, información y elementos del SI a su cargo.
Nombre:

d) **Definiciones**.
n/a

e) **Materiales: Hardware y Software**.
1. Editores de Texto
2. Herramienta de planificación

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores y por los dueños del SI.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 4	Título: Monitorear Cumplimiento del SI	
Revisión número:	Fecha de vigencia:	Hoja 2 de 3

g) **Procedimiento.**

4. Etapa 4: Monitorear Cumplimiento del SI

4.1. Seguimiento a las acciones establecidas en el Plan de Mejora
4.1.1. Seguimiento de los controles y correcciones implementadas como resultado del Plan de Mejora.
4.1.1.1. Determinar el personal a cargo del seguimiento y las fechas de Revisión de las correcciones e implementaciones realizadas sobre el SI.
4.1.1.2. Determinar los lineamientos sobre los que se determinará si los controles y correcciones implementadas en el SI cumplen con los objetivos y tareas establecidas en el Plan de Mejora.
4.1.1.3. Definir documentación requerida de las actividades derivadas del seguimiento del Plan de Mejora.
4.1.1.4. Generación y entrega del Informe de seguimiento del SI, donde se describan las actividades realizadas para atender el Plan de Mejora del SI y los resultados obtenidos

4.2. Programar auditorías subsecuentes
4.2.1. Planificar las auditorías subsecuentes del SI
4.2.1.1. Determinar posibles fechas de auditorías subsecuentes
4.2.1.2. Determinar responsables de esta actividad para dar el seguimiento apropiado.
4.2.1.2.1. Determinar condiciones especiales sobre las cuales se puede hacer una petición de auditoría extraordinaria para refrendar la decisión de operación del SI.
4.2.1.3. Determinar aspectos adicionales que serán presentados en una auditoría subsecuente
4.2.1.3.1. Informes de seguimiento del SI
4.2.1.3.2. Informes del monitoreo continuo de los controles de Seguridad implementados en el SI.
4.2.1.3.3. Documentación adicional.

INSTITUTO POLITÉCNICO NACIONAL
ESIME CULHUACÁN
Laboratorio de Seguridad Informática

Número de POE: 4	Título: Monitorear Cumplimiento del SI	
Revisión número:	Fecha de vigencia:	Hoja 3 de 3

4.3. Monitorear continuamente el cumplimiento de los Controles de Seguridad del SI
- 4.3.1. Determinar responsables del seguimiento de los Controles de Seguridad implementados en el SI
- 4.3.2. Definir documentación requerida de las actividades derivadas del seguimiento del Plan de Mejora.
- 4.3.3. Generación y entrega del Informe del monitoreo continuo de los controles de seguridad implementados en el SI.

Referencias.

- ISO 27002
- ISO 9126
- COBIT

5.6 Recomendaciones para aplicar el Modelo Propuesto.

El modelo de auditoría de seguridad de SI que se propone, debe ser considerado como un proceso interno de la organización que lo implementa. Partiendo de este punto, existen algunas consideraciones previas que cualquier organización debe considerar antes de la ejecución del modelo de auditoría de seguridad de SI propuesto:

1 Integrar formalmente el área responsable de auditar la seguridad de los SI, independiente del área de diseño y desarrollo.

2 Determinar los lineamientos que guiarán la forma de proceder del área responsable de auditar la seguridad de los SI.

3 Integrar el comité autorizador del SI y definir las responsabilidades de este.

4 Determinar los lineamientos que guiarán la forma de proceder del comité autorizador del SI.

5 Documentar dentro de los procedimientos organizacionales del área de Sistemas, la necesidad y obligatoriedad de realizar una auditoría de seguridad de los SI antes de su puesta en producción, como el medio para obtener la 'autorización para operar el SI'.

6 Concientizar a los propietarios del SI de la importancia y obligatoriedad de realizar la auditoría de seguridad de sus SI antes de su puesta en producción, aceptando todas las consecuencias que se deriven de ella (considerar dentro de su planeación las consideraciones en tiempo y recursos para gestionar el proceso de auditoría, ejecución de la auditoría, correcciones al SI derivados de la auditoría, etc.).

7 Definir y documentar los procedimientos organizacionales para clasificar la Información y los SI (revisar punto 4.3 de esta tesis), ya que con base en ello se definirá la severidad y extensión de los aspectos a evaluar y se hará el conjunto de recomendaciones para el SI.

8 Definir conforme a la clasificación de la información y los SI, el conjunto de requerimientos funcionales para cada clasificación de la información y SI (bajo, moderado, alto).

9 Definir conforme a la clasificación de la información y los SI, el conjunto de requerimientos de seguridad para cada clasificación de información y SI (bajo, moderado, alto).

10 Difundir en la organización la existencia del proceso de auditoría y concientizar al personal de la importancia en la consecución de los objetivos organizacionales.

11 Mantener disponibles los resultados e informes de la auditoría, ya que esto contribuye en la mejora continua de los SI organizacionales y permiten la comparación entre SI.

12 Revisar y redefinir constantemente los Procedimientos Organizaciones Bien Conocidos (POBC) que dan soporte al proceso de auditoría de seguridad. .

5.7 Aplicación de la metodología propuesta en la auditoría de seguridad de un SI.

Como se mencionó anteriormente, el modelo de auditoría presentado en la tesis es un procedimiento interno, por lo que no ha sido posible implementarlo dentro de una organización. Idealmente la metodología propuesta debería ser utilizada bajo el mismo contexto.

En este apartado, se realizó una prueba de la metodología para un SI comercial, de forma que se pueda apreciar la factibilidad y efectividad de las fases propuestas por la metodología.

Se ha planteado un escenario ficticio, ya se considera que esta auditoría se lleva de manera interna.

Auditoría de Seguridad a un navegador comercial "Mozilla Firefox® 3.6.13"

La empresa "Mi empresa" ha utilizado desde hace algunos años el navegador Mozilla Firefox® como el navegador autorizado dentro de la organización. Recientemente el área de informática solicitó una auditoría de seguridad al área de Auditoría de Seguridad para el navegador Mozilla Firefox® 3.6.13 (última versión en español) para determinar el nivel de exposición del mismo y determinar si es buena opción seguir utilizándolo o sustituirlo por otro navegador.

Se utilizó la metodología planteada en esta tesis para auditar la seguridad del navegador Mozilla Firefox®, En el Apéndice G se muestra el llenado de cada uno de los POE considerados para cada etapa de la metodología.

Resultados Obtenidos de la Auditoría:

Se analizó la evidencia obtenida de la auditoría, entre los que se encuentran reportes de seguridad emitidos por los propietarios de Mozilla Firefox®. Las vulnerabilidades reportadas para Mozilla Firefox®, se agrupan respecto a su criticidad en **[54]**:

• Crítico: Una vulnerabilidad puede ser utilizada para ejecutar código malintencionado e instalar software, sin necesidad de interacción del usuario más allá de la navegación normal. En esta clasificación se encontraron 9 vulnerabilidades reportadas para Mozilla Firefox® 3.6.13:

• Alta: La vulnerabilidad puede ser utilizada para recopilar los datos sensibles de los sitios en otras ventanas o inyectar datos o código en esos sitios, que no requiere más que acciones de navegación normal. En esta clasificación se encontró 1 vulnerabilidad reportada para Mozilla Firefox® 3.6.13:

• Moderado: Las vulnerabilidades que de otro modo sería alto o crítico, excepto que sólo funcionan en configuraciones poco comunes no por defecto o requiere que el usuario realice complicados y/o pasos poco probables. En esta clasificación se encontró 1 vulnerabilidad reportada para Mozilla Firefox® 3.6.13:

Se determinaron las causas que originaron las vulnerabilidades encontradas en Mozilla Firefox®, el resultado es que se debieron a un mal diseño de la arquitectura del navegador y una mala codificación por parte de los desarrolladores.

El equipo de auditores sugirió que para eliminar las vulnerabilidades encontradas en la versión actual del navegador, será necesario implementar las acciones emitidas por los propietarios de Mozilla Firefox®. Para ello se necesita actualizar, a la brevedad posible, la versión actual del navegador (3.6.13), ya que las actualizaciones incluyen las correcciones a las vulnerabilidades encontradas y citadas anteriormente en el punto 2.2.1. Estas actualizaciones en las versiones de los navegadores deberá ser de ahora en adelante una actividad primordial por parte de los usuarios, por lo que será una tarea primordial de las áreas de seguridad dar el seguimiento necesario y establecer las políticas y procedimientos para su cumplimiento.

El equipo de auditores sugirió realizar un esfuerzo para concientizar y capacitar a los usuarios que utilicen el navegador como parte de sus funciones de trabajo, en los aspectos relacionados a los peligros y posibles amenazas a los que se encuentren sometidos al utilizar un navegador, así como acciones preventivas para evitar cualquier tipo de violación a la seguridad y divulgación de información confidencial.

El equipo auditor se dio a la tarea de estimar el Riesgo del navegador Mozilla Firefox® con el propósito de determinar si las vulnerabilidades conocidas en el navegador representan un nivel aceptable de riesgo para las operaciones, activos e individuos de la empresa, el resultado fue el siguiente:

Requerimientos a Evaluar	Ponderación	% Cumplimiento del navegador	Total por Aspecto evaluado
Funcionales	20	100	20
Normativos	20	100	20
Documentales	20	100	20
Seguridad	NA		
Libre de Vulnerabilidades conocidas	40	70	28
		Cumplimiento del navegador =	88 %

Para determinar el riesgo estimado del navegador, se tomaron en cuenta los siguientes aspectos:

- Clasificación de Seguridad (CS) del navegador: La CS del navegador fue determinada como alta, lo que conllevo a los integrantes del comité autorizador a ser más estrictos en la decisión a tomar.

- Cumplimiento del Navegador: El navegador cumple con un 88% de los aspectos evaluados, el restante 12% corresponde a las vulnerabilidades encontradas al evaluar que el navegador se encontrará libre de vulnerabilidades conocidas.

- Facilidad para implementar mejoras al navegador para reducir las vulnerabilidades encontradas: El comité autorizador tomo como base las recomendaciones realizadas por equipo auditor y determino que no existe complejidad alguna para implementar las mejoras propuestas.

- Prioridad del navegador de seguir en operación dentro de la organización: La prioridad de utilizar el navegador por los usuarios de la empresa fue considerada como alta, debido a que la mayoría de las aplicaciones informáticas que son utilizadas dentro de su trabajo diario, son soportadas por el navegador.

- Comparativa con otros navegadores: Al ser un producto comercial, el comité autorizador, pudo darse una idea de que otros navegadores

podrían sustituir a Mozilla Firefox®, considerando los aspectos funcionales, documentación, soporte, seguridad, etc. Lo anterior, conllevo a consultar diversas fuentes, la mayoría apuntaba a que la mejor opción en navegadores es Mozilla Firefox® **[53]**.

Después de evaluar estos puntos, el equipo auditor determino que:

El riesgo del navegador es Medio. Se considero que si bien el cumplimiento del navegador es de un 88%, las vulnerabilidades encontradas son ya conocidas y pueden ser explotadas por usuarios con los medios, conocimientos y recursos disponibles.

El comité autorizador evaluó la evidencia obtenida de la auditoría, el nivel de riesgo estimado y algunos otros aspectos como:

- Clasificación de Seguridad (CS) del navegador: La CS del navegador fue determinada como alta, lo que conllevo a los integrantes del comité autorizador a ser más estrictos en la decisión a tomar.
- Porcentaje de cumplimiento del Navegador
- Facilidad de implementación de mejoras al navegador para reducir las vulnerabilidades encontradas
- Prioridad del navegador de seguir en operación dentro de la organización
- Comparativa con otros navegadores

Y se llegó al siguiente resultado:

Considerando que la CS del navegador es alta, estrictamente hablando no debería de permitirse la operación del navegador dentro de la empresa; ya que las vulnerabilidades encontradas presentan un gran riesgo en las operaciones, procesos e individuos de la empresa. Pero, considerando que:

La prioridad de que el navegador siga operando es alta,

Aún con las vulnerabilidades encontradas en el navegador, Mozilla Firefox® es considerado como la mejor opción comparado con productos similares y finalmente

La implementación de mejoras para el navegador puede realizarse sin complejidad alguna, para disminuir el número de vulnerabilidades encontradas.

De lo anterior, el comité autorizador ha determinado que el navegador Mozilla Firefox® está AUTORIZADO CONDICIONADO PARA OPERAR, es decir puede seguir operando siempre y cuando atienda las recomendaciones emitidas por el equipo auditor en el tiempo y forma que se le especifique.

Una de las actividades más importantes dentro de la auditoría, consistió en la elaboración del Plan de Mejora del navegador. Para ello se requirió la colaboración del líder de auditoría, del personal del área de informática y del personal del área de seguridad, los cuales:

- Definieron y planificaron las tareas necesarias para dar seguimiento a las recomendaciones hechas por el equipo auditor para eliminar o reducir las vulnerabilidades encontradas. Las tareas principales que se definieron se componen de :
- Programa de actualización continúa del navegador: ya que gran parte de las vulnerabilidades encontradas en un navegador son eliminadas mediante la actualización o instalación de versiones más recientes del navegador.
- Campañas de concientización y capacitación a los usuarios que utilicen el navegador como parte de sus funciones de trabajo, en los aspectos relacionados a los peligros y posibles amenazas a los que se encuentren sometidos al utilizar un navegador, así como acciones preventivas para evitar cualquier tipo de violación a la seguridad y divulgación de información confidencial.
- Determinaron a los responsables de cada tarea
- Determinaron los recursos que son necesarios para la ejecución de cada tarea
- Estimaron y determinaron fechas compromiso para la realización de cada tarea
- Estimar fechas de inicio y fin del Plan de Mejora del SI

Finalmente la etapa del monitoreo de cumplimiento se deriva de que el proceso de auditoría ha concluido con la decisión de operación del SI, y de aquí en adelante se deberá iniciar un nuevo proceso de mejora continua, en el cual las acciones realizadas contribuyan al continuo perfeccionamiento del SI.

Para lograr el perfeccionamiento del navegador evaluado, el líder de la auditoría, en colaboración con los responsables de las áreas de informática y de seguridad, realizaron la declaración formal y por escrito, de las tareas de supervisión y seguimiento de las actividades definidas dentro del Plan de mejora para el navegador, programación de las auditorías subsecuentes del SI y finalmente la definición de actividades y responsabilidades del monitoreo continuo a los controles de seguridad implementados en el SI de manera que aseguren que los controles implementados son eficaces a lo largo del tiempo.

Conclusiones

El navegador auditado, es un SI comercial, por lo que al llevar a cabo la auditoría de seguridad se encontraron varias limitaciones, ya que la auditoría paso de ser considerada de un contexto interno (como es el caso de los SI desarrollados a la medida) a un contexto externo, es decir, solo se pudo evaluar la seguridad desde un enfoque limitado, ya que no se contó con información de ciertos aspectos considerados como "restringidos" por parte de los propietarios del navegador.

Dentro de la ejecución de la auditoría, en primera instancia se considero la evaluación del os aspectos funcionales, normativos, documentales, seguridad y que el SI estuviera libre de vulnerabilidades conocidas. Al ir avanzando en la ejecución de la auditoría, se encontró con limitaciones para poder evaluar ciertos aspectos como lo fue para el caso de los requerimientos mínimos de seguridad, ya que dentro de los 17 requerimientos mínimos a evaluar considerados por el FIPS PUB 200, 10 de ellos resultaron NO APLICABLES ya que no se contaba con la información necesaria para determinar su cumplimiento. Por lo anterior se tuvo que descartar a los requerimientos mínimos de seguridad de los aspectos a evaluar en el navegador.

Otra limitante que se encontró al evaluar los requerimientos mínimos de un SI, fue el aspecto funcional, debido a que la funcionalidad como tal del navegador no puedo ser acotada, ya que el detalle de los requerimientos de usuario y de los diseños funcionales no están a disposición de los usuarios finales. Dada esta situación, se considero que tanto los requerimientos mínimos funcionales y normativos del SI evaluado, debieron evaluarse antes de ser puestos en operación y a disposición de los usuarios finales, por lo que para SI comerciales los requerimientos mínimos funcionales y normativos son considerados como cubiertos.

Con respecto al cumplimiento de los requerimientos documentales, se tuvo que adaptar el concepto, ya que al ser un SI comercial, la única información exigible y disponible es la información proporcionada en apoyo a la fácil utilización por parte de los usuarios finales y la información concerniente a la instalación, requerimientos técnicos y de soporte a la aplicación.

De los puntos anteriores, se puede concluir que para el caso de auditoría de seguridad a SI comerciales, el enfoque que se le debe de dar a la auditoría es el de "caja negra", donde no se cuenta con información acerca de las relaciones, arquitectura, flujos, dependencias y demás aspectos considerados como confidenciales y de los que solo tienen conocimiento los propietarios del SI y que por razones de seguridad no son de libre distribución.

El caso ideal bajo el que tanto el modelo como la metodología propuesta se debieran de aplicar es dentro de la comunidad de desarrollo del navegador, es decir, con los propietarios. Lo cual permitiría evaluar todos los aspectos considerados como mínimos dentro de un SI.

CONCLUSIONES

Actualmente es un proceso muy común por parte de las organizaciones incluir tecnología dentro de sus procesos productivos, la mayoría de estas adquisiciones se realiza en la forma de SI que apoyen y automaticen gran parte de los procesos del negocio. Desafortunadamente estas adquisiciones de SI se realizan para un mundo en condiciones ideales, donde el entorno permanece estático a lo largo del tiempo y los usuarios de los SI no representan algún peligro alguno para la operación normal del SI. Partiendo de este último punto, las metodologías tradicionales de desarrollo de software utilizadas por los equipos de desarrollo, tanto internos como externos a la organización, sólo consideran estas condiciones ideales, no construyen SI capaces de asegurar la confidencialidad, disponibilidad e integridad de la información y de los SI que manejan esta información.

Actualmente el mayor porcentaje de inversión en seguridad es destinado a la seguridad perimetral (infraestructura), dejando de lado a la seguridad en las aplicaciones. Paradójicamente, el mayor número de vulnerabilidades en los SI se encuentra en las propias aplicaciones y no en la infraestructura que la soporta.

Así como ha crecido el número de adquisiciones de SI por parte de las organizaciones, también los SI se han convertido en el blanco preferido por los atacantes, debido a que el mayor número de vulnerabilidades encontradas en estos SI, son vulnerabilidades ya conocidas, documentadas y ampliamente difundidas. Las publicaciones de vulnerabilidades más comunes, deberían ser tomadas como una herramienta de capacitación y sensibilización para los equipos de diseño y desarrollo, de manera que les permita prevenir las diferentes vulnerabilidades que afectan en la actualidad a la industria del software.

Un aspecto importante a considerar en cualquier proceso de perfeccionamiento en los SI, p.ej. el modelo de auditoría en seguridad propuesta en este trabajo de tesis, debería ser la revisión de que el SI auditado está libre de los errores de

programación más comunes que pudieran ser utilizados para vulnerar la seguridad de las aplicaciones y comprometer la información que estas manejan.

Así pues, es responsabilidad tanto de propietarios, desarrolladores y especialistas de seguridad, procurar y promover acciones dentro de los procesos organizacionales que permitan reducir el número de vulnerabilidades en las aplicaciones desarrolladas dentro de la organización como apoyo a los procesos del negocio.

Partiendo de la hipótesis planteada, hablando solamente de la seguridad en los SI, se tienen 2 opciones para dotar a los SI de seguridad, la primera integrando la seguridad como una característica de todo el ciclo de desarrollo de software, lo que conlleva a un cambio en la forma e ideología del trabajo de las organizaciones y la segunda, llevando una revisión de seguridad exhaustiva de las aplicaciones desarrolladas con la intención de encontrar el mayor número de vulnerabilidades para posteriormente hacer las sugerencias necesarias al propietario del SI y equipo de de desarrollo para eliminar las vulnerabilidades encontradas.

Si bien parece más fácil optar por un modelo de auditoría de seguridad para garantizar cierto grado de seguridad en las aplicaciones, en realidad no lo es. El no cambiar la forma en que los equipos de desarrollo y departamentos asociados trabajan y la concepción de la alta gerencia en la forma de adquirir los SI que apoyen sus procesos, a la larga trae consigo un mayor gasto en recursos, esfuerzo y tiempo derivados de la corrección y en ocasiones el rediseño del SI. La mayoría de las veces las deficiencias encontradas resultan de un mismo origen, "el desconocimiento de las implicaciones y prácticas de seguridad por parte de los equipos de trabajo".

Sin duda alguna, la opción ideal para dotar seguridad a los SI es mediante la adopción de una metodología de CVDS Seguro, de tal manera que el aspecto de seguridad sea visto como parte integral del ciclo de vida de desarrollo de software y no solo como parte final del proceso de desarrollo. Desgraciadamente, este cambio no se logra de un día para otro, este se debe llevar a cabo de manera gradual, ya que la mayoría de las organizaciones aún no cuentan con la madurez tecnológica y cultura organizacional necesaria que les permita la implementación de este modelo de desarrollo. Los principales retos a los que la adopción de un CVDS dentro de una organización se enfrenta son los siguientes:

- Erradicar la idea errónea por parte de la alta gerencia, propietarios del SI, usuarios, equipos de diseño y desarrollo de que dotar de seguridad a un SI

es un proceso independiente al Ciclo de Vida de Desarrollo del SI y generalmente se lleva en las últimas fases del ciclo de vida.

- Escaso compromiso por parte de la alta gerencia con respecto a las consideraciones de seguridad de los SI organizacionales.

- Erradicar el pensamiento erróneo por parte de la alta gerencia, propietarios del SI, usuarios, e integrantes de los equipos de diseño y desarrollo, de que el área de seguridad sólo entorpece el trabajo y ejecución habitual de sus actividades diarias.

- Escasa sensibilización y capacitación de la gerencia y equipo de liderazgo de la organización en los temas de seguridad informática, lo que deriva en la incomprensión del incremento en tiempo, recursos y esfuerzos derivado de las acciones planeadas al incluir seguridad en los SI.

- Escaso entrenamiento en seguridad de los profesionales de TI, no se analiza, diseña y programa pensando en seguridad.

- Desconocimiento por parte de los equipos de diseño y desarrollo de las consideraciones y uso de las mejores prácticas de seguridad como parte de sus procesos en el desarrollo de SI.

- Poca colaboración entre las áreas de seguridad y las áreas de diseño y desarrollo.

- La inversión inicial para realizar el cambio en la forma de trabajo por las áreas de diseño y desarrollo es alta, considerando que se tiene que trabajar e invertir esfuerzo en la reorganización de la estructura de trabajo y en la capacitación de sus equipos.

- Se requiere tiempo y esfuerzo para que una organización absorba cambios, y más cuando estos se reflejan en sus procesos internos y cultura organizacional.

- Resistencia al cambio, por parte de los propietarios de los SI y áreas de diseño y desarrollo; debido al trabajo adicional que conlleva el implementar acciones de seguridad en cada una de las etapas del ciclo de vida comparado con los tradicionales procesos de desarrollo.

Aún se requiere mucho tiempo, recursos, esfuerzo, trabajo de concientización y capacitación por parte de las organizaciones para lograr el cambio en la manera de adquirir, analizar, diseñar, desarrollar y probar los SI. Pasará todavía algún

tiempo para que las organizaciones integren totalmente el CVDS Seguro en sus procesos de desarrollo de SI, mientras tanto el uso de un modelo de auditoría de seguridad de SI seguirá siendo una buena y atractiva opción. E incluso en un futuro, cuando las organizaciones hayan logrado implementar totalmente el CVDS Seguro en sus procesos internos de desarrollo, sería importante complementar y evaluar el resultado final de este proceso de CVDS Seguro con la ejecución periódica de auditorías de seguridad, las cuales determinen el nivel de exposición del SI desarrollado. Es en este último punto donde entra en acción el modelo de auditoría propuesto en esta tesis.

No existe un modelo de auditoría único y valido para todas las organizaciones, la selección e implementación de estos modelos, dependerán de las características, necesidades, infraestructura y reglas de negocio en cada organización. El modelo de auditoría propuesto en esta tesis, centra su importancia en la definición de los POBC, los cuales reflejarán e irán acorde a la cultura, prioridades, negocio y necesidades de la organización que las define e implementa, por lo que es de vital importancia que los POBC sean definidos formalmente antes de realizar cualquier proceso de auditoría de SI. Debido a que los POBC son la base del proceso de auditoría, estos deberán estar en continua valoración y redefinición de manera que puedan responder a los cambios del entorno a través del tiempo y ser fortalecidas con las lecciones aprendidas; recordando que el ambiente de operación de los SI organizacionales no es constante.

Debe ser una tarea primordial de cualquier organización, definir, difundir y vigilar el cumplimiento de políticas que impulsen la evaluación de los requerimientos mínimos de un SI, antes de que este sea adquirido o puesto en operación dentro de la organización, de tal manera que se garantice la confidencialidad, integridad y disponibilidad de la información que se maneja.

Un punto muy importante de los modelo de auditoría de seguridad es que contribuye en la mejora continua de los SI organizacionales, encontrando el mayor número de vulnerabilidades en el SI antes de que este sea puesto en operación, lo que permite corregir esta serie de vulnerabilidades conocidas antes de que sean explotadas. Como parte de la mejora continua del proceso de desarrollo de SI organizacionales, debe ser una tarea crucial del área responsable de auditar la seguridad de los SI, tener información disponible y actualizada acerca de las vulnerabilidades con mayor incidencia en sus SI, así como la forma de resolver estas posibles vulnerabilidades con el fin de robustecer su SI y adoptar las recomendaciones hechas para SI similares.

A pesar de la aplicación del CVDS Seguro durante el desarrollo y/o una auditoría de seguridad, las prácticas de desarrollo más avanzadas no consideran que se pueda tener una SI libre de vulnerabilidad de seguridad. Incluso aunque el proceso de desarrollo pudiera eliminar todas las deficiencias de seguridad, con el transcurso del tiempo se descubrirían nuevos ataques y el software considerado "seguro" pasaría a ser vulnerable. Por tanto, los equipos de desarrollo, de auditoría y de seguridad deben prepararse y estar en continua actualización para hacer frente a las nuevas amenazas que atenten a los SI y con ello comprometer la información y recursos asociados a estos.

TRABAJOS A FUTURO

- Implementar el modelo de auditoría propuesto dentro de una organización como un procedimiento de auditoría interno.
- Integrar al modelo, el uso de métricas que permitan evaluar de el nivel de exposición de los SI.
- A la par, los trabajos futuros en el área de seguridad en aplicaciones, deberán encaminarse hacia la implementación de modelos de CVDS Seguro, es decir implementar modelos de CVDS que incluyan consideraciones de seguridad en cada una de las fases del ciclo de vida.

APÉNDICES

APÉNDICE A: GENERALIDADES DE LOS SISTEMAS DE INFORMACIÓN

Sistema

Ian Sommerville **[10]**, define un sistema como un conjunto de componentes inter-relacionados trabajando conjuntamente para un fin común. El sistema puede incluir software, dispositivos mecánicos y eléctricos, hardware, y ser operado por gente. Los componentes del sistema son dependientes de otros componentes.

De lo anterior, se define un sistema como un conjunto de elementos interrelacionados, orientados a lograr un fin común. Un sistema puede formar parte de uno más general, que sería su entorno, y/o estar formado por otros sistemas, lo que comúnmente llamamos subsistemas.

Información

Se puede definir a la información como un conjunto de datos ordenados y sistematizados que proporciona significado o sentido de las cosas.

Sistemas de información

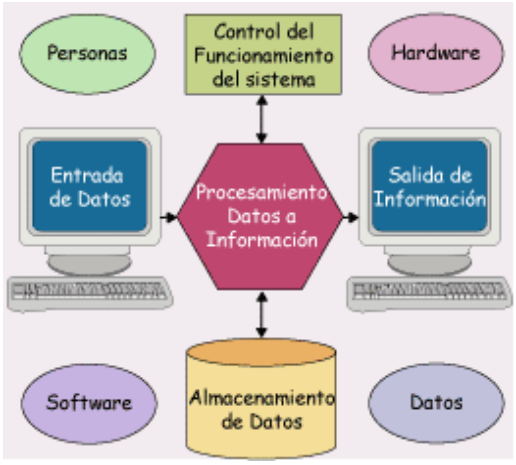
Fernando Espinosa **[11]**, define un sistema de información como un conjunto de procedimientos interrelacionados que forman un todo, es decir, obtiene, procesa, almacena y distribuye información datos manipulados, para apoyar la toma de decisiones y el control en una organización. Los elementos, interactúan entre si con el fin de apoyar las actividades de las empresas, negocios u organizaciones.

El NIST **[12]**, define un sistema de información como un conjunto discreto de recursos de información organizados para la recolección, procesamiento, mantenimiento, uso, diseminación o destrucción de la información.

De las definiciones anteriores podemos decir que un sistema de información es un conjunto de elementos interrelacionados con el fin de obtener, procesar, almacenar, administrar, formatear, difundir y en determinado momento destruir la información procesada.

En el portal de la Red Nacional de Venezuela **[13]**, como se aprecia en la figura 3, en un sistema de información intervienen:

- Personas
- Datos
- Procedimientos
- Hardware
- Software



Fuente: Red Escolar Nacional de Venezuela, Sistemas de Información, http://www.rena.edu.ve/cuartaEtapa/Informatica/Tema10.html,

Fig 3. Componentes de un sistema de Información

Un sistema de Información, pude descomponerse en 4 subsistemas funcionales:

Dos subsistemas internos:

- Tratamiento de la información
- Almacenamiento

Dos subsistemas de enlace con el entorno:

- Obtención de datos
- Salida de datos

El almacenamiento de los datos se refiere básicamente al almacenamiento de programas, estructuras de datos, archivos y bases de datos.

El tratamiento de la información consiste en recibir información de entrada y bajo la ejecución de ciertos procesos, generar informaciones a la salida en forma de resultados.

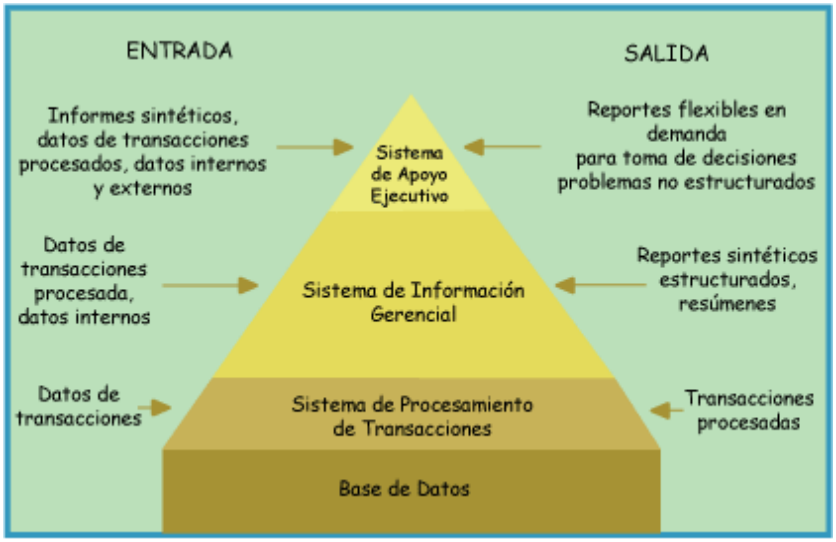
La obtención de datos se refiere a la recepción de datos proporcionados por el usuario del sistema o por algún otro subsistema con el que se tenga comunicación.

La salida de datos se refiere a la transformación, formateo y distribución de los datos almacenados o resultantes de un tratamiento en una salida.

Clasificación de los sistemas de información

En la medida en que más funciones de las organizaciones se han automatizado, los sistemas de información se han tornado aceleradamente más especializados, dando origen a distintos sistemas de información. Los sistemas componen una pirámide, sirviendo de apoyo esencialmente a alguno de los niveles jerárquicos de la organización.

En la figura 4 se puede apreciar la clasificación de los sistemas de información conforme al nivel jerárquico que dan soporte según la Red Escolar Nacional de Venezuela **[13]**.



Fuente: Red Escolar Nacional de Venezuela, Sistemas de Información, http://www.rena.edu.ve/cuartaEtapa/Informatica/Tema10.html,

Fig 4. Categorías de los sistemas de información organizacionales.

Sin importar la clasificación a la que pertenezcan los sistemas de información o la forma de adquisición, todos ellos convergen en que aportan valor a la organización.

Seguridad

El Instituto Nacional de Estadística y Geografía **[14]**(INEGI) define seguridad como, aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

De lo anterior, se puede definir a la seguridad como todas aquellas medidas encaminadas para proteger y salvaguardar lo(s) activo(s).

La seguridad debe ser tomada como una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo.

Seguridad de la Información

ISO, en su norma 7498 define la seguridad de la información como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización, donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotada **[15]**.

ISO/IEC, en su norma 27002 define la seguridad de la información como la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio**[16]**.

El NIST, define la seguridad de la información como la protección de los sistemas de información y la información del acceso, uso, divulgación, alteración, modificación o destrucción con el fin de proteger la confidencialidad, integridad y disponibilidad **[12]**.

De lo anterior, podemos definir la seguridad informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos de una organización para preservar la confidencialidad, integridad y disponibilidad de la información.

Sistemas de información seguros

Con base a los conceptos definidos anteriormente de seguridad, sistemas de información y seguridad de la información, se puede definir un SI seguro como:

Un SI que garantiza la confidencialidad, integridad y disponibilidad de los recursos del sistema y de la Información que maneja, mediante la aplicación de controles de seguridad, derivados del previo establecimiento de los requerimientos mínimos de seguridad a satisfacer.

La confidencialidad se refiere a que los objetos (información, módulos, recursos, etc.) de un sistema han de ser accedidos únicamente por elementos autorizados a ello (personas, procesos, etc.), y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.

La integridad se refiere a que los objetos sólo pueden ser modificados o eliminados por elementos autorizados, y de una manera controlada.

La disponibilidad se refiere a que los objetos del sistema tienen que permanecer accesibles a elementos autorizados y en el tiempo esperado.

APÉNDICE B: ISO 17799/ISO 27002

La norma ISO/IEC 27002 (resultante de la norma ISO/IEC 17799) es una compilación de las mejores prácticas de seguridad en TI aplicables a las empresas y organizaciones de cualquier tamaño o cualquier sector de actividad.

La norma se conforma de 11 dominios principales de seguridad, la cual agrupa un conjunto de objetivos de control y controles para cada uno de ellos. Los 11 dominios principales son:

a) Política de Seguridad;

b) Organización de la Seguridad de la Información;

c) Gestión de Activos;

d) Seguridad de Recursos Humanos;

e) Seguridad Física y Ambiental;

f) Gestión de Comunicaciones y Operaciones;

g) Control de Acceso;

h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información;

i) Gestión de Incidentes de Seguridad de la Información;

j) Gestión de la Continuidad Comercial;

k) Conformidad.

La norma ISO indica los objetivos de seguridad que deben lograrse pero no describe los procesos de gestión que deben aplicarse.

APÉNDICE C: COBIT, DS5: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.

El objetivo de control de alto nivel DS5 "Garantizar la seguridad de los Sistemas", incluye los siguientes objetivos de control específicos **[29]**:

DS5.1 Administración de la seguridad de TI: Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

DS5.2 Plan de seguridad de TI: Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware.

DS5.3 Administración de identidad: Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

DS5.4 Administración de cuentas del usuario: Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad: Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

DS5.6 Definición de incidente de seguridad: Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto.

DS5.7 Protección de la tecnología de seguridad: Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

DS5.8 Administración de llaves criptográficas : Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

DS5.9 Prevención, detección y corrección de software malicioso Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso.

DS5.10 Seguridad de la red: Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos sensitivos: Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

APÉNDICE D: CRITERIOS COMUNES DE EVALUACIÓN ISO/IEC 15408

ISO/IEC 15408

La norma ISO/IEC 15408(Common criteria)**[30]**, define un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o sistema IT. Proporciona un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto en base al conjunto de requisitos de seguridad y garantía, que satisface respecto a esta norma obteniendo de esa forma una certificación oficial de nivel de seguridad que satisface.

Por tanto, la norma ISO/IEC 15408 proporciona una guía muy útil a diferentes perfiles relacionados con las tecnologías de la seguridad

- Por un lado, desarrolladores de productos o sistemas de tecnologías de la información, que pueden ajustar sus diseños.
- Por otro lado, consumidores que pueden conocer el nivel de confianza y seguridad que los productos de tecnologías de la información y sistemas le ofrecen.
- En último lugar, los evaluadores de seguridad, que juzgan y certifican en que medida se ajusta una especificación de un producto o sistema IT a los requisitos de seguridad deseados.

El ISO/IEC 15408, establece los criterios de evaluación basados en un análisis riguroso del producto o sistema IT a evaluar y los requisitos que este satisface. Para ello, establece una clasificación jerárquica de los requisitos de seguridad. Se determinan diferentes tipos de agrupaciones de los requisitos siendo sus principales tipos los que vemos a continuación:

Clase: Conjunto de familias comparten un mismo objetivo de seguridad.

Familia: un grupo de componentes que comparten objetivos de seguridad pero con diferente énfasis o rigor.

Componente: un pequeño grupo de requisitos muy específicos y detallados. Es el menor elemento seleccionable para incluir en los documentos de perfiles de protección (PP) y especificación de objetivos de seguridad (ST).

La norma ISO/IEC 15408 se presenta como un conjunto de tres partes diferentes pero relacionadas:

- Parte 1. Introducción y modelo general.

Define los principios y conceptos generales de la evaluación de la seguridad en tecnologías de la información y presenta el modelo general de evaluación. También establece cómo se pueden realizar especificaciones formales de sistemas o productos IT atendiendo a los aspectos de seguridad de la información y su tratamiento.

- Protection Profile (PP): un conjunto de requisitos funcionales y de garantías independientes de implementación dirigidos a identificar un conjunto determinado de objetivos de seguridad en un determinado dominio. Especifica de forma general que se desea y necesita respecto a la seguridad de un determinado dominio de seguridad.

- Security Target (ST): un conjunto de requisitos funcionales y de garantías usado como especificaciones de seguridad de un producto o sistema concreto. Especifica que requisitos de seguridad proporciona o satisface un producto o sistema, ya basados en su implementación.

- Parte 2. Requisitos Funcionales de Seguridad.

Este tipo de requisitos definen un comportamiento deseado en materia de seguridad de un determinado producto o sistema IT y se agrupa en clases. Contiene las siguientes clases:

FAU- Auditoría

FCO- Comunicaciones

FCS- Soporte criptográfico

FDP- Protección de datos de usuario

FIA- Identificación y autenticación de usuario

FMT- Gestión de la seguridad

FPR- Privacidad

FPT- Protección de las funciones de seguridad del objetivo a evaluar

FRU- Utilización de recursos

FTA- Acceso al objetivo de evaluación

FTP- Canales seguros

- Parte 3. Requisitos de Garantías de Seguridad

Este tipo de requisitos establecen los niveles de confianza que ofrecen funciones de seguridad del producto o sistema. Trata de evaluar que garantías proporciona el producto o sistema en base a los requisitos que se satisfacen a lo largo del ciclo de vida del producto o sistema. Contiene las siguientes clases:

ACM- Gestión de la configuración

ADO- Operación y entrega

ADV- Desarrollo

AGD- Documentación y guías

ALC- Ciclo de vida

ATE- Prueba

AVA- Evaluación de vulnerabilidades

APE- Evaluación de perfiles de protección (PP)

ASE- Evaluación de objetivos de seguridad (ST)

AMA- Mantenimiento de garantías

Common Criteria o ISO/IEC 15408, proporciona niveles de garantía (EAL) como resultado final de la evaluación. Estos consisten en agrupaciones de requisitos vistos anteriormente en un paquete, de forma que obtener cierto nivel de garantía equivale a satisfacer por parte del objeto de evaluación ciertos paquetes de requisitos. Todo proceso de evaluación comienza con la definición del objeto a evaluar, que definimos a continuación:

Target of Security (TOE): Documento que realiza una descripción del producto o sistema que se va a evaluar, determinando los recursos y dispositivos que utiliza, la documentación que proporciona y el entorno en el que trabaja.

El principal objetivo de la norma ISO/IEC 15408, como hemos visto, es establecer de forma estándar un criterio de evaluación de la seguridad de los productos y sistemas IT. Ya hemos visto como la medición se realiza en base a un conjunto de requisitos y la demostración de que éstos son satisfechos. Esta norma nos proporciona dos tipos diferentes de evaluación.

Evaluación de Perfiles de Protección (PP)

El objetivo de tal evaluación es demostrar que un PP es completo, consistente y técnicamente sólido. Podrá ser utilizado como base para establecer requisitos destinados a definir un objetivo de seguridad (ST). Herramienta útil ya que permite definir especificaciones de seguridad independientes de implementación, que pueden ser utilizadas como base de especificaciones para productos o sistemas.

Evaluación de Objetivos de Evaluación (TOE)

Utilizando un objetivo de seguridad (ST) previamente evaluado como base, el objetivo de la evaluación es demostrar que todos los requisitos establecidos en el ST se encuentran implementados en el producto o sistema IT.

Respecto a los niveles de seguridad que se pueden lograr, voy a tratar resumidamente de describir cada uno de ellos a continuación.

EAL 1. Functionally tested.

Proporciona un nivel básico de seguridad realizado a través del análisis de las funciones de seguridad usando especificaciones informales de aspectos funcionales, de interfaz y las guías y documentación del producto o sistema IT para entender el comportamiento de seguridad.
Es aplicable cuando se requiere confianza en la correcta operación pero las amenazas de seguridad no se contemplan como un peligro serio. Este tipo de evaluación proporciona evidencias de que las funciones de seguridad del TOE se

encuentran implementadas de forma consistente con su documentación y proporcionan una protección adecuada contra las amenazas identificadas.

EAL 2. Structurally tested.

Exige, además de los requisitos del nivel anterior, haber realizado una descripción informal del diseño detallado, haber realizado pruebas en el desarrollo en base a las especificaciones funcionales , una confirmación independiente de esas pruebas, un análisis de la fuerza de las funciones de seguridad implementadas y evidencias de que el desarrollo ha verificado la respuesta del producto o sistema IT a las vulnerabilidades mas comunes. Requiere de la cooperación del equipo de desarrollo que entregue información sobre el diseño y resultados de pruebas. Este tipo de evaluación es adecuado en circunstancias en donde desarrolladores o usuarios requieren cierto nivel de garantías de seguridad cuando no tienen acceso a toda la documentación generada en la fase de desarrollo.

EAL 3. Methodically tested and checked.

Este nivel establece unos requisitos que obligan en la fase de diseño a un desarrollo metódico determinando. Este nivel añade a los requisitos del nivel anterior, el uso de controles de seguridad en los procesos de desarrollo que garantizan que el producto no ha sido manipulado durante su desarrollo. Por tanto, se realiza un análisis de las funciones de seguridad, en base a las especificaciones funcional de alto nivel, la documentación, guías del producto y los test obtenidos en la fase de prueba.

EAL 4. Methodically designed, tested and reviewed.

Requiere, además de los requisitos del nivel anterior, un análisis de vulnerabilidad independiente que demuestre resistencia a intrusos con bajo potencial de ataque y una especificación de bajo nivel del diseño de la implementación.

EAL 5. Semiformally designed and tested.

Representa un cambio significativo respecto al nivel anterior puesto que requiere de descripciones semiformales del diseño y la arquitectura además de completa documentación de la implementación. Además se realiza un completo análisis de vulnerabilidad que pruebe la resistencia frente atacantes de potencial medio y

mejora los mecanismos de control para garantizar y demostrar que el producto no es manipulado con respecto a las especificaciones durante el desarrollo.

EAL 6. Semiformally verified design and tested.

Añade respecto a los requisitos del nivel anterior, un detallado análisis de las funciones de seguridad, una representación estructurada de su implementación y semiformal demostración de la correspondencia entre las especificaciones de alto y bajo nivel con la implementación. Además debe demostrarse con un análisis de vulnerabilidades independiente, que en el desarrollo se ha probado la robustez de las funciones de seguridad frente a atacantes de alto potencial de daño.

EAL 7. Formally verified design and tested.

Es el nivel de certificación más alto. Debe probarse formalmente las fases de desarrollo y prueba. Además se exige una evaluación independiente de la confirmación de los resultados obtenidos, de las pruebas para detectar vulnerabilidades durante la fase de desarrollo así como sobre la robustez de las funciones de evaluación. Además, deberá realizarse un análisis independiente de vulnerabilidades para demostrar resistencia frente a un atacante de alto potencial.

La aparición de la norma ISO/IEC 15408 proporciona un criterio internacional que permite evaluar bajo criterios rigurosos y estrictos que protecciones en materia de seguridad nos proporciona un determinado producto o sistema IT. Los acuerdos firmados por diferentes países, permiten el reconocimiento mutuo de certificaciones realizadas en los diferentes organismos de certificación reconocidos internacionalmente. Ello facilita que los principales fabricantes de software estén evaluando sus productos para proporcionar "valor añadido" en la confianza y seguridad que en ellos se puede depositar.

Estos niveles de certificación serán mínimos exigibles para la selección y adquisición de software. Por otro lado, la aparición de diferentes perfiles de protección para diversos entornos de seguridad proporcionará conjuntos de especificaciones técnicas que se incorporarán a futuros desarrollos, proporcionando requisitos de seguridad establecidos ya en las fases de diseño de productos y sistemas IT. Todo ello contribuirá, seguramente, al incremento de la calidad y seguridad de los diferentes productos y sistemas IT, y por tanto, de la confianza que podrá depositarse en ellos.

APÉNDICE E: FIPS PUB 199

FISMA (Federal Information Security Management Act) es una ley por la que se decretan las medidas que deben aplicarse con el fin de asegurar los bienes y la información federal de los Estados Unidos.

El FISMA asigna al NIST(Nacional Institute of Normal and Technology) la responsabilidad de desarrollar las normas y procedimientos de seguridad que las agencias gubernamentales de los EUA deben respetar con el objetivo de reforzar el nivel de seguridad de los sistemas de información.

Estas normas se publicaron en los documentos "Federal Information Processing Standards Publication" (FIPS PUB, por sus siglas en inglés).

FIPS PUB 199, describe las normas para la clasificación de seguridad de la información federal y los Sistemas de Información (SI), en esta publicación se detalla la forma en que las organizaciones pueden clasificar la información y los SI.

La publicación FIPS 199 requiere que la organización clasifique sus sistemas de información como de bajo impacto, impacto moderado o alto impacto para los objetivos de seguridad de la confidencialidad, integridad y disponibilidad.

Los valores del impacto potencial asignado a los objetivos de seguridad correspondientes, son los valores más altos de entre las categorías de seguridad que se han determinado para cada tipo de información residente en estos sistemas de Información.

El formato generalizado para expresar la categoría de seguridad (CS) de un SI es:

$$CS_{SI} = \{(\text{confidencialidad, impacto}), (\text{integridad, impacto}), (\text{disponibilidad, impacto})\}$$

Los valores aceptables para el impacto potencial son bajo, moderado o alto.

- Un sistema de bajo impacto es un sistema de información en la que los tres objetivos de seguridad son bajos.

- Un sistema de moderado impacto es un sistema de información en los que al menos uno de los objetivos de seguridad es moderado y sin un objetivo de seguridad es mayor que la moderada.

- Y, por último, un sistema de alto impacto es un sistema de información en los que al menos uno de los objetivos de seguridad es alto.

Este documento y otros correspondientes a PUB FIPS, puede ser consultado en la página oficial de NIST:

http://csrc.nist.gov/publications/PubsFIPS.html

APÉNDICE F: FIPS PUB 200

FISMA (Federal Information Security Management Act) es una ley por la que se decretan las medidas que deben aplicarse con el fin de asegurar los bienes y la información federal de los Estados Unidos.

El FISMA asigna al NIST(Nacional Institute of Normal and Technology) la responsabilidad de desarrollar las normas y procedimientos de seguridad que las agencias gubernamentales de los Estados Unidos de America deben respetar con el objetivo de reforzar el nivel de seguridad de los sistemas de información.

Estas normas se publicaron en los documentos "Federal Information Processing Standards Publication" (FIPS PUB, por sus siglas en inglés).

En la publicación 200 (FIPS PUB 200), se describen los requerimientos mínimos de seguridad para la información y los sistemas de información. Las exigencias de seguridad descritas en FIPS PUB 200 cubren 17 dominios, estos son:

1. Control de acceso
2. Sensibilización y formación
3. Auditoría y responsabilidad
4. Evaluación de los controles
5. Gestión de las configuraciones
6. Plano de continuidad
7. Identificación y autentificación
8. Gestión de los incidentes
9. Mantenimiento
10. Protección de medios
11. Protección material y del entorno
12. Planificación
13. Acreditación
14. Evaluación de los riesgos
15. Adquisición de los sistemas y servicios
16. Protección de los sistemas y comunicaciones
17. Integridad de los sistemas y de la información

Descripción de los dominios sugeridos por FIPS PUB 200

1.- Control de acceso (AC)

Las organizaciones deben limitar el acceso de la información del sistema a los usuarios autorizados, procesos que actúan en nombre de los usuarios autorizados, o dispositivos (incluyendo otros SI) y los tipos de operaciones y funciones que a los usuarios autorizados se les permite ejecutar.

2.- Sensibilización y Formación (AT)

Las organizaciones deben: (i) asegurar que los administradores y usuarios de los sistemas de información de la organización son conscientes de los riesgos de seguridad asociados con sus actividades y de las leyes aplicables, órdenes ejecutivas, directivas, políticas, normas, instrucciones, reglamentos o procedimientos relacionados con la seguridad de los sistemas de información de la organización, y (ii) asegurar que el personal de organización están adecuadamente capacitados para llevar a cabo sus deberes y responsabilidades asignadas con respecto a la seguridad de la información.

3.- Auditoría y Rendición de Cuentas (AU)

Las organizaciones deben: (i) crear, proteger y conservar los registros de auditoría del SI en la medida necesaria para permitir el seguimiento, análisis, investigación y presentación de informes de actividades ilegales, no autorizadas o inapropiadas, del SI y (ii) asegurar que las acciones de los distintos usuarios del SI únicamente puede ser rastreado a estos usuarios para que puedan ser responsables de sus acciones.

4.- Certificación, Acreditación y evaluaciones de Seguridad (CA)

Las organizaciones deben: (i) evaluar periódicamente los controles de seguridad en los SI de la organización para determinar si los controles son eficaces en su aplicación; (ii) desarrollar e implementar planes de acción destinado a corregir las deficiencias y reducir o eliminar las vulnerabilidades en los SI de la organización, (iii) autorizar el funcionamiento de los SI de la organización y las conexiones con SI asociados, y (iv) supervisar los controles de seguridad del SI de manera continua para garantizar la continua efectividad de los controles.

5.- Gestión de la Configuración (CM)

Las organizaciones deben: (i) establecer y mantener las configuraciones de base y los inventarios de los SI de la organización (incluyendo hardware, software, firmware y documentación) a lo largo de los ciclos de vida de desarrollo del sistema respectivo, y (ii) establecer y aplicar los valores de configuración de seguridad para los productos de tecnología de la información empleada en los SI de la organización.

6.- Planes de Contingencia (CP)

Las organizaciones deben establecer, mantener e implementar eficazmente los planes de respuesta a emergencia, las operaciones de backup y recuperación de desastre de los SI de la organización para asegurar la disponibilidad de recursos de información crítica y la continuidad de las operaciones en situaciones de emergencia.

7.- Identificación y autenticación (IA)

Las organizaciones deben identificar a los usuarios del SI, procesos que actúan en nombre de los usuarios o dispositivos y autenticar (o comprobar) la identidad de estos usuarios, procesos o dispositivos, como requisito previo para permitir el acceso a los SI de la organización.

8.- Respuesta a Incidentes (IR)

Las organizaciones deben: (i) establecer el manejo de incidentes operacionales para los SI de la organización que incluye la preparación adecuada, la detección, análisis, contención, recuperación y actividades de respuesta del usuario, y (ii) rastrear, documentar e informar los incidentes a los oficiales de organización y/o autoridades.

9.- Mantenimiento (MA): Las organizaciones deben: (i) realizar un mantenimiento periódico y puntual sobre los SI de la organización, y (ii) proporcionar un control eficaz de las herramientas, técnicas, mecanismos y personal utilizado para llevar a cabo el mantenimiento del SI.

10.-Protección de Medios (MP): Las organizaciones deben: (i) proteger los medios de información del sistema, tanto en papel como digitales, (ii) limitar el acceso a la información sobre los medios de comunicación del SI a los usuarios autorizados,

y (iii) eliminar o destruir los medios de información del SI antes de su disposición o liberación para su reutilización.

11.- Protección física y Ambiental (PE)

Las organizaciones deben: (i) limitar el acceso físico a los SI, el equipo y los entornos operativos respectivos a las personas autorizadas, (ii) proteger la planta física e infraestructura de apoyo para los SI; (iii) proveer servicios de apoyo para los SI, (iv) proteger los SI contra riesgos ambientales, y (v) proporcionar los controles ambientales oportunos en las instalaciones que contienen los SI.

12.- Planificación (PL)

Las organizaciones deben desarrollar, documentar, actualizar periódicamente, e implementar planes de seguridad para los SI de la organización que describen los controles de seguridad implementados o planeados para los SI y de las normas de comportamiento para las personas que accedan a los SI.

13.- Personal de Seguridad (PS)

Las organizaciones deben: (i) garantizar que las personas que ocupan puestos de responsabilidad dentro de las organizaciones (incluidos los proveedores de servicios) son confiables, conocen y cumplen con los criterios de seguridad establecidos para esas posiciones, (ii) asegurar que la información de organización y SI están protegidos durante y después de las acciones del personal, tales como terminaciones y transferencias, y (iii) emplear sanciones formales para el personal que no cumplan con las políticas de seguridad y procedimientos de organización.

14.- Evaluación de Riesgos (RA)

Las organizaciones periódicamente deben evaluar el riesgo para las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), los activos de la organización y los individuos, como resultado de la operación de los SI de la organización y el consiguiente tratamiento, almacenamiento o transmisión de información de la organización.

15.- Adquisición de sistema y servicios (SA)

Las organizaciones deben: (i) asignar recursos suficientes para proteger adecuadamente los SI de la organización, (ii) emplear los procesos del ciclo de vida de desarrollo que incorporan consideraciones de seguridad de información;

(iii) emplear el uso del software y las restricciones de instalación, y (iv) garantizar que los proveedores externos emplean las medidas de seguridad adecuadas para proteger la información, aplicaciones y/o servicios externos de la organización.

16.- Protección de Sistemas y Comunicaciones (SC)

Las organizaciones deben: (i) monitorear, controlar y proteger las comunicaciones de la organización (es decir, la información transmitida o recibida por los SI de la organización) fuera de los limites internos y externos del SI, y (ii) emplear diseños de arquitectura, técnicas de desarrollo de software, ingeniería de sistemas y principios que promueven la seguridad de la información efectiva en los SI de la organización.

17.- Integridad de Sistema y la información (SI)

Las organizaciones deben: (i) identificar, reportar y corregir de manera oportuna los defectos encontrados en la información y los SI, (ii) proporcionar la protección apropiada contra código malicioso en los SI de la organización, y (iii) monitorear las alertas y avisos de seguridad del SI y tomar las acciones apropiadas en respuesta.

Tras el proceso de clasificación de seguridad de la información y los SI, la organización deberá seleccionar un conjunto apropiado de controles de seguridad para sus SI que satisfagan los requerimientos mínimos de seguridad establecidos correspondientes a la clasificación de seguridad del SI.

Para efectos de SI-bajo, las organizaciones deben, como mínimo, emplear debidamente los controles de seguridad definidos para la categoría de seguridad 'bajo' en el NIST 800-53

Para efectos de SI-moderado, las organizaciones deben, como mínimo, emplear debidamente los controles de seguridad definidos para la categoría de seguridad 'moderado' en el NIST 800-53

Para efectos de SI-alto, las organizaciones deben, como mínimo, emplear debidamente los controles de seguridad definidos para la categoría de seguridad 'alto' en el NIST 800-53

Este documento y otros correspondientes a PUB FIPS, puede ser consultado en la página oficial de NIST: http://csrc.nist.gov/publications/PubsFIPS.html

APÉNDICE G: APLICACIÓN DE LA METODOLOGÍA PROPUESTA

"MI EMPRESA"

Área de Auditoría de Seguridad

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 1 de 3

PROCEDIMIENTO OPERATIVO ESTANDAR

a) Objetivo. El objetivo de este POE es dar soporte a las actividades propias de la etapa de Planeación y Organización de la auditoría.

b) **Alcance.** Este procedimiento es utilizado para apoyar las actividades de definición, planeación, organización y preparación de los recursos, actividades y procedimientos necesario para obtener la información del SI que nos servirá de base para ejecutar la auditoría de seguridad.

c) **Responsable(s).**
Cargo: Líderes de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Equipo de Auditoría
Habilidad: Amplio conocimiento técnico en las áreas de seguridad, SI y auditoría, así como el conocimiento y utilización de múltiples herramientas de trabajo que apoyen sus actividades definidas en los planes y programas de auditoría.
Nombre:

d) **Definiciones**.
n/a

e) **Materiales: Hardware y Software**.
3. Editores de Texto
4. Plantillas de Instrumentos, pruebas y procedimientos diseñados para auditar el SI

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

"MI EMPRESA"

Área de Auditoría de seguridad

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 2 de 3

g) **Procedimiento.**

Etapa 1: Planeación y Organización de la Auditoría

1.1. El equipo de auditores de "Mi empresa" Identificaron el Origen de la Auditoría como una "Auditoría Subsecuente", dado que el navegador ya ha sido utilizado durante largo tiempo dentro de la empresa y se necesita determinar si los controles de seguridad implementados por el navegador han sido eficaces a través del tiempo.

Debido a que el navegador a analizar es una aplicación comercial, el enfoque que se le dio a la auditoría es el de un "entorno externo" o caja negra, es decir, estará limitado a la información que los propietarios de Mozilla Firefox® han puesto a disposición de los usuarios finales.

1.2. Una vez determinado el origen de la auditoría y el enfoque que se le daría a la auditoría, el equipo de auditores se dio a la tarea de recopilar información concerniente al navegador a evaluar, esta información se encontró de los sitios destinados por los propietarios de Mozilla Firefox® para proveer información de utilidad a los usuarios.

1.3. En "Mi empresa" los empleados utilizan el navegador Mozilla Firefox® para correr diversas aplicaciones que acceden a información confidencial de la organización, por lo que se ha clasificado la seguridad del navegador Mozilla Firefox® conforme al impacto que tendría sobre los objetivos de Confidencialidad, Integridad y disponibilidad de la Información en caso de ocurrir una violación de seguridad. La Clasificación de seguridad calculada conforme al FIPS 199 arrojo que C_S SI = "ALTO"

1.4. El equipo de auditores de "Mi empresa", realizo el estudio Preliminar del SI, obteniendo información concerniente a los manuales de usuario, requerimientos, características del navegador, aspectos de instalación entre otros. Debido a que Mozilla Firefox® es una aplicación comercial, no se pudo tener acceso a información considerada como "restringida" por lo que esto limitó el alcance de la auditoría. No fue necesario recopilar información correspondiente al marco regulatorio, ni los aspectos relacionados con la funcionalidad del SI; ya que se considera que estos aspectos ya han sido considerados por la empresa que los desarrolló antes de ser puestos a disposición de los usuarios finales.

1.5. El líder del equipo auditor, se dio a la tarea de definir el trabajo de auditoría que se realizaría:

1.5.1. Objetivo General: Auditar la seguridad del navegador Mozilla Firefox® para determinar la conveniencia de seguir utilizando el navegador dentro de la empresa o remplazarlo por otro.

"Mi Empresa"

Área de Auditoría de Seguridad

Número de POE: 1	Título: Planeación y Organización de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 3 de 3

1.5.2. Objetivos Específicos:

- Encontrar las vulnerabilidades de seguridad del navegador Mozilla Firefox®
- Calcular en Nivel de Riesgo de Mozilla Firefox® sobre los individuos, procesos y activos que utiliza.
- Tomar la decisión de seguir utilizando Mozilla Firefox®.

1.5.3. Alcance de la Auditoría: La auditoría de seguridad a Mozilla Firefox® se limitará a realizar una auditoría de caja negra, es decir bajo un entorno externo, delimitado a los aspectos que se encuentran documentados y de libre distribución por los dueños del SI (ya que el acceso a procedimientos, manuales, diseños y cierta documentación especializada se encuentra restringida a los usuarios finales).

1.6. El equipo de auditores de "Mi empresa " estableció los puntos que serían evaluados en la auditoría de Mozilla Firefox®, para ello se consideró que la auditoría sería realizada desde un entorno externo, por lo que el alcance de la auditoría sería limitado a los siguientes aspectos:

- ❖ Cumplimiento documental (orientado a documentación de apoyo a usuarios)
- ❖ Requerimientos mínimos de seguridad basados en la clasificación de seguridad del SI conforme al FIPS 200(limitado a la información distribuida por los propietarios de Mozilla Firefox®)
- ❖ Revisión de que el SI auditado está libre de los errores de programación más comunes.
- ❖ El cumplimiento funcional y normativo, no se evaluará dentro de la auditoría, ya que por ser un producto que ya se encuentra a disposición de los usuarios finales, se puede considerar que satisfacen totalmente estos 2 requerimientos.

1.7. El líder del equipo de auditores elaboró el Plan y Programa de auditoría para evaluar el nivel de exposición de Mozilla Firefox®, en los cuales definió responsables de cada actividad, estableció tiempos a cada actividad y los recursos necesarios.

1.8. El equipo de auditoría definió que la auditoría se llevaría a cabo mediante la aplicación de cheklists para los aspectos contemplados anteriormente (cumplimiento documental, requerimientos mínimos de seguridad, revisión de SI libre de errores más comunes). De igual manera, el líder del equipo auditor estableció los documentos, plantillas, medios y lineamientos con los cuales se llevaría a cabo la auditoría.

1.9. "Mi empresa" asigno al equipo de auditoría los recursos necesarios para llevar a cabo el Plan de auditoría desarrollado.

Referencias.

- FIPS 199, FIPS 200, Metodología de Auditoría en Seguridad para SI

"MI EMPRESA"

Área de Auditoría de Seguridad

Número de POE: 2	Título: Ejecución de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 1 de 7

PROCEDIMIENTO OPERATIVO ESTANDAR 2

a) **Objetivo.** El objetivo de este POE es dar soporte a las actividades propias de la etapa de Ejecución de la auditoría.

b) Alcance. Este procedimiento es utilizado para apoyar las tareas de ejecución de la auditoría, mediante la ejecución de las actividades previstas en el plan y programa de auditoría generado en la etapa anterior.

c) **Responsable(s).**
Cargo: Líder de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Equipo de Auditoría
Habilidad: Amplio conocimiento técnico en las áreas de seguridad, SI y auditoría, así como el conocimiento y utilización de múltiples herramientas de trabajo que apoyen sus actividades definidas en los planes y programas de auditoría.
Nombre:

d) **Definiciones**.
n/a

e) **Materiales: Hardware y Software**.
4. Herramientas y tecnología de apoyo para la búsqueda de vulnerabilidades y pruebas de seguridad.
5. Instrumentos, pruebas y procedimientos diseñados para auditar el SI

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

g) **Procedimiento.**

Etapa 2: Ejecución de la auditoría.

2.1. El equipo auditor ejecuto las actividades programadas para la auditoría conforme a los planes y programas desarrollados en la etapa 1.

2.1.1.Se evaluó el cumplimiento documental y se determino que **Mozilla Firefox® satisface los requerimientos documentales**.

Debido a que la auditoría se realizó a un SI comercial, solamente se consideró indispensable la disponibilidad de documentación de apoyo a las funciones y soporte al navegador. La información que los propietarios de Mozilla Firefox® ponen a disposición de los usuarios finales son:

- Documentos de apoyo a la descarga e instalación
- Tutoriales de navegación
- Tutoriales para personalizar el navegador
- Tutoriales para solucionar problemas con la seguridad del navegador
- Documentos para solucionar problemas frecuentes del navegador

2.1.2. Se evaluó el cumplimiento de los requerimientos mínimos de seguridad de acuerdo al FIPS PUB 200 y se determino que **para Mozilla Firefox® no se puede determinar si se satisfacen los requerimientos mínimos de seguridad;** debido a que no se cuenta con mucha información considerada como restringida y que es necesaria para validar el cumplimiento.

Debido a que la auditoría se realizó desde un entorno externo, no se pudo evaluar el nivel de cumplimiento de todos los requisitos de seguridad, en algunos casos por falta de información que se restringe por los propietarios del SI y en otros No Aplica (NA) por la naturaleza del SI:

1) **Sensibilización y Formación**: **Cumple.** Existe amplia documentación para usuarios conforme al uso y soporte del navegador, así como concientización a los usuarios del aspecto de seguridad.
2) **Gestión de la Configuración**: **Cumple.** Se lleva la gestión adecuada entre las diversas versiones del navegador, además de que permite la descarga de versiones anteriores a petición del usuario.
3) **Mantenimiento: Cumple**. Se toman las medidas necesarias para dar mantenimiento al navegador y dar respuesta a los incidentes reportados.

4) **Integridad de Sistema y la información**: **Cumple**. La información consultada afirma que las funciones implementadas por el navegador protegen la integridad de la información y del navegador.
5) Control de acceso: **NA**, la naturaleza de los navegadores no restringe el acceso.
6) Identificación y autenticación: **NA**, existe la identificación entre los componentes del navegador, pero por la naturaleza de los navegadores no existe autenticación por parte de los usuarios, la autenticación propiamente se lleva en las aplicaciones que se ejecutan sobre el navegador.
7) Certificación, Acreditación y evaluaciones de Seguridad: **NA,** la información obtenida de Mozilla Firefox® indica que existen evaluaciones de seguridad antes de que cada versión del navegador sea liberada, pero no se dispone de información de la certificación y acreditación de la seguridad del navegador.

Para los siguientes requerimientos no se cuenta con la información necesaria para validar el cumplimiento:

8) Auditoría y Rendición de Cuentas: **NA**.
9) Planes de Contingencia: **NA**.
10) Respuesta a Incidentes: **NA**.
11) Protección de Medios: **NA**.
12) Protección física y Ambiental: **NA**.
13) Planificación: **NA**.
14) Personal de Seguridad: **NA**.
15) Evaluación de Riesgos: **NA**.
16) Adquisición de sistema y servicios: **NA**.
17) Protección de Sistemas y Comunicaciones: **NA**.

2.1.3. Al ser una auditoría desde un entorno externo, no se contempla la revisión del cumplimiento documental, debido a que esta validación se debió llevar a cabo por los propietarios del navegador antes de poner el navegador a disposición de los usuarios finales. Bajo este enfoque se determina que Mozilla Firefox® satisfacen los requerimientos funcionales.

2.1.4. Al ser una auditoría desde un entorno externo, no se contempla la revisión del cumplimiento de los requerimientos regulatorios del navegador, debido a que esta validación se debió llevar a cabo por los propietarios del navegador antes de poner el navegador a disposición de los usuarios finales. Bajo este enfoque se determina que Mozilla Firefox® satisfacen los requerimientos regulatorios del SI.

2.1.5.Se determino que el navegador **Mozilla Firefox® no está libre de las vulnerabilidades más comunes y peligrosas en los SI**, conforme a reportes de seguridad emitidos por el sitio oficial del navegador **[54]**.

2.2. El equipo de auditores identificó y elaboró los documentos concernientes a los hallazgos obtenidos de la auditoría de seguridad a Mozilla Firefox®.

2.2.1.Se analizó la evidencia obtenida de la auditoría, entre los que se encuentran reportes de seguridad emitidos por los propietarios de Mozilla Firefox®. Las vulnerabilidades reportadas para Mozilla Firefox®, se agrupan respecto a su criticidad en **[54]**:

• Crítico: Una vulnerabilidad puede ser utilizada para ejecutar código malintencionado e instalar software, sin necesidad de interacción del usuario más allá de la navegación normal. En esta clasificación se encuentran las siguientes vulnerabilidades reportadas para Mozilla Firefox® 3.6.13:

- MFSA 2010-74: vulnerabilidades en la seguridad de memoria **[42]**.
- MFSA 2010-75: problemas asociados al desbordamiento de búfer al pasar cadenas de gran tamaño **[43].**
- MFSA 2010-76: aumento de privilegios de Chrome a través de "window.open" y un elemento "isindex" **[44]**.
- MFSA 2010-77: ejecución remota de código utilizando las etiquetas HTML dentro de un árbol XUL**[45]**.
- MFSA 2010-78: Añade soporte OTS, una librería para la normalización de fuentes descargables **[46]**.
- MFSA 2010-79: vulnerabilidad que permite evitar la seguridad de Java de LiveConnect cargado a través de los datos "URL meta refresh" **[47]**.
- MFSA 2010-80: vulnerabilidad de usar después de liberar los recursos en "nsDOMAttribute MutationObserver" **[48]**.
- MFSA 2010-81: vulnerabilidad de desbordamiento de entero en "NewIdArray" **[49]**.
- MFSA 2010-82: solución incompleta del CVE-2010-0179 **[50]**.

• Alta: La vulnerabilidad puede ser utilizada para recopilar los datos sensibles de los sitios en otras ventanas o inyectar datos o código en esos sitios, que no requiere más que acciones de navegación normal. En esta clasificación se encuentran la siguiente vulnerabilidad reportada para Mozilla Firefox® 3.6.13:

- MFSA 2010-83: suplantación del estado SSL de la barra de localización utilizando una página de error **[51]**.

• Moderado: Las vulnerabilidades que de otro modo sería alto o crítico, excepto que sólo funcionan en configuraciones poco comunes no por defecto o requiere que el usuario realice complicados y/o pasos poco probables. En esta clasificación se encuentra la siguiente vulnerabilidad reportada para Mozilla Firefox® 3.6.13:

- ❖ MFSA 2010-84: vulnerabilidad de XSS en la codificación de múltiples caracteres **[52]**.

2.2.2. Se determinarón las causas que originaron las vulnerabilidades encontradas en Mozilla Firefox®, el resultado es que se debieron a un mal diseño de la arquitectura del navegador y una mala codificación por parte de los desarrolladores.

2.2.3. El equipo de auditores ha sugerido que para eliminar las vulnerabilidades encontradas en la versión actual del navegador, será necesario implementar las acciones emitidas por los propietarios de Mozilla Firefox®. Para ello se necesita actualizar, a la brevedad posible, la versión actual del navegador(3.6.13), ya que las actualizaciones incluyen las correcciones a las vulnerabilidades encontradas y citadas anteriormente en el punto 2.2.1. Estas actualizaciones en las versiones de los navegadores deberá ser de ahora en adelante una actividad primordial por parte de los usuarios, por lo que será una tarea primordial de las áreas de seguridad dar el seguimiento necesario y establecer las politicas y procedimientos para su cumplimiento.

De igual manera, el equipo de auditores sugirió realizar un esfuerzo para concientizar y capacitar a los usuarios que utilicen el navegador como parte de sus funciones de trabajo, en los aspectos relacionados a los peligros y posibles amenazas a los que se encuentren sometidos al utilizar un navegador, asi como acciones preventivas para evitar cualquier tipo de violación a la seguridad y divulgación de información confidencial.

2.3. El equipo aditor se dió a la tarea de estimar el Riesgo del navegador Mozilla Firefox® con el propósito de determinar si las vulnerabilidades conocidas en el navegador representan un nivel aceptable de riesgo para las operaciones, activos e individuos de la empresa, el resultado fue el siguiente:

"MI EMPRESA"

Área de Auditoría de Seguridad

Número de POE: 2	Título: Ejecución de la Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 6 de 7

Requerimientos a Evaluar	Ponderación	% Cumplimiento del navegador	Total por Aspecto evaluado
Funcionales	20	100	20
Normativos	20	100	20
Documentales	20	100	20
Seguridad	NA		
Libre de Vulnerabilidades conocidas	40	70	28

Cumplimiento del navegador = 88 %

Para determinar el riesgo estimado del navegador, se tomaron en cuenta los siguientes aspectos:

- Clasificación de Seguridad (CS) del navegador: La CS del navegador fue determinada como alta, lo que conllevo a los integrantes del auditor a ser más estrictos en la estimación del riesgo.
- Cumplimiento del Navegador: El navegador cumple con un 88% de los aspectos evaluados, el restante 12% corresponde a las vulnerabilidades encontradas al evaluar que el navegador se encontrará libre de vulnerabilidades conocidas.
- Facilidad para implementar mejoras al navegador para reducir las vulnerabilidades encontradas: se encontró que no existe complejidad alguna para implementar las mejoras propuestas.
- Prioridad del navegador de seguir en operación dentro de la organización: La prioridad de utilizar el navegador por los usuarios de la empresa fue considerada como alta, debido a que la mayoría de las aplicaciones informáticas que son utilizadas dentro de su trabajo diario, son soportadas por el navegador.
- Comparativa con otros navegadores: Al ser un producto comercial, el comité autorizador, pudo darse una idea de que otros navegadores podrían sustituir a Mozilla Firefox®, considerando los aspectos funcionales, documentación, soporte, seguridad, etc. Lo anterior, conllevo a consultar diversas fuentes, la mayoría apuntaba a que la mejor opción en navegadores es Mozilla Firefox® **[53]**.

Después de evaluar estos puntos, el equipo auditor determino que:

El riesgo del navegador es Medio. Se considero que si bien el cumplimiento del navegador es de un 88%, las vulnerabilidades encontradas son ya conocidas y pueden ser explotadas por usuarios con los medios, conocimientos y recursos disponibles.

2.4. Una vez que el equipo auditor determino el riesgo del navegador, se dio a la tarea de elaborar el informe y dictamen preliminar de auditoría, el cual incluyó:

- Un resumen de los hallazgos obtenidos en el SI evaluado (obtenidos en el punto 2.2 de este POE)
- La estimación del riesgo del SI calculado con base en los hallazgos obtenidos de la auditoría(obtenidos en el punto 2.3 de este POE),
- El conjunto de recomendaciones emitidas por el equipo auditor para reducir las vulnerabilidades encontradas.
- El dictamen preliminar (opinión del equipo de auditoría con respecto a los resultados obtenidos).

Y finalmente se armo el paquete de evidencia de auditoría obtenida de la ejecución de la auditoría del navegador Mozilla Firefox®

2.5. El lider de la auditoría, presento el informe y dictamen preliminar de auditoría con el área de informática y seguridad para su discusión.

Referencias.

- Metodología de Auditoría en Seguridad para SI.
- Reporte de Vulnerabilidades para Mozilla Firefox® **[54].**
- Comparación de navegadores de internet **[53]**.

"Mi empresa"

Área de Auditoría de Seguridad

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 1 de 4

PROCEDIMIENTO OPERATIVO ESTANDAR 3

a) **Objetivo.** El objetivo de este POE es dar soporte a las actividades propias de la etapa de Dictamen de Auditoría.

b) **Alcance.** Este POE pretende proporcionar la documentación necesaria (evidencia obtenida y la determinación del nivel de riesgo del SI) al Comité autorizador de SI para que se tome la decisión de operación del SI auditado, se genere el informe y dictamen de auditoría y el plan de mejora.

c) **Responsable(s).**
Cargo: Líder de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Equipo de Auditoría
Habilidad: Amplio conocimiento técnico en las áreas de seguridad, SI y auditoría, así como el conocimiento y utilización de múltiples herramientas de trabajo que apoyen sus actividades definidas en los planes y programas de auditoría.
Nombre:

d) **Definiciones**.
Comité Autorizador de SI: Es un órgano conformado como mínimo por el líder de la auditoría, los responsables del área de seguridad de la información y un representante ejecutivo de la organización el cual pueda dar respaldo a la decisión tomada.

e) **Materiales: Hardware y Software**.
4. Editores de Texto.
5. Herramienta de planificación.
6. Plantillas de Informes y Plan de Mejora.

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

"Mi empresa"

Área de Auditoría de Seguridad

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 2 de 4

g) **Procedimiento.**

Etapa 3: Dictamen de la auditoría.

3.1. El comité autorizador, se dio a la tarea de tomar la decisión de operación del navegador Mozilla Firefox®, para ello se realizaron las siguientes actividades:

3.1.1. El líder de la auditoría, ubico y convoco al comité Autorizador de SI, el cual se conformo por el líder de la auditoría, personal del área de seguridad y un alto directivo de la empresa,

3.1.2. El equipo de auditoría preparó el "paquete de autorización" que se entrego a los integrantes del comité autorizador, el paquete de autorización se conformo de:

- ❖ La evidencia y documentación obtenida de la auditoría
- ❖ La estimación del Riesgo del navegador

3.1.3. El comité autorizador evaluó la evidencia obtenida de la auditoría, el nivel de riesgo estimado y algunos otros aspectos como:

- ❖ Clasificación de Seguridad (CS) del navegador: La CS del navegador fue determinada como alta, lo que conllevo a los integrantes del comité autorizador a ser más estrictos en la decisión a tomar.
- ❖ Porcentaje de cumplimiento del Navegador
- ❖ Facilidad de implementación de mejoras al navegador para reducir las vulnerabilidades encontradas
- ❖ Prioridad del navegador de seguir en operación dentro de la organización
- ❖ Comparativa con otros navegadores

Y se llegó al siguiente resultado:

Considerando que la CS del navegador es alta, estrictamente hablando no debería de permitirse la operación del navegador dentro de la empresa; ya que las vulnerabilidades encontradas presentan un gran riesgo en las operaciones, procesos e individuos de la empresa. Pero, considerando que:

- ❖ La prioridad de que el navegador siga operando es **alta**,
- ❖ Aún con las vulnerabilidades encontradas en el navegador, Mozilla Firefox® es considerado como la mejor opción comparado con productos similares y finalmente
- ❖ La implementación de mejoras para el navegador puede realizarse sin complejidad alguna, para disminuir el número de vulnerabilidades encontradas.

De lo anterior, el comité autorizador ha determinado que el navegador Mozilla Firefox® está **AUTORIZADO CONDICIONADO PARA OPERAR**, es decir puede seguir operando siempre y cuando atienda las recomendaciones emitidas por el equipo auditor en el tiempo y forma que se le especifique.

"Mi empresa"

Laboratorio de Auditoría de Seguridad

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hoja 3 de 4

3.6. Una vez emitida la decisión de autorización para el navegador Mozilla Firefox®, el equipo de auditores elaboró el informe y dictamen final de auditoría, para lo cual:

- ❖ Se hicieron las correcciones necesarias sobre el informe y dictamen preliminar de auditoría
- ❖ Se añadió al informe y dictamen final de auditoría, la decisión de autorización del navegador Mozilla Firefox®.
- ❖ Y finalmente se armo el paquete de evidencia obtenida como resultado de la auditoría.

3.6.1. Una de las actividades más importantes dentro de la auditoría, consistió en la elaboración del Plan de Mejora del navegador. Para ello se requirió la colaboración del líder de auditoría, del personal del área de informática y del personal del área de seguridad, los cuales:

- ❖ Definieron y planificaron las tareas necesarias para dar seguimiento a las recomendaciones hechas por el equipo auditor para eliminar o reducir las vulnerabilidades encontradas. Las tareas principales que se definieron se componen de :
  - Programa de actualización continua del navegador: ya que gran parte de las vulnerabilidades encontradas en un navegador son elimindas mediante la actualización o instalación de versiones más recientes del navegador.
  - Campañas de concientización y capacitación a los usuarios que utilicen el navegador como parte de sus funciones de trabajo, en los aspectos relacionados a los peligros y posibles amenazas a los que se encuentren sometidos al utilizar un navegador, asi como acciones preventivas para evitar cualquier tipo de violación a la seguridad y divulgación de información confidencial.
- ❖ Determinaron a los responsables de cada tarea:
  - El área de informática será responsable de llevar a cabo el programa de actualización continua del navegador.
  - El área de seguridad será responsable de llevar a cabo las campañas de concientización y capacitación a los usuarios finales
- ❖ Determinaron los recursos que son necesarios para la ejecución de cada tarea
- ❖ Estimaron y determinaron fechas compromiso para la realización de cada tarea
- ❖ Estimaron fechas de inicio y fin del Plan de Mejora del SI

“Mi empresa”

Área de Auditoría de Seguridad

Número de POE: 3	Título: Dictamen de Auditoría	
Revisión número:	Fecha de vigencia:	Hola 4 de 4

3.7. Finalmente, el informe y dictamen final de auditoría se presentado al responsable del área de informática, la persona que solicito la ejecución de una auditoría para el navegador Mozilla Firefox®. De igual manera se hizo llegar una copia de este informe y dictamen final al comité autorizador.

Una tarea crucial de esta etapa fue el resguardo y disponibilidad de consultar los resultados obtenidos de las auditorías y los planes de mejora elaborados, de tal manera que únicamente los usuarios autorizados puedan consultar los aspectos auditados en SI similares y no repetir errores y vulnerabilidades ya conocidas.

Referencias.

- Metodología de Auditoría en Seguridad para SI.
- Reporte de Vulnerabilidades para Mozilla Firefox® **[54].**
- Comparación de navegadores de internet **[53]**.

"Mi Empresa"

Área de Auditoría de Seguridad

Número de POE: 4	Título: Monitorear Cumplimiento del SI	
Revisión número:	Fecha de vigencia:	Hoja 1 de 3

PROCEDIMIENTO OPERATIVO ESTANDAR 4

a) **Objetivo.** El objetivo de este POE es dar soporte a las actividades propias de la etapa de monitoreo del cumplimento del SI auditado.

b) **Alcance.** Este POE pretende dar soporte al definición y documentación de actividades relacionas con el seguimiento de la implementación del plan de mejora, de igual manera apoya asentando formalmente las bases del monitoreo continuo del cumplimiento de los controles implementados por el SI y finalmente define, documentar y planifica las auditorías subsecuentes de seguridad al SI considerando que el ambiente de operación es cambiante.

c) **Responsable(s).**
Cargo: Líder de Auditoría
Habilidad: Planificar, Programar, Ejecutar y Dirigir la auditoría de seguridad del SI, mediante la aplicación y adaptación de la metodología de auditoría propuesta.
Nombre:

Cargo: Propietario del SI auditado
Habilidad: Coordinar las actividades y tareas destinadas a la adquisición, implementación y correcto funcionamiento del SI adquirido. Así como la gestión de los recursos, información y elementos del SI a su cargo.
Nombre:

d) **Definiciones**.
n/a

e) **Materiales: Hardware y Software**.
3. Editores de Texto
4. Herramienta de planificación

f) **Aspectos de seguridad.** La información generada y recopilada por este POE deberá ser resguardada, ya sea de manera física o digital por el equipo de auditores y por los dueños del SI.

APROBACIÓN

Elaboró	Supervisó	Autorizó
Fecha:	Fecha:	Fecha:

"Mi Empresa"

Área de Auditoría de Seguridad

Número de POE: 4	Título: Monitorear Cumplimiento del SI	
Revisión número:	Fecha de vigencia:	Hoja 2 de 3

g) **Procedimiento.**

Etapa 4: Monitorear Cumplimiento del SI

El monitoreo de cumplimiento se deriva de que el proceso de auditoría ha concluido con la decisión de operación del SI, y de aquí en adelante se deberá iniciar un nuevo proceso de mejora continua, en el cual las acciones realizadas contribuyan al continuo perfeccionamiento del SI.

Para lograr el perfeccionamiento del navegador evaluado, el líder de la auditoría, en colaboración con los responsables de las áreas de informática y de seguridad, realizaron la declaración formal y por escrito, de las tareas de supervisión y seguimiento de las actividades definidas dentro del Plan de mejora para el navegador, programación de las auditorías subsecuentes del SI y finalmente la definición de actividades y responsabilidades del monitoreo continuo a los controles de seguridad implementados en el SI de manera que aseguren que los controles implementados son eficaces a lo largo del tiempo.

4.1. Se definio un responsable del equipo de auditoría, quién será el responsable de dar el seguimiento a las acciones previstas dentro del Plan de Mejora. Por lo que fue necesario definir los criterios y aspectos necesarios para realizar el seguimiento, entre ellos se tiene:

- El establecimiento de fechas compromiso para comenzar con la revisión de las correcciones e implementaciones realizadas .
- La determinación de los lineamientos necesarios con los que se validará si los controles y correcciones implementadas cumplen con los objetivos y tareas establecidas en el Plan de Mejora.
  Entre los lineamientos más importantes por mencionar alguno, se encuentra que para valida la completa y correcta actualización de las versiones de los navegadores; se tomará una muestra de equipos al azar para validar que los navegadores que corren en las computadoras de la empresa han sido actualizados correctamente.
- De igual manera se solicitó a las áres de seguridad e informática, las cuales están acargo de la Implementación del Plan de mejora, del SI, la documentación de las actividades realizadas y problemas encontrados para atender el Plan de Mejora del SI.

"Mi Empresa"

Área de Auditoría de Seguridad

Número de POE: 4	Título: Monitorear Cumplimiento del SI	
Revisión número:	Fecha de vigencia:	Hoja 3 de 3

4.2. Programación de auditorías subsecuentes

Es bien sabido que el entorno de operación no es constante, por lo que tanto amenazas que atacan a los SI y vulnerabilidades encontradas en los SI crecen día con día, de ello se deriva la necesidad de realizar auditorías subsecuentes para determinar el nivel de exposición del navegador a lo largo del tiempo.

El lider de auditoría planificó las auditorías subsecuentes al navegador para refrendar la decisión de operación del navegador, se determinaron la fechas de realización y se establecieron los responsables a cargo de esta actividad.

4.3. Monitoreo Continuo del cumplimiento de los Controles de Seguridad del SI

El líder de la auditoría, determino conveniente establecer el monitoreo continuo del navegador, es decir de qué manera se comporta el navegador con el paso del tiempo.

Por ello se establecieron las acciones necesarias para monitorear el nivel de cumplimiento de los controles y funciones implementados en el SI, mediante la búsqueda de reportes de vulnerabilidades, e incidentes asociados al navegador, lo cual nos permitirá soporta la decisión de operación del navegador o procederá en la ejecución de una nueva auditoría para realizar una evaluación exhaustiva del nivel de exposición del navegador.

Referencias.

- Metodología de Auditoría en Seguridad para SI.

APÉNDICE H: PUBLICACIONES

Congresos Nacionales

1. **Propuesta de una instancia en la APF que contribuya a mejorar la seguridad de los sitios WEB del dominio MX**, M. Rodríguez-Argueta, A. Santiago-López, R. Vázquez-Medina, ROC&C 2010, Acapulco, México, Noviembre 2010.

Congresos Internacionales

2. **Alternativas para incorporar seguridad a los Sistemas de Información**, A. Santiago-López, M. Rodríguez-Argueta, A. Castañeda-Solís y R. Vázquez-Medina, VI Congreso de Telemática y telecomunicaciones, CUJAE, La Habana, Cuba, Noviembre 2010.

3. **Metodología de Evaluación de la Seguridad de Sitios Web**, M. Rodríguez-Argueta, A. Santiago-López, M.A. Morales-Santos, L.O. Pérez-González, R. Vázquez-Medina, VI Congreso de Telemática y telecomunicaciones, CUJAE, La Habana, Cuba, Noviembre 2010.

Propuesta de una instancia en la APF que contribuya a mejorar la seguridad de los sitios WEB del dominio MX

M. Rodríguez-Argueta
Instituto Politécnico Nacional, México
mrodriguezh0905@ipn.mx

A. Santiago-López
Instituto Politécnico Nacional, México
asantiagol0800@ipn.mx

R. Vázquez-Medina
Instituto Politécnico Nacional, México
rvazquez@ipn.mx

Abstract

A partir de un inventario reciente de sitios Web nacionales, que presentan o presentaron problemas de seguridad relacionados con XSS (Cross Site Scripting) y/o SQL Injection, y de sitios Web públicos destinados a la realización de prácticas de intrusión ética, se determina la necesidad de contar con una estrategia a nivel nacional dentro de las dependencias de la Administración Pública Federal (APF) que permita valorar el riesgo al que están expuestos sus sitios WEB y con ello se ofrecer una serie de recomendaciones de solución que los administradores de dichos sitios podrían seguir para mejorar la seguridad en sus portales WEB. Finalmente, se sugiere la puesta en operación de una instancia que supervise y de seguimiento a los problemas de seguridad informática en los sitios WEB de las APF, la cual pueda surgir a partir de la conocida Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico en México (CIDGE), creada por acuerdo presidencial el 9 de diciembre de 2005.

Introducción

Los servidores y aplicaciones Web tienen una alta probabilidad de ser comprometidos. Esto es porque deben estar disponibles públicamente en la Internet.

Más aún si estos servidores están asociados a portales WEB de alguna de las dependencias de la Administración Pública Federal (APF). Una vez que un servidor Web ha sido comprometido, el sistema puede proveer a los atacantes de un posible acceso a la red interna, aplicaciones, bases de datos y sistemas operativos. Resulta ser que estos activos son también susceptibles de ataques informáticos, ya que pudieran tener deficiencias de seguridad por un inadecuado mantenimiento o una mala administración.

Debido a que los servidores Web típicamente residen en la zona pública de una red de datos (DMZ: Demilitarized Zone) se convierten en activos más accesibles que otros sistemas, y en muchos casos, por esa razón se encuentran menos protegidos. De ahí que se consideren "más fáciles de explotar". Nótese que un servidor Web debe estar disponible en la Internet 7x24x365, lo cual lo hace más propenso como un potencial blanco de ataque y un consecuente punto acceso a la red interna institucional.

Bajo este escenario, cuando se observa a un servidor Web, en realidad se consideran cinco componentes relevantes: Hardware, Sistema Operativo, Aplicaciones, Bases de Datos y Servidor Web. Cada uno de estos componentes tiene sus propias deficiencias, derivadas de su conceptualización, diseño, implementación y administración. Sin embargo, para el alcance de este trabajo, los problemas relacionados con el hardware y el sistema operativo se consideran resueltos, debido a la intervención de los fabricantes de equipos y diseñadores de sistemas operativos. En estos casos, se considera que ellos proveen las actualizaciones correspondientes, y es decisión del administrador de estos equipos que sean aplicadas debidamente.

Así, en el alcance de este trabajo se consideran los problemas que pueden existir debido a una inadecuada

programación de las aplicaciones y configuración del servidor Web. En su caso, se considera también el inadecuado diseño de la base de datos, así como a las deficiencias en el manejador respectivo. La manifestación de estos problemas puede ser vista cuando un servidor Web puede ser objeto de ataques del tipo XSS (Cross Site Scripting) y SQL Injection, en todas sus variantes.

La estrategia a seguir en este trabajo ha sido la siguiente:

a) Usar las herramientas de Google Hacking para precisar el inventario de sitios Web nacionales que presentan o presentaron problemas de seguridad con XSS y/o SQL Injection.
b) Determinar las condiciones que facilitan la realización de los ataques XSS y SQL Injection en servidores WEB.
c) Precisar los indicadores y precursores de los ataques XSS y SQL Injection de acuerdo con las guías del NIST SP800-61.
d) Identificar en la Internet sitios Web públicos destinados a la realización de prácticas y ejercicios inofensivos de intrusión ética en los que se puedan aplicar ataques y documentar la evidencia que estos dejan de modo que se puedan generar las recomendaciones para los administradores de los servidores WEB.
e) Analizar y comprender los motivos por los cuales un atacante trata de comprometer un servidor Web.
f) Crear recomendaciones para disminuir el riesgo de una posible intrusión a la red corporativa de una organización desde su servidor Web.

Situación del mundo digital y el mundo real

"Internet es la copia digital de nuestro mundo real" y eso tiene implicaciones muy fuertes de seguridad para las personas y las instituciones. Diariamente se pueden leer noticias de seguridad informática relacionadas con ataques muy sofisticados como las siguientes: "Google to build great wall in wake of cyber attack" [1], "Google on the prowl, Web attacks increase, social networks unravel: All part of bold 2009 prophesies" [2] y "Web attack that poisons Google results gets worse" [3], entre otras.

Dada esta condición, existe una naturaleza dual de los ataques, pueden ocurrir en el mundo real o en el digital. En el mundo real, los ataques tienen una condición estoica o invariable; mientras que, en el mundo digital existen ataques cuya condición también es estoica, pero existen otros con una condición evolutiva o cambiante. En el mundo digital, las amenazas pueden ser las mismas que en el mundo real. Sin embargo, el ciberespacio impone condiciones que las hace diferentes. Aunque las amenazas en el mundo digital pueden tener los mismos objetivos y compartir las mismas técnicas que los ataques en el mundo real; en cierto modo, son diferentes, ya que cada vez son más comunes, se diseminan con más frecuencia, se hace muy difícil rastrear, capturar y condenar a los perpetradores; y sus efectos son más devastadores.

Bajo este escenario, se considera para esta discusión que la Internet tiene tres nuevas características. Individualmente, cada una de ellas es mala y la combinación de las tres es escalofriante.

a) *Automatización.* Permite que los ataques con una mínima probabilidad de éxito sean rentables, tal como el ataque salami. Este ataque se usa para desviar pequeñas cantidades de una fuente con grandes recursos como los bancos, de manera que su acción pasa desapercibida.
b) *Acción a la Distancia.* Internet permite que los atacantes NO estén físicamente en el lugar del cual desean obtener información, sobrepasando incluso, leyes de censura y marcos legales que tipifican acciones como actos criminales.
c) Técnicas de Propagación. Se refiere a la velocidad de propagación del Malware, la cual puede crecer en forma exponencial. Además del malware, existen herramientas de intrusión disponibles en la Internet, las cuales una vez liberadas, son imposibles de controlar.

Por otro lado, más allá de la parte tecnológica, lo que ocurre en la Internet NO es del todo diferente a lo que sucede en el mundo real. En el mundo digital, las personas interactúan con otras personas formando complejas redes sociales y empresariales, tal y como ocurre en el mundo real, pero ocurre a mayor escala, rebasando credos, fronteras e intereses. En el ciberespacio se tienen una amplia diversidad de ideologías en las comunidades, las cuales pueden ser grandes o pequeñas, locales o amplias. Además, en la Internet se tiene el comercio, hay acuerdos y contratos, desacuerdos y penalizaciones.

Las amenazas del mundo digital solamente reflejan las amenazas del mundo real. Si los desfalcos son una amenaza, entonces los desfalcos digitales son también una amenaza. Si los bancos son físicamente saqueados, entonces los bancos digitales también serán robados. La invasión a la privacidad es el mismo problema si toma la forma de un paparazzi con una cámara con un gran zoom, o si toma la forma de un hacker quien puede escuchar disimuladamente sesiones de chat "privadas".

El crimen en el ciberespacio incluye todo lo que se espera del mundo real: amenazas, negocios sucios, vandalismo, voyeurismo, extorsión, timos, fraude, etc.

Es por esta razón, que cuando estos ataques se llevan a cabo en una organización, sin pensar si son o NO exitosos, y producen un incidente de seguridad, es menester del personal de seguridad informática o administrador de red, saber recolectar evidencia en el momento. En este escenario, se requiere llevar a cabo un análisis de la evidencia digital, y establecer medidas más robustas de seguridad, de manera que se busque minimizar el posible impacto en la organización, de un ataque exitoso. Este análisis se debe realizar en el contexto de la informática forense, la cual es una ciencia muy poco difundida en México, a comparación de otros países quienes cuentan con instituciones certificadas y mundialmente conocidas, que crea recomendaciones para la recolección,

análisis, manejo y organización de la evidencia forense en un caso que tienen implicaciones administrativas, civiles o legales.

Estadísticas del dominio MX

Según estadísticas del Network Information Center–México, (NIC-México), actualmente la cantidad de nombres de dominio registrados bajo *mx* es de 394 200. De estos, el dominio *com.mx* corresponde al 73.53%, esto es, 289 834 subdominios; el dominio *org.mx* corresponde al 3.67%, esto es 14 478 subdominios; el dominio *edu.mx* corresponde al 1.63 %, esto es 6 416 subdominio; el dominio *gob.mx* corresponde al 1.33%, esto es 5 228 subdominios; y finalmente, el dominio *net.mx* corresponde al 0.10 %, esto es 413 subdominios. [4]

Se hizo una investigación en el CERT-UNAM y en otros sitios como NIC-México y el Instituto Nacional de Estadística Geografía e Informática (INEGI) y en México NO existen referencias sobre cuantos son los sitios web nacionales que se encuentran comprometidos. Asimismo, tampoco existen referencias que indiquen cuales son los tipos de ataques más usados hacia los servidores WEB.

Por lo tanto, es necesario contar con un inventario de sitios WEB comprometidos que ayude a las organizaciones a preservar la, confidencialidad, integridad y disponibilidad de la información que manejan, para evitar un mal uso de esta, así como a mantener la seguridad de los usuarios que acceden a los servicios del Portal Web de la organización.

De igual manera, es necesario contar con procedimientos operativos estándar, en el contexto de la informática forense, para saber a qué tipo de ataques un sitio WEB es susceptible y ubicar con precisión y rapidez la evidencia disponible.

Situación de los Portales WEB en la APF

En la actualidad, dentro de las dependencias de la APF existe la necesidad de contar con un portal que sea atractivo, ya que la buena imagen es causal de admiración. Se puede decir que una imagen vale más que mil palabras, pues tiene más poder de convencimiento.

Al paso del tiempo, la tecnología ha sufrido muchas transformaciones en busca de mejorar. Con ello, la forma de desarrollar software en general, y portales WEB en particular también se ha visto modificada. Antes los desarrolladores solamente se enfocaban en el diseño de su aplicación, dejando de lado la seguridad; por lo que para los atacantes las aplicaciones expuestas en la Internet resultaban ser presa fácil. Un ejemplo de esto es el surgimiento de la denominada "Ciber Protesta Mexicana", donde un grupo de Hackers boicoteó 33 páginas de medios de comunicación, negocios y sobre todo de gobiernos estatales y municipales.

En la actualidad los portales WEB, todavía se diseñan y se ponen en operación sin el uso de buenas prácticas de seguridad. Muchos portales de la APF han sido presa de ataques e intrusiones maliciosos (Black-Hat). Un porcentaje importante de los administradores de esos sitios NO se ha dado cuenta de que su sitio ha sido objeto de (ataque).

A pesar de los esfuerzos tan importantes que realiza el Gobierno Federal en México, NO existe una Unidad especializada de la APF que, de manera coordinada, realice actividades de identificación, clasificación y seguimiento en la mejora de los sitios WEB del gobierno federal que se encuentran vulnerables y/o que han sido comprometidos. Muestra de los esfuerzos a los que se hacen referencia son por ejemplo: la Policía Científica en la Secretaría de Seguridad Pública Federal, la cual tiene como misión reforzar las labores de investigación e inteligencia. Otro ejemplo es la Policía Cibernética como parte de la Policía Federal, cuyas funciones desde el año 2001 son combatir la pornografía infantil vía Internet, prevenir otros delitos que se cometen en y a través de una computadora, principalmente aquellos que atentan contra las instituciones y la población vulnerable y actualmente están conformando un banco de datos sobre pedofilia y agresiones sexuales.

Si México fuera víctima de un ataque cibernético dirigido como el sufrieron EUA y Corea del Sur, el 4 de julio del 2009, sería muy difícil que pudiera reaccionar de forma adecuada para soportar el impacto económico y social.

La creación del portal Web NO es solo la solución para ofrecer un servicio de calidad si NO que es necesario que este se conserve actualizado y protegido contra ataques malintencionados (Hackers, Crackers, etc.).

Ante tal situación se plantea la siguiente pregunta:

¿Cuál es el modelo de una Unidad de monitoreo y seguimiento de eventos de seguridad informática en las páginas WEB del Gobierno Federal?

Condiciones la propuesta

En este trabajo se sostiene la hipótesis de que es posible proponer un modelo integral para la conformación de una Unidad de Monitoreo y Seguimiento de Eventos de Seguridad Informática, que cuente con atribuciones legales que permitan ayudar a las dependencias de la APF, a mejorar la imagen y el servicio de sus portales WEB, y que además cuente con personal altamente calificado, el cual interactúe con los administradores de sistemas o portales WEB de otras dependencias de la APF, para ayudarles en la resolución de sus problemas de seguridad de la información. Para la conformación de esta Unidad es importante tener en cuenta los estándares internacionales y los lineamientos de la Comisión Intersecretarial de Gobierno Electrónico (CIDGE), considerando también las características administrativas, técnicas y funcionales suficientes de la Unidad de monitoreo y seguimiento para que actúe con autonomía, imparcialidad y autoridad sobre las dependencias de la APF que tengan Portales WEB afectados maliciosamente.

La CIDGE se crea con la intención reducir la brecha digital y transitar hacia una etapa de innovación de los procesos de la gestión pública y con el objetivo de promover y consolidar el uso y aprovechamiento de dichas tecnologías, mediante la coordinación de las acciones que, para ello, proponga la Secretaría de la Función Pública (SFP). La SFP de acuerdo con el decreto respectivo, será la responsable de

promover los mecanismos de comunicación e intercambio de información al interior de la APF. Entonces, la CIDGE es una comisión considerada como herramienta de apoyo para mejorar y transparentar la gestión pública, reducir la corrupción y ofrecer servicios electrónicos con mayor calidad a todos los ciudadanos.

Además de los aspectos administrativos y operativos antes mencionados en este trabajo se ha considerado pertinente conocer y entender como funcionan los ataques de XSS y SQL Injection, de manera que se pueda saber como ocurren y como pueden ser atendidos. Además se requiere conocer como puede ser posible la recolección de la evidencia factual cuando se realiza un análisis forense. Así mismo, con esta información se puede determinar las habilidades, capacidad e interés que requiere una persona para tener éxito cuando realiza un ataque de este tipo, siempre y cuando se genere el momento de oportunidad. Por ello, en este trabajo, se sostiene la hipótesis de que para lograr la formalidad requerida, la metodología propuesta deberá desarrollarse con base en Procedimientos Operativos Estándar.

De este modo, si un oficial de seguridad, administrador de sistemas o las personas involucradas en el aspecto técnico tratan de defender a la organización para la cual prestan sus servicios, se necesitan preguntar: "¿Cómo haría un atacante para entrar a su organización, que información trataría de conseguir y como borraría las huellas de su intrusión?" Estas serían las preguntas fundamentales que ayudarían a abordar este problema.

En resumen, la Unidad de Monitoreo y Seguimiento de Eventos de Seguridad Informática para mejorar la condición de seguridad de los Portales WEB de las dependencias de la APF, deberá contar con las características que le permitan ser incluida en la Comisión Intersecretarial del Gobierno Electrónico y que sus procesos estén alineados a los estándares internacionales. Además deberá contar con personal capacitado, el cual tenga facultades de interactuar con administradores y homólogos de las demás dependencias de la APF. Se espera que si esta unidad se pudiera conformar oficialmente se reduciría el número de portales WEB afectados por intrusiones o ataques maliciosos.

La estrategia a seguir en la conformación de la Unidad de Monitoreo y Seguimiento de Eventos de Seguridad informática sugerimos que sea la siguiente:

a) Realizar una revisión de los estándares internacionales que permitan definir los procesos y funciones de esta Unidad.
b) Investigar las condiciones que debe cumplir dicha Unidad, en el contexto de la Comisión Intersecretarial de Gobierno Electrónico, para que cuente con las atribuciones que le permitan ayudar a la APF a mejorar la imagen y servicio que proporcionan todas las dependencias, a través de sus portales WEB estando dirigidos a realizar recomendaciones, inspecciones, control, vigilancia, proponer soluciones y hasta poder sancionar por el incumplimiento de alguna obligación.
c) Diseñar y proponer un organigrama que permita que la Unidad propuesta cuente con el personal y las funciones pertinentes para el cumplimiento de su objetivo, misión y visión.
d) Identificar la manera que el personal de esta Unidad habrá de interactuar con los administradores de sistemas o portales WEB de dependencias de la APF.
e) Identificar el impacto que tendría en las entidades de la APF la creación de esta Unidad.
f) A partir del inventario de sitios WEB pertenecientes a la APF que han sido afectados identificar a los administradores de los portales y servicios WEB con los que se debe tener contacto.

El modelo de investigación que hemos adoptado para la conformación de esta Unidad es como el mostrado en la Figura 1.

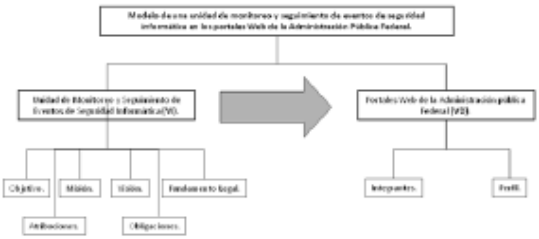


Figura 1. Modelo de Investigación en la conformación de la Unidad de Monitoreo y Seguimiento de Eventos de Seguridad Informática.

Dadas las necesidades de la Unidad de Monitoreo y Seguimiento de Eventos de Seguridad Informática, se busca que se encuentre dentro de la Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico como una Subcomisión, a fin de que esta Unidad cuente con las atribuciones suficientes para encargarse de monitorear los Portales Web de la APF. De esta manera, al momento de detectar un patrón fuera de lo estandarizado, deberá generarse un reporte que sugiera la solución más adecuada, buscando con ello reducir los incidentes de seguridad en los Portales Web. Además, de promover los estándares nacionales, internacionales y las mejores prácticas de seguridad de la información. También deberá tener atribuciones relacionadas con la creación y puesta en operación de programas de concientización en materia de Seguridad Informática en los Portales Web de la APF. De modo que, el personal de la APF esté capacitado en las mejores prácticas emitidas por esta unidad, lo cual le permita ser capaz de anticipar, detectar y actuar ante diferentes circunstancias relacionadas con incidentes de seguridad de la información.

Creemos que los objetivos que deberá alcanzar la Unidad especializada que aquí se propone, son los siguientes:

a) Desarrollar guías que ayuden a la creación de políticas en materia de Seguridad Informática para todos los administradores de los portales WEB de la APF.
b) Proporcionar las herramientas de software libre útiles para la buena administración de los portales WEB de la APF.
c) Vigilar los portales WEB de la APF mediante la utilización de técnicas de intrusión ética.
d) Difundir la existencia del software de actualización.
e) Planear programas de concientización del personal que administra los portales WEB de la APF.
f) Promover estándares, guías y las mejores prácticas en materia de Seguridad Informática aplicables a los portales WEB de la APF.
g) Revisar la integridad de los portales WEB de la APF.
h) Mantener una base de datos con las vulnerabilidades y acciones realizadas a solucionar vulnerabilidades de los sistemas con los que cuentan las entidades de la APF.
i) Emisión periódica de boletines informativos.

Recomendaciones

La recomendación que es posible establecer hasta el momento es tener en cuenta lo que sugieren los siguientes referentes nacionales, los cuales tiene su soporte y son congruentes con los respectivos referentes internacionales.

NMX-I-095-NYCE-2005 Tecnología de la Información – Software – Esta Norma Mexicana tiene como objetivo el proporcionar un Modelo para el Ciclo de Vida del software, adecuado a las necesidades de la industria de software mexicana para el desarrollo de Sistemas de información basados en WEB que promueva el uso de procesos normalizados, con el fin de elevar la calidad de sus productos y guíe a las organizaciones a la adopción de normas para obtener niveles de competitividad a nivel internacional.

NMX-I-27001-NYCE-2009 Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad Información – Requisitos. Esta Norma Mexicana aplicable a todo tipo de institución y detalla las necesidades para la creación, implementación, operación, supervisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información documentado, en el marco de los riesgos empresariales generales de la organización.

NMX-I-27002-NYCE-2009 Tecnología de la Información – Código de Buenas Prácticas para la Gestión de la Seguridad de la información. Es la Norma Mexicana que establece recomendaciones para realizar la gestión de la Seguridad de la Información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización.

Conclusiones

El contar con una Unidad de Monitoreo y Seguimiento de Eventos de Seguridad Informática en los portales WEB de las dependencias de la APF permitirá al Gobierno Federal reducir el riesgo que tiene de que alguna de sus entidades, personal o usuarios pueda ser victima de un ataque, agresión o afectación a la reputación al reducir el número de sitios WEB de la APF que tiene problemas de seguridad debido al seguimiento y monitoreo del estado que guarda la seguridad de estos sitios.

Según el Computer Security Institute, en su encuesta de 1998, las pérdidas económicas ocasionadas en EUA por delitos relacionados con nuevas tecnologías (principalmente accesos internos no autorizados) ascienden anualmente a más de 20.000 millones de pesetas, cifra que cada año se incrementa en más del 35%. De igual manera para México se requiere que exista una Unidad que permita generar información que pueda servir para establecer este tipo de conclusiones.

Referencias

[1]. http://www.theaustralian.com.au/business/news/google-to-build-great-wall-in-wake-of-cyber-attack/story-e6frg90x-1225818914737
[2]. http://www.networkworld.com/news/2008/123108-crystal-ball-prophesies.html
[3]. http://www.networkworld.com/news/2009/051909-web-attack-that-poisons-google.html
[4]. www.nic.mx

Biografía

Mario Rodríguez Argueta
Recibió el título de Ingeniero en Comunicaciones y Electrónica en Abril del 2007 en el Instituto Politécnico Nacional. Actualmente estudia la Maestría en Ingeniería en Seguridad y Tecnologías de la Información en la unidad Culhuacan del IPN. Sus áreas de interés son las redes de datos, seguridad de la información e informática forense.

Rubén Vázquez Medina
Recibió el título de Ingeniero en Electrónica especialidad en Comunicaciones en Octubre de 1988 en la Universidad Autónoma Metropolitana, el grado de Maestro en Ciencias especialidad en Ingeniería Eléctrica opción en Telecomunicaciones en Septiembre de 1991 en el CINVESTA- IPN, y el grado de Doctor en Ciencias en la Universidad Autónoma Metropolitana en Octubre de 2008. Fue jefe de la Sección de Estudios de Posgrado e Investigación de la ESIME Culhuacan del 28 de Marzo del 2003 al 17 de agosto del 2006. Su puesto actual es de profesor/investigador en el Instituto Politécnico Nacional.

15 del 29 de Noviembre al 3 de Diciembre de 2010
CONVENCION CIENTIFICA
DE INGENIERÍA Y ARQUITECTURA

46 ANIVERSARIO cujae 2010

ALTERNATIVAS PARA INCORPORAR SEGURIDAD A LOS SISTEMAS DE INFORMACIÓN.

Azucena Santiago López, Mario Rodríguez Argueta, Antonio Castañeda Solís y Rubén Vázquez Medina

Instituto Politécnico Nacional, ESIME Culhuacan, México, D.F., C.P. 04430

e-mail: {asantiagol0800, mrodriguezh0905, acastanedas, ruvazquez}@ipn.mx.

RESUMEN. Para los dueños de los sistemas de información (SI), especialistas en informática, desarrolladores y auditores de seguridad de la información debe ser importante contar con un mecanismo que les permita tener un grado de certeza en la seguridad de sus SI. En este artículo se propone que para un SI, desarrollado o adquirido, debe considerarse como prioridad cumplir no solo con los requisitos funcionales, sino también con requisitos mínimos de seguridad. Así, en este artículo se comienza con una descripción general de los SI, conceptos generales de seguridad y lo que debe considerarse en un SI Seguro. Se abordan dos opciones para dotar de seguridad a los SI. La primera (a priori), sugiere la adopción de una metodología que considere el ciclo de vida de desarrollo seguro. La segunda opción (a posteriori), sugiere el uso de un modelo de auditoría de seguridad de SI, el cual garantice que las aplicaciones desarrolladas cuenten con los controles necesarios que reduzcan la vulnerabilidad típica de las aplicaciones. Se pretende que estas dos opciones en el aseguramiento de un SI sirvan como recomendaciones para reducir su riesgo y vulnerabilidad.

Palabras Claves. Auditoria de seguridad, Ciclo de vida de desarrollo seguro, Sistemas de Información, Sistemas de Información Seguros.

ALTERNATIVES TO HARDEN INFORMATION SYSTEMS.

ABSTRACT. This paper shows that is very important to count with a mechanism that let to the Information Systems (IS) owners, computer specialists, developers and information security auditors to have a trust-security rate regarding to their IS. It's proposed that for a developed or acquired system not only the functional requirements but the less security requirements must be fulfilled to be considered as a priority. Therefore, in this paper a general description about IS, general security concepts and topics that have to be considered as a secured IS is begun with. Two options are brought up to give security to the IS. The first manner (a priori) suggests the adoption of a methodology that consider to the IS Security Development Life Cycle. The second manner (a posteriori) suggest a IS Security Audit model usage, which guarantees that the developed applications count with necessary controls that reduce the usual application vulnerabilities. These two options in the IS hardening are pretended to aid as recommendations to reduce the risk and vulnerabilities in the IS.

Key words: Security audit, Security Development Lifecycle, Information Systems, Secure Information Systems.

I. INTRODUCCIÓN

El activo más importante dentro de cualquier organización es la información. A través de su procesamiento se puede crear valor y se puede contribuir al logro de objetivos. Por ello, las organizaciones, como parte de sus procesos de negocio, crecimiento e innovación, adquieren tecnologías que apoyen el procesamiento de información y la toma de decisiones, así como la automatización de sus procesos de negocio. Muchas organizaciones adquieren tecnología de software, aplicaciones diseñadas a la medida, mediante consultores informáticos especializados, quienes mediante diversas metodologías realizan un análisis de requerimientos y un diseño del sistema. Para luego desarrollar aplicaciones, sus pruebas unitarias e integrales de la funcionalidad, así como su implementación y mantenimiento.

En la actualidad el desarrollo de SI está adquiriendo mucha importancia. En este sentido, en el artículo "La inversión en Tecnologías de la Información crecerá a nivel mundial un 4.6 por ciento en 2010 " publicado en enero de 2010 [1], Martín Pérez hace una investigación acerca de la inversión en los mercados de las tecnologías de la información (TI). Respecto a la adquisición de software, comenta que el gasto en software va a experimentar un crecimiento de 4.9%, alcanzando los 231,500 millones de dólares a nivel mundial.

Generalmente, los desarrolladores de aplicaciones orientan su tiempo, conocimientos, recursos y esfuerzo a la funcionalidad especificada, sin considerar a la par, la implementación de

controles de seguridad en sus desarrollos. Dejan la fase de validación de seguridad para el final y la mayoría de los casos es independiente al proceso de desarrollo. Con este proceder es una tarea difícil establecer un nivel determinado de seguridad en los sistemas que se desarrollan. Esta situación genera incertidumbre en las organizaciones propietarias de los SI, pues sus SI interactúan con otros sistemas a través de las redes de datos, lo cual generalmente pone en evidencia su vulnerabilidad.

En este trabajo se ofrece información de utilidad para los dueños de SI, especialistas en informática y seguridad, de manera que no solo se cumplan con los requisitos funcionales, sino también con requisitos mínimos de seguridad cuando se desarrolla o adquiere un SI. Adoptar cualquiera de las dos opciones que aquí se proponen, dará un grado de certeza de que los SI cubren los requisitos mínimos de seguridad y son aptos para minimizar el impacto causado por fallos, violaciones o alteraciones que se pudieran llegar a efectuar sobre ellos.

II. Sistemas de Información, Consideraciones de Desarrollo, Implementación y Seguridad.

Un SI es un conjunto de elementos interrelacionados para obtener, procesar, almacenar, administrar, formatear, difundir y, en determinado momento, destruir la información procesada. Un SI concentran todos los elementos que forman parte de un proceso productivo, es la realización en software de un conjunto de tareas y actividades para cumplir un objetivo. Esta realización incluye la administración del sistema, la alimentación de información y el procesamiento de datos, así como su transporte, formateo y distribución dentro y fuera de la organización.

Los SI se pueden clasificar por los objetivos que persiguen, o la funcionalidad que implementan. En cualquier caso, una decisión importante a considerar, es la forma en que la organización adquirirá el sistema. Al adquirir un SI se pueden encontrar dos tipos: sistemas comerciales y sistemas diseñados a la medida. Los sistemas comerciales aportan un comportamiento global del proceso que automatizan; es decir, parten y se crean de la totalidad de funciones posibles del proceso. Así, al adquirir un sistema comercial, será necesario definir parámetros dentro de las funciones que integran al SI que se ha adquirido. En el mismo sentido, cuando se adquieren sistemas comerciales muchas de sus funciones son desaprovechadas, ya sea porque no se alinean a la cultura organizacional o porque simplemente el modelo de negocio no lo requiere. En general, adquirir un sistema comercial es mucho más costoso que el diseñado a la medida; entre otras razones, por el tiempo, esfuerzo y trabajo adicional para validar la totalidad de sus funciones y proveer cierto grado de seguridad a la aplicación. Por otro lado, los sistemas diseñados a la medida, dan la certeza de que el SI adquirido, refleja en su totalidad el proceso que automatiza; es decir, la funcionalidad se diseña única y exclusivamente para los requerimientos del negocio. Esto genera un mejor aprovechamiento de recursos, procesos alineados al negocio y seguridad de que el SI cumple al 100% con las expectativas funcionales, de negocio y requerimientos especificados, además de proveer una aplicación exclusiva para la organización.

En muchos casos, cuando se adquiere un SI se pone escasa atención, o peor aún se deja de lado un aspecto muy importante, la seguridad. Definiendo a la seguridad como todas aquellas medidas encaminadas a proteger y salvaguardar los activos. La seguridad debería ser tomada como un requisito de cualquier sistema, lo cual indique que el sistema está libre de todo peligro, daño o riesgo.

Actualmente, existen innovaciones que procuran que los SI sean lo menos vulnerables posible, tratando de evitar todo aquello que pueda afectar su funcionamiento. El concepto de seguridad sigue siendo, para varios, de carácter utópico, ya que no existe un sistema que pueda ser considerado 100% seguro. Morrie Gasser [2], describe que a pesar de los avances significativos en el estado del arte de la seguridad informática, en los últimos años, la información en las computadoras es más vulnerable que nunca. Cada avance tecnológico importante en informática plantea nuevas amenazas de seguridad que requieren nuevas soluciones, la tecnología avanza más rápido que la velocidad con la que este tipo de soluciones son desarrolladas.

Por lo general, la seguridad en las aplicaciones se lleva de forma independiente a su desarrollo. Las organizaciones se preocupan por invertir en seguridad perimetral que les proporcione cierto grado de certeza de que su infraestructura informática está protegida. El error en esta concepción e implementación está en que en muchos casos la vulnerabilidad se encuentra en el diseño de las aplicaciones, no en su infraestructura. En [3] se hace alusión a este error y se resume en la Fig. 1.

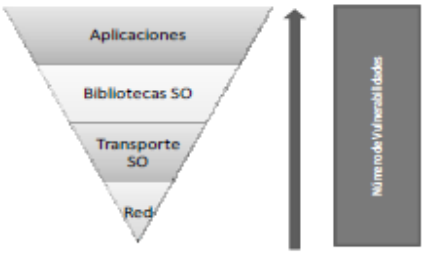


Fig 1. Vulnerabilidades en Red, Sistemas Operativos y Aplicaciones.

Ahora bien, mantener un sistema seguro consiste básicamente en garantizar cinco aspectos: confidencialidad, integridad, disponibilidad, confiabilidad y no repudio, según los requerimientos impuestos por la visión, misión y objetivos de la organización. La confidencialidad se refiere a que los objetos (información, módulos, recursos, etc.) de un sistema han de ser accedidos únicamente por elementos autorizados (personas, procesos, etc.), y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades. La integridad se refiere a que los objetos sólo

pueden ser modificados por elementos autorizados, y de una manera controlada. La disponibilidad se refiere a que los objetos del sistema tienen que permanecer accesibles a elementos autorizados, en tiempo y forma. La confiabilidad se refiere a que el sistema debe realizar la función para la que fue diseñado, es decir que genere los resultados esperados. El no repudio se refiere a la protección que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

III. Ciclo de Vida de Desarrollo de Software SDLC.

Metodología de desarrollo de SI.

Una metodología provee apoyo en la planificación de las actividades de un proyecto. Permite unificar criterios en la organización y proporciona puntos de control y revisión. Existen diversas metodologías de desarrollo de software, cada una de ellas tiene su propio enfoque, algunas son más conocidas y aceptadas que otras. En general, una metodología consta de las siguientes fases: análisis, diseño, construcción, pruebas e implementación, considerando que el mantenimiento y la documentación son procesos continuos. La mayoría de las metodologías no toman en cuenta las consideraciones de seguridad en cada fase. Se ve a la seguridad como una parte aislada del proceso de desarrollo. En el mejor de los casos, la seguridad solo es evaluada en la fase de pruebas, donde se busca detectar la mayor cantidad de fallas funcionales y en menor medida las fallas de seguridad.

Evaluación de vulnerabilidades en las distintas fases del Ciclo de Vida de Desarrollo de Software.

Dentro de cada fase del ciclo de vida de desarrollo (CVDS) se aportan, por error u omisión, diversas deficiencias al producto final, las cuales pueden ser de tipo funcional y de seguridad. Las deficiencias funcionales, son aquellas ligadas específicamente a los aspectos del negocio. La mayoría de las veces se debe a una mala conceptualización de las necesidades reales del negocio, suele suceder en las etapas de análisis y diseño. Las deficiencias de seguridad, son aquellas ligadas con medidas de seguridad implementadas erróneamente, insuficientemente o de manera nula. Generalmente, estas deficiencias se conocen ampliamente y se encuentran clasificadas. Joseph Feiman en [4], realizó un análisis y detectó que las deficiencias de los SI son concebidas desde las primeras etapas del ciclo de vida del desarrollo. El porcentaje que en ese trabajo se dio de aportación en cada etapa del ciclo de vida de desarrollo se puede apreciar en la Fig. 2.

Por lo anterior, surge la necesidad de tener estrategias adicionales a la seguridad perimetral, a la que actualmente se encuentran sometidos los SI en una organización. Este enfoque sugiere no confiar plenamente en los mecanismos de seguridad externos y optar por fortalecer a los SI desde su creación.

Controles de seguridad a lo largo del Ciclo de vida de desarrollo de Software		
Deficiencias encontradas	**Fases**	**Aportación de Deficiencias**
En la toma de requerimientos, definición de flujos de procesos de negocio, algoritmos.	Análisis	15%
Causadas por interrelaciones de módulos y servicios (Web), lógica y flujo de datos.	Diseño	40%
En las instrucciones del lenguaje, implementación de la lógica y flujo de datos	Construcción	35%
En ejecutables, interfaz de Usuario. Montaje de los servicios de seguridad	Pruebas	10%
Falta de actualizaciones, errores administrativos, errores de configuración. Si se encuentran deficiencias se regresa al análisis.	Operación	

Fig. 2 Controles de seguridad a lo largo del Ciclo de vida de desarrollo de Software (CVDS)

IV. Ciclo de Vida de Desarrollo Seguro.

En un Ciclo de vida de desarrollo seguro (CVDS Seguro), la seguridad se aborda desde la primera etapa del ciclo de desarrollo y a lo largo de todas las etapas. En cada etapa, se realizan diversas actividades que en su conjunto aumentan la seguridad de la aplicación. Incluir seguridad tempranamente en el CVDS suele resultar menos costoso y más eficiente que agregarla a un sistema en operación [5]. Es importante que el personal de seguridad de la información participe en las distintas etapas de desarrollo.

Las organizaciones han empezado a darle la importancia debida a la seguridad en las aplicaciones. Existen modelos de desarrollo seguro, los cuales están disponibles al público. La idea es que estos modelos puedan ser aceptados y utilizados, y posteriormente enriquecidos con las aportaciones y sugerencias y experiencia de los profesionales que han implementado estos modelos dentro de las organizaciones.

Existen algunas publicaciones que abordan el CVDS Seguro. Entre las más documentadas y aceptadas, se tiene la metodología de Microsoft "Security Development LifeCycle" y a las recomendaciones emitidas por el Instituto Nacional de Estándares y Tecnologías (NIST: NAtional Institute of Standards and Technology) las cuales se documentan en el estándar SP800-64 "Security Considerations in the Information System Development Life Cycle".

En general, las tareas de seguridad que son necesarias para dotar de seguridad a los SI en cada fase del CVDS son:

- Etapa de Análisis.- Se debe identificar aquellos requerimientos funcionales que tendrán impacto en la seguridad de la aplicación. Por ejemplo, requerimientos de cumplimiento regulatorio, tipo de información que se manejará y requerimientos de registros de auditoría.

- Etapa de diseño.- Se debe contemplar el diseño de autorización (roles, permisos y privilegios de la aplicación), diseño de autenticación, diseño de mensajes de error y advertencia y diseño de los mecanismos de protección de datos. Una vez que se cuenta con el diseño detallado de la aplicación, una práctica interesante es realizar sobre el diseño un análisis de riesgos. Estas técnicas permiten definir un marco para identificar debilidades de seguridad en el software, antes de la etapa de codificación.

- Etapa de codificación.- El equipo de desarrollo programa, prueba unitariamente e integra el SI. Las tareas de seguridad que se aplican son: uso de estándares de codificación y pruebas, uso de herramientas de comprobación de seguridad, revisiones del código y exploración del código con herramientas especializadas.

- Etapa de pruebas.- Se desarrollan casos de prueba de funcionalidad y seguridad. Las pruebas de seguridad se basan principalmente en probar la aplicación con escenarios no planificados, es decir, valores fuera de rango, formatos incorrectos, valores nulos, en general entradas y comportamiento no esperados.

- Etapa de implementación.- Se deben contemplar las tareas de transición de un ambiente a otro, como son: cambio de usuarios y contraseñas iniciales o por defecto, borrado de datos de prueba y cambio de permisos de acceso.

Metodología de Microsoft "Security Development LifeCycle".

Microsoft Security Development Lifecycle (SDL) [6], incorpora varias actividades y materiales relacionados con la seguridad a cada una de las fases del proceso de desarrollo de software. Estas actividades y materiales incluyen el desarrollo de modelos de amenazas durante el diseño de software, el uso de herramientas de exploración del código de análisis estático, durante la implementación, y la realización de revisiones del código y pruebas de seguridad durante una "campaña de seguridad". Antes del lanzamiento de software sometido al SDL, un equipo independiente del grupo de desarrollo debe realizar una revisión final de seguridad. En comparación con el software que no se ha sometido al SDL, el software que ha seguido este proceso ha presentado una reducción considerable en el número de detección externa de vulnerabilidades de seguridad.

Esta metodología supone que hay un grupo central en la organización que controla el desarrollo y la evolución de las prácticas recomendadas de seguridad y las mejoras de los procesos. Actúa como fuente de conocimientos para toda la organización y realiza la revisión final de seguridad antes del lanzamiento del software. Según la experiencia de Microsoft, la existencia de tal organización es vital para implementar adecuadamente el SDL, así como para mejorar la seguridad del software. Sin embargo, algunas organizaciones delegan en un consultor externo esta función de "equipo de seguridad central". Describe la integración de un conjunto de pasos destinados a aumentar la seguridad del software durante el proceso de desarrollo que suelen utilizar grandes organizaciones. El objetivo de dichas mejoras de procesos es reducir el número y la gravedad de las deficiencias de seguridad. Recomienda que el equipo de seguridad pertenezca a la organización donde se desarrollo el software, debido a que el equipo de seguridad debe estar disponible para recurrir a él con frecuencia durante el diseño y el desarrollo del software, y es preciso confiarle información técnica y empresarial confidencial.

Las fases de SDL definidas por Microsoft son las siguientes: entrenamiento, análisis de requerimientos, diseño, implementación, verificación, liberación y respuesta. Durante la fase de Entrenamiento, se llevan acabo actividades de capacitación, las cuales permiten aprender acerca de las bases de seguridad, uso de técnicas especificas y actualización de las amenazas recientes en el ámbito de seguridad. Durante la fase de análisis de requisitos se llevan acabo actividades para integrar las características de seguridad y las medidas de control con los programas que probablemente se utilizarán con el software que están desarrollando. Esta fase es considerada como la mejor para integrar la seguridad a los procesos de desarrollo e identificar los objetivos de seguridad. En la fase de diseño, se debe identificar la estructura y los requisitos globales del software y se establece el uso de las mejores prácticas a utilizar. Desde el punto de vista de la seguridad, los elementos clave de la fase de diseño son: definir la arquitectura de seguridad y las directrices de diseño, documentar los elementos de la superficie de ataque del software y realizar un modelado de las amenazas. Durante la fase de implementación, se prueba e integra el software. Los pasos destinados a eliminar los errores de seguridad o a impedir que se incluyan desde el principio reducen la probabilidad de que las deficiencias de seguridad lleguen a la versión final. Las tareas que se aplican en la fase son: uso de: estándares de codificación y de pruebas, herramientas de comprobación de seguridad, herramientas de exploración del código de análisis estático y realizar revisiones del código. En la fase de verificación, se realizan revisiones del código de seguridad aparte de las realizadas en la fase de implementación, así como la realización de pruebas centradas en la seguridad. Durante la fase de liberación, el software debe someterse a una revisión final de seguridad, la cual definirá si desde el punto de vista de la seguridad el software está preparado para su lanzamiento. Esta revisión se lleva a cabo mediante una revisión independiente del software que realiza el equipo de seguridad central de la organización. Adicional a ello, se lleva a cabo la creación del plan de respuesta a

incidentes. Durante la fase de respuesta, el equipo de desarrollo debe estar disponible para responder a cualquier posible deficiencia de seguridad, también ayuda a los equipos de desarrollo y de seguridad a adaptar los procesos para que otros errores similares no se repitan en el futuro.

SP800-64 Consideraciones de Seguridad en el ciclo de Vida de desarrollo de SI.

El NIST emite una serie de recomendaciones de seguridad en la publicación SP800-64 [7], la cual lleva por nombre "Security Considerations in the Information System Development Life Cycle". Esta guía presenta un marco para incorporar la seguridad en todas las fases del proceso de CVDS. Este documento es una guía para ayudar a seleccionar y adquirir los controles de seguridad explicando la forma de incluir requisitos de información del sistema de seguridad en las fases adecuadas del SDLC.

Para el NIST, un CVDS seguro de un SI incluye las siguientes fases: iniciación, adquisición/desarrollo, implementación, operación/mantenimiento, y disposición. Cada una de estas cinco fases incluye un conjunto mínimo de medidas de seguridad necesarias para integrar de manera eficaz la seguridad en un sistema durante su desarrollo. NIST recomienda que las organizaciones incorporen medidas de seguridad de TI asociados de esta SDLC general en sus procesos de desarrollo. En la fase de iniciación se consideran las tareas de categorización de seguridad y una evaluación preliminar del riesgo. Durante la fase de adquisición y desarrollo se consideran las tareas de evaluación del riesgo, análisis de requerimientos funcionales de seguridad, análisis de requerimientos de aseguramiento, consideraciones de costo y presentación de informes, planificación de seguridad, control de seguridad para el desarrollo, desarrollo de controles de seguridad, pruebas de seguridad del desarrollo y evaluación, y finalmente, la consideración de otros componentes de planificación. Durante la fase de implementación se consideran tareas de inspección y aceptación, integración de controles de seguridad, certificación y acreditación de la seguridad. Durante la fase de operación y mantenimiento se consideran las tareas de control y administración de la configuración y vigilancia continua. Durante la fase de disposición se consideran las tareas de preservación de la información, media sanitización, eliminación de Hardware y Software.

V. Metodología de Auditoria de Seguridad de SI.

Es importante realizar una revisión de la seguridad de las aplicaciones antes de puesta en producción que permita identificar las amenazas a las que la aplicación se encuentra expuesta y que a su vez permita hacer las recomendaciones necesarias al equipo de desarrollo para eliminar las deficiencias encontradas en la aplicación auditada.

Auditoria de Seguridad.

Se refiere a aquellos trabajos de análisis, revisión, evaluación y propuesta de perfeccionamiento de los SI, de forma tal que se contribuya a que su uso apoye las funciones para los que fueron creados. Una auditoria de seguridad da una visión exacta del nivel de exposición de sus SI. Los objetivos de una auditoría de seguridad de los SI son: revisar la seguridad de los entornos y sistemas, verificar el cumplimiento de las normas y legislación vigentes, elaborar un informe independiente, utilización de estándares y mejores prácticas.

En una auditoría de seguridad se verifica la seguridad en la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad de la información tratada por los sistemas. Una auditoria de seguridad debe seguir como mínimo las siguientes etapas:

- Planeación de la auditoría. Actividades del estudio preliminar del SI, misión, objetivos, funciones y características de desempeño. Así como la definición de objetivos, alcance y criterios de la auditoria. Los objetivos de la auditoría están directamente relacionados con la función del SI. Un SI no es un fin, es una herramienta de trabajo para apoyar las actividades de gestión, comunicación, negocios, etc. Por esa razón, los aspectos a evaluar en la auditoría de seguridad estarán alineados con los objetivos del SI.

- Organización de la auditoría. Actividades relativas a la definición de aspectos a investigar, asignación del equipo de trabajo, responsabilidades de cada uno, métodos y técnicas a emplear, definición de entregables y formatos de los mismos, etc.

- Ejecución o realización de la auditoría. Actividades de revisión documental y revisión funcional y de seguridad del SI, mediante diversos métodos, técnicas y herramientas de trabajo. La revisión documental determina la conformidad del SI con el marco normativo establecido en la planeación de la auditoria (institucional, sectorial, nacional, internacional, etc.)

- Una revisión funcional. Tiene como objetivo validar que el SI realiza funcionalmente aquello para lo que fue diseñado. Esta revisión busca encontrar deficiencias funcionales, las cuales están ligadas al negocio, por lo que no están previamente categorizadas.

- Una revisión de seguridad. Tiene como objetivo encontrar el mayor número de vulnerabilidades en el SI auditado.

- Elaboración y presentación del informe auditoria. Debe incluir un breve resumen de las deficiencias encontradas en el SI evaluado, el grado de certeza de

la seguridad del SI, las recomendaciones de la auditoria de seguridad y finalmente la conclusión de la auditoria. Este informe debe presentarse tanto a dueños, como al equipo desarrollador del SI. Es conveniente acordar fechas y tiempos para dar seguimiento de la corrección de las deficiencias encontradas.

- Plan de Mejora. Incluye el diseño e implementación de las recomendaciones propuestas para subsanar las incidencias de seguridad encontradas y mantener en el futuro una situación estable y segura de los SI.

- Seguimiento. La adopción de medidas correctivas, preventivas y de mejora por parte del auditado no es parte de la auditoria. La verificación de la implementación de las recomendaciones resultantes de la evaluación, es parte de una auditoria posterior.

Detalle de los aspectos a evaluar en una auditoría de Seguridad.

No existe como tal, una lista de los aspectos a considerar en una auditoria de seguridad. Conforme a las actividades que se debe seguir en un CVDS se proponen los siguientes: revisión de mecanismos de autorización y autenticación, revisión de mensajes de error y advertencia , revisión de mecanismos de protección de datos, revisión de casos de pruebas unitarias utilizados en la etapa de desarrollo y pruebas de integración en la etapa de pruebas, utilización de normas de codificación y pruebas, revisiones del código, exploración del código con herramientas especializadas, validar la estabilidad de la aplicación con escenarios no planificados, valores fuera de rango, formatos de entrada incorrectos, valores de entrada nulos, entradas y comportamiento no esperados, validar las tareas de transición de un ambiente a otro, validar el cambio de usuarios y contraseñas iniciales o por defecto cuando se pasa a entorno productivo, borrado de datos de prueba en ambientes productivos y validación de permisos de acceso adecuados en ambiente productivo.

En el mismo sentido, se sugiere revisar las listas de deficiencias de seguridad más comunes a nivel mundial. El sitio Web CWE1, publica anualmente una lista de los errores de programación más comunes que pueden conducir a graves deficiencias de software [8]. El último artículo presentado lleva por título '2010 CWE/SANS Top 25 Most Dangerous Programming Errors'. Esta lista presentan las descripciones detalladas de los 25 principales errores de programación, junto con una guía autorizada para mitigarlos y evitarlos. Adicionalmente, el sitio también contiene información sobre más de 800 errores de programación adicionales, errores de diseño, arquitectura y los errores que pueden llevar a vulnerabilidades explotables. Esta lista es una herramienta para la educación y sensibilización que apoya a los programadores a prevenir los tipos de vulnerabilidades que afectan a la industria del software.

[1] http://cwe.mitre.org/

VI. Conclusiones

Las aplicaciones se han convertido en el blanco preferido por los atacantes, es responsabilidad tanto de propietarios, desarrolladores y especialistas de seguridad, procurar y promover acciones dentro de los procesos organizacionales que permitan reducir el número de deficiencias en las aplicaciones desarrolladas dentro de la organización. Hablando solamente de la seguridad en las aplicaciones, se tienen 2 opciones para dotar a las aplicaciones de seguridad, la primera integrando la seguridad como una característica de todo el ciclo de desarrollo de software, lo que conlleva a un cambio en la forma e ideología del trabajo de las organizaciones y la segunda, llevando una revisión de seguridad exhaustiva de las aplicaciones desarrolladas con la intención de encontrar el mayor número de vulnerabilidades para posteriormente hacer las sugerencias necesarias al equipo de trabajo de desarrollo para eliminar las vulnerabilidades encontradas.

Si bien parece más fácil optar por un modelo de auditoria de seguridad para garantizar cierto grado de seguridad en las aplicaciones, en realidad no lo es. El no cambiar la forma en que los equipos de desarrollo y departamentos asociados trabajan, a la larga trae consigo un mayor gasto en recursos, esfuerzo y tiempo, ya que la mayoría de las veces las deficiencias encontradas resultan de un mismo origen, el desconocimiento de las implicaciones de seguridad por parte de los equipos de trabajo.

Sin duda alguna, la mejor opción para dotar seguridad a los SI es mediante la adopción de una metodología de CVDS Seguro, de tal manera que el aspecto de seguridad sea visto como parte integral del ciclo de vida de desarrollo y no solo como parte final del proceso de desarrollo. Desgraciadamente, este cambio no se logra de un día para otro, se lleva a cabo de manera gradual, la mayoría de las organizaciones aún no cuentan con la madurez necesaria para adoptar el uso de una metodología de CVDS Seguro, aún se requiere mucho tiempo, recursos, esfuerzo, trabajo de concientización y capacitación por parte de las organizaciones para lograr el cambio en la manera de analizar, diseñar, desarrollar y probar los SI. Pasará todavía algún tiempo para que las organizaciones integren totalmente el CVDS Seguro en sus procesos de desarrollo de SI, mientras tanto el uso de una metodología de auditoria de seguridad de SI seguirá siendo una buena opción.

A pesar de la aplicación del CVDS Seguro durante el desarrollo o una auditoria de seguridad, las prácticas de desarrollo más avanzadas no consideran que se pueda tener una aplicación libre de vulnerabilidad de seguridad. Incluso aunque el proceso de desarrollo pudiera eliminar todas las deficiencias de seguridad, se descubrirían nuevos ataques y el software considerado "seguro" pasaría a ser vulnerable. Por tanto, los equipos de desarrollo, de auditoria y de seguridad deben prepararse y estar en continua actualización para hacer frente a las nuevas amenazas que atenten a las aplicaciones.

RECONOCIMIENTOS

Se agradece a la Comisión Nacional de Ciencia y Tecnología CONACYT y al Instituto Politécnico Nacional IPN por el apoyo brindado.

Azucena Santiago López, no. de registro CVU 300949, Maestría en Ingeniería en Seguridad y Tecnologías de Información.

REFERENCIAS

1. **Pérez Martín**, Inversiones en TI, http://sociedaddelainformacion.wordpress.com/2010/01/22/la-inversion-en-tecnologias-de-la-informacion-crecera-un-46-por-ciento-en-2010-en-el-mundo/, Fecha de consulta: 2 de Febrero de 2010.
2. **Morrie Gasser.** Building a Secure Computer System. Editorial Van Nostrand Reinhold. EUA, 1988.
3. **SANS,** Vulnerabilidades de las aplicaciones, http://www.sans.org/top-cyber-security-risks/trends.php. Fecha de consulta: Noviembre 2009.
4. **Joseph Feiman**, Building Secure Applications. Gartner.
5. **Tim Grance**, Joan Hash, Marc Stevens, NIST , Security Considerations in the Information System Development Life Cycle. EUA, Octubre 2003.
6. **Microsoft**, Security Development Lifecycle, http://www.microsoft.com/security/sdl/default.aspx. Fecha de consulta: Septiembre 2010.
7. **Gary Locke, Patrick D. Gallagher**, "Security Considerations in the Information System Development Life Cycle". NIST. EUA, Febrero 2010
8. **CWE**, Vulnerabilidades de los SI, http://cwe.mitre.org/top25/#Brief, Fecha de consulta: Agosto 2010.

Metodología de Evaluación de la Seguridad de Sitios Web

[1]M. Rodríguez-Argueta, [1]A. Santiago-López, [1]M.A. Morales-Santos, [2]L.O. Pérez-González, [1]R. Vázquez-Medina.

[1]IPN SEPI ESIME CULHUACAN, Av. Santa Ana No. 1000 Col Culhuacan, México D.F. C.P. 04430
e-mail: {mrodriguezh0905, asantiagol0800, mmoraless0401, ruvazquez}@ipn.mx

[2]SECRETARÍA DE LA FUNCIÓN PÚBLICA, Insurgentes Sur 1735 Col. Guadalupe Inn México D.F. C.P 01020
email: choscar69@hotmail.com

RESUMEN. En este artículo se toman en cuenta las estadísticas y los informes sobre los ataques más peligrosos a los servicios Web para evaluar la seguridad de Sitios Web de un dominio objetivo. Se usa como referencia la norma **ISO 2859-1:1999** "Procedimientos de muestreo para inspección por atributos", la norma mexicana **NMX-Z-012-1-1987** "Muestro para la Inspección por Atributos" y la norma de la Defensa de los Estados Unidos **MIL-STD-1916** "Métodos para aceptación de Producto". Adicionalmente, se realiza un estudio sobre las cualidades o atributos de seguridad que deberían tener los sitios Web para considerarse aceptablemente seguros. Este estudio determina cuáles son los factores que se presentan en los servicios Web para que las vulnerabilidades del tipo de inyección de código (Cross-Site Scripting, SQL Injection, XML Injection, etc.) sean explotadas. Así mismo, una vez que estos factores se han detectado, se realiza una recomendación de mitigación de riesgos de acuerdo a recomendaciones tales como las de NIST SP 800-42 y NIST SP 800-95. Los resultados muestran que el universo o lote completo de los más de 5000 sitios Web que se encuentran en un subdominio de objetivo es rechazado debido a una seguridad deficiente en la muestra considerada. Finalmente, haciendo uso de herramientas de código libre, diseñadas como laboratorios de lecciones de seguridad de aplicaciones Web, se pudieron determinar los precursores e indicadores de los ataques a las servicios Web, de acuerdo con lo que se especifica en la recomendación NIST SP 800-61, con lo que es posible determinar cuál es la evidencia factual de dichos ataques.

Palabras Claves. Dominio, Evaluación, Metodología, Seguridad, Webservices.

WebSites Security Assessment Methodology

ABSTRACT. In this paper, statistics and rankings about the most dangerous attacks over the Web services are covered, to assess the National Websites Security of a target domain. It is used as a reference the ISO2859-1:1999 regulation "Sampling procedures for inspection by Attributes", the NMX-Z-012-1987 Mexican regulation "Sampling procedures for inspection by Attributes" and the MIL-STD-1916 United States Defense regulation "Preferred Methods for Acceptance of Product". In addition, a study on the security attributes that should have the websites to consider them acceptably secure is made. This study determines which the factors are that are present in the Web services to the code injection vulnerabilities (Cross-Site Scripting, SQL Injection, XML Injection) were exploited. Therefore, once that these factors have been detected, a risk mitigation is made regarding to the NIST SP 800-42 y NIST SP 800-95 recommendations. The results show that the set of the more than 5000 Websites that are in the target domain is rejected due to an inefficient security on the tested sample. Finally, using free code tools, designed to specifically teach web application security lessons, the precursors and indicators of the web services attacks could be determined, regarding to the NIST SP 800-61 recommendation, and that's a support to determine the factual evidence of such attacks.

Key words: Domain, Assessment, Methodology, Security, Web services

I. INTRODUCCIÓN

Los servidores y aplicaciones Web tienen una gran probabilidad de ser comprometidos, debido a que están públicamente disponibles en Internet, especialmente aquellos que están asociados con sitios gubernamentales. Dada esta condición, es necesario contar con un indicador que constituya una herramienta útil para establecer los parámetros objetivos sobre el nivel de seguridad que guardan los sitios Web. Para ello, se toma una muestra representativa del dominio analizado.

Se realizan pruebas y se obtienen resultados que permitan tomar medidas correctivas o preventivas a fin de reaccionar rápidamente ante un incidente de seguridad.

II. Situación Actual de los Ataques a Servicios Web

Ataques Comunes contra Servicios Web

Debido a los constantes cambios en la naturaleza de las amenazas y vulnerabilidades de las aplicaciones Web organizaciones como el OWASP (Open Web Application Security Proyect) [1] presenta informes anuales sobre riesgos críticos en las aplicaciones Web. En dicho informe destacan los ataques de inyección de comandos. A continuación se mencionan los ataques más peligrosos, según el informe del OWASP:

Inyección. Ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o una consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceder a datos no autorizados.

Cross-Site Scripting (XSS). Ocurren cuando una aplicación toma datos no confiables y los envía al navegador Web sin una validación o escape de caracteres apropiado. El XSS permite a un atacante ejecutar scripts en el navegador de la víctima, lo que puede llevar al robo de sesiones de usuario, desfigurar la presentación del sitio o redireccionar al usuario a sitios maliciosos.

Pérdida de autenticación y administración de sesiones. Las credenciales de cuentas y los testigos de sesión (session token) frecuentemente no son protegidos. Los atacantes obtienen contraseñas, claves, o testigos de sesión para obtener identidades de otros usuarios.

Referencia insegura y directa a objetos ("direct object reference"). Ocurre cuando un programador expone una referencia hacia un objeto interno de la aplicación, tales como un archivo, directorio, registro de base de datos, o una clave tal como una URL o un parámetro de formulario Web. Un atacante podría manipular este tipo de referencias en la aplicación para acceder a otros objetos sin autorización.

Falsificación de Petición en Sitios Cruzados (CSRF: Cross Site Request Forgery). Un ataque CSRF fuerza al navegador validado de una víctima a enviar una petición a una aplicación Web vulnerable, la cual entonces realiza la acción elegida por el atacante a través de la víctima. CSRF puede ser tan poderosa como la aplicación siendo atacada.

Mala configuración de seguridad. Una buena seguridad requiere tener una configuración segura definida y desplegada en la aplicación, el servidor de aplicaciones, servidor Web y servidor de base de datos. Todos estos valores deben ser definidos, implementados y mantenidos ya que en la mayoría de los casos, los valores por defecto no son los más seguros. Esto incluye mantener todo el software actualizado, incluyendo las librerías de código utilizadas por la aplicación.

Almacenamiento Criptográfico Inseguro. Las aplicaciones Web no utilizan de funciones criptográficas de manera adecuada para proteger datos y credenciales. Los atacantes usan datos débilmente protegidos para llevar a cabo robos de identidad y otros crímenes, tales como fraude de tarjetas de crédito.

Falla de restricción de acceso a URL. Frecuentemente, una aplicación solo protege funcionalidades delicadas previniendo la visualización de enlaces o URLs a usuarios no autorizados. Los atacantes utilizan esta debilidad para acceder y llevar a cabo operaciones no autorizadas accediendo a esas URLs directamente.

Protección insuficiente en capa de transporte. Las aplicaciones fallan frecuentemente al autenticar, cifrar y proteger la confidencialidad e integridad de tráfico de red de datos sensibles.

Redirecciones no validados. Las aplicaciones Web frecuentemente redireccionan a los usuarios a otras páginas y sitios Web, y utilizan datos no confiables para determinar las páginas destino. Sin una validación adecuada, un atacante puede redireccionar a las víctimas a sitios de phishing o malware, o utilizar redireccionamiento para acceder a páginas no autorizadas.

Por la amplia variedad de posibilidades existentes, se hace necesario saber si la seguridad de los servicios web del dominio analizado puede verse comprometida, se hace presente.

III. Metodología Propuesta

Con base en las recomendaciones de organizaciones internacionales como el NIST, OWASP, SANS, entre otros, se propone la siguiente metodología para la intrusión ética a servidores web y evaluación de sus aplicaciones. Cabe mencionar que no se tomó como referencia ninguna institución o documento nacional debido a que no existe un organismo en México como tal que se dedique al desarrollo de normas o técnicas en esta materia.

1. **Determinación del Tamaño del Universo de Unidades a Analizar.** Es frecuente encontrarse con redes compuestas por una gran cantidad de equipos que guardan diversos servicios. Si el número de estos equipos es demasiado grande como para realizar el análisis correspondiente para cada uno, entonces es aconsejable la utilización de un método de muestreo.

2. **Selección de la Muestra Representativa**. Si se ha optado por un método de muestreo, se recomienda que el uso del nivel de verificación y el procedimiento a utilizar sean normales, si es que se va a realizar una selección por primera vez. Si se va a realizar alguna corrección y se vuelve a utilizar un método de muestreo, entonces los parámetros deben cambiar a un nivel reducido o riguroso, según sea el caso.

3. **Determinación del Tipo de Incidente.** Es importante conocer el tipo de precursores e indicadores [2] a las que están expuestas las aplicaciones de la organización; de esta manera se pueden desarrollar técnicas sobre como detectar potenciales ataques futuros y ataques que se estén efectuando o se hayan efectuado por medio de herramientas de monitoreo y exploración de archivos bitácoras. Los tipos de incidentes considerados son: a) Denegación del Servicio, b) Código malicioso, c) Acceso no autorizado y d) Uso inapropiado.

4. **Preparación para la Evaluación.** Preparar herramientas, permisos y aprobaciones administrativas y técnicas [3]. Se debe preparar el laboratorio desde el cual se realizarán las actividades de intrusión; seleccionando y precisando las herramientas para el análisis y explotación de vulnerabilidades. Este ambiente de laboratorio deberá garantizar información confiable y útil para la elaboración de los informes. Adicionalmente en esta etapa se hace necesario contar con la autorización y visto bueno de la alta dirección, quien deberá tener pleno conocimiento de las actividades que se van realizar.

5. **Realización de Pruebas de Seguridad.** La utilización de las herramientas seleccionadas, que siendo especializadas, permitan descubrir vulnerabilidades y servicios abiertos en las aplicaciones Web, así como en los servidores donde viven dichas aplicaciones. En esta etapa también se aplicarán las herramientas (exploits) que validan la existencia de las vulnerabilidades.

6. **Análisis de Resultados de Pruebas de Seguridad.** A través de la utilización de las herramientas es posible localizar los huecos de seguridad que un atacante explotaría para tener acceso a las aplicaciones. Una vez identificados dichos puntos es posible crear medidas correctivas para reducir el riesgo de alguna intrusión no autorizada. En esta etapa se validan los falsos positivos y los falsos negativos.

7. **Presentación de Informes.** Una vez analizados los resultados, se debe documentar los hallazgos encontrados del estudio. El informe debe ser claro, para todas las partes involucradas, al destacar la función exacta que ha sido afectada por la vulnerabilidad con las asociadas recomendaciones para su solución en un lenguaje entendible y sencillo [4]. Así mismo, pero no menos importante, la redacción del reporte no debe ser agobiante para los verificadores de seguridad.

8. **Recomendaciones de Seguridad.** Por último, se dan sugerencias con respecto a las posibles correcciones y acciones de mitigación a las fallas de seguridad encontrados.

IV. CASO DE APLICACIÓN

Muestra Representativa

Con base en la norma internacional ISO 2859-1:1999, a la norma Mexicana NMX-Z-012-1987 y a la norma americana de defensa MIL-STD-1916, fue posible realizar un estudio utilizando un plan de muestreo por atributos de un lote (los más de 5000 sitios Web), cuyas condiciones son que todo el lote consista en una característica única, que se determine un nivel de verificación (importancia subjetiva del lote) y que se determine el tipo de procedimiento del estudio (normal, riguroso o reducido).

Así pues, se proponen las condiciones iniciales mencionadas como sigue:

- Plan de muestreo preferido: **Por atributos**.
- Identificación del lote: **Perteneciente al dominio objetivo.**
- Nivel de Verificación (Importancia): **Normal (IV).**
- Procedimiento: **Normal (II).**

Cabe señalar que las normas recomiendan que al iniciar un muestreo por atributos se realice utilizando los parámetros normales. De esta manera, con ayuda de la Tabla 1 obtenida del estándar MIL-STD-1916, se observa que dado el número de unidades (sitios web) del lote (dominio objetivo), y el nivel de verificación Normal (IV), la letra seleccionada es la **D.**

Lot or production interval size	Verification levels						
	VIII	VII	V	IV	III	II	I
2–170	A	A	A	A	A	A	A
171–280	A	A	A	A	A	A	B
281–500	A	A	A	A	A	B	C
501–960	A	A	A	A	B	C	D
961–1632	A	A	A	B	C	D	E
1633–3072	A	A	B	C	D	E	E
3073–5440	A	B	C	D	E	E	E
5441–9216	B	C	D	E	E	E	E
9217–17408	C	D	E	E	E	E	E
17409–30720	D	E	E	E	E	E	E
30721 and larger	E	E	E	E	E	E	E

Tabla 1. Código de letras para uso de tablas de muestreo

Enseguida se consulta la Tabla 2, para determinar el tamaño de la muestra representativa del lote. El nivel de verificación normal que se toma es el II, debido a que solo es necesaria una pequeña muestra del lote para realizar el estudio, según el criterio establecido. Ahora se sabe que el tamaño de unidades a seleccionar de manera aleatoria de la muestra representativa es 24.

Code letter	Verification levels								
	T	VIII	VII	V	IV	III	II	I	R
	Sample size (n_q)								
A	3072	1280	512	192	80	32	12	5	3
B	4096	1536	640	256	96	40	16	6	3
C	6150	2048	768	320	128	48	20	8	3
D	8144	2560	1024	384	160	64	24	10	4
E	8192	3072	1280	512	192	80	32	12	5

NOTES:

(1) When the lot size is less than or equal to the sample size, 100 percent attributes inspection is required.

(2) One verification level (V_L) to the left/right of the specified normal V_L is the respective tightened/reduced plan. Tightened inspection of V_L+1 is T, reduced inspection of V_L-1 is R.

Tabla 2. Código de letras para uso de tablas de muestreo

Conformación de la Muestra

Partiendo de un inventario reciente de sitios Web que presentan o presentaron problemas relacionados con XSS o SQL Injection, se escogen aleatoriamente 24 sitios para realizarles pruebas de seguridad por medio de herramientas de software libre. Dichas pruebas consisten en encontrar vulnerabilidades y clasificarlas de acuerdo a su nivel de severidad según se describa en el CWE (Common Weakness Enumeration). Este nivel de severidad va desde el nivel "Bajo" hasta el "Alto", tomado en cuenta factores como el tipo de ataque, el tipo de plataformas que afecta el ataque, las consecuencias comunes de un ataque exitoso (consecuencias a la confidencialidad, integridad y disponibilidad) y la posibilidad de explotación.

Criterio de Aceptación

El requisito de aceptación que se propone para considerar el lote como aceptablemente seguro, es que de la muestra representativa, al menos uno de ellos presente un nivel de severidad alto. Si llegara a ocurrir esta condición de incumplimiento del requisito especificado (no conformidad), entonces el lote se considera rechazado, o en este caso, se determina que dicho lote es de una calidad insegura. Por lo tanto, se debe de llevar a cabo una acción correctiva y generar nuevamente un muestreo por atributos, utilizando un cambio de procedimiento que vaya del procedimiento normal al procedimiento riguroso.

Eventos e Incidentes

Un evento es una ocurrencia observable en un sistema o red. Los eventos incluyen a un usuario conectándose a un recurso compartido o un servidor recibiendo una petición a una página Web. Los eventos adversos son eventos con consecuencias negativas, tal como un sistema colapsado, uso no autorizado de privilegios, etc. Actualmente, un incidente de seguridad puede pensarse como una violación o una inminente amenaza de violación de las políticas y normas de seguridad informática. Ejemplos de incidentes actuales son: a) Denegación de Servicio, b) Código Malicioso, c) Acceso NO autorizado, y d) Uso Inapropiado.

De esta manera, se puede identificar el tipo de incidente al que pertenece un ataque a los servicios Web. Para este caso dichos incidentes caen en las categorías de Código Malicioso y Acceso NO autorizado.

Precursores e Indicadores

Los signos de un incidente caen en dos categorías: indicadores y precursores. Un precursor es un signo de que un incidente puede ocurrir en el futuro. Un indicador es un signo de que un incidente pudo haber ocurrido o esté ocurriendo. La Tabla 3 menciona los precursores que aplican para los tipos de incidentes arriba mencionados, sobre las vulnerabilidades de inyección de comandos (XSS, Inyección SQL)

Precursor	Respuesta
Los accesos NO autorizados están precedidos por una actividad de reconocimiento para contrastar hosts y servicios y para identificar vulnerabilidades. Esta actividad puede incluir escaneo de puertos, escaneo de equipos, escaneo de vulnerabilidades, pings, traceroutes, transferencias de zonas, identificación de sistemas operativos, identificación de versión de servidor web. Tal actividad se detecta inicialmente por IDS 's, después por un análisis de bitácoras.	Se debe de buscar distintos patrones de reconocimiento, por ejemplo, un repentino interés por conocer los puertos abiertos, por conocer la versión del servidor web o por saber sobre que plataforma esta realizado el servicio web de la organización.
Un nuevo exploit sobre la plataforma de trabajo sobre la cual esta hecha el servicio Web, está publicado libremente, lo cual es una amenaza significativa para la organización.	La organización debe de investigar el nuevo exploit y si es posible modificar los controles de seguridad para minimizar el impacto potencial del exploit en la organización.
Reportes de intentos de ingeniera social como correos electrónicos para hacer que los usuarios visiten sitios no confiables y revelen información sensible.	El propósito de la actividad se tiene que determinar y verificar el estado de los controles de seguridad.

Tabla 3. Precursores para vulnerabilidades de inyección de comandos.

Así también, la Tabla 4 menciona los indicadores que aplican sobre las vulnerabilidades de inyección de comandos (XSS, Inyección SQL).

Acción Maliciosa	Indicador
Modificación NO autorizada de datos (Defacement a un sitio Web)	•Alertas de red sobre detección de intrusos •Incremento del uso de los recursos •Reportes de modificación de datos (defacement) •Modificación de archivos críticos •Directorios o archivos nuevos con nombres inusuales. •Cambios significativos en el uso de los recursos.
Uso NO autorizado de una cuenta de usuario	•Acceso a archivos críticos. •Uso inexplicable de una cuenta (cuenta reservada en uso, cuenta en uso desde multiples lugares, comandos que son inesperados de un usuario particular. •Bitácoras de un proxy indicando la descarga de herramientas de hackeo.
Acceso NO autorizado a datos	Alertas de detección de Intrusos de intentos de obtención de acceso a través de protocolos FTP, HTTP, etc.

Tabla 4. Indicadores para vulnerabilidades de inyección de comandos.

V. Resultados y Discusiones

Los resultados obtenidos de acuerdo a los criterios que se establecieron para conformar la muestra a ser evaluada son los que se presentan en la Tabla 5.

*Severidad	APF	Estados	Municipios
Alta	5	6	5
Media	1	-	-
Baja	6	-	1

Tabla 5. Numero de Sitios Web catalogados por severidad

Se observa que del total de sitios Web de la muestra, 16 de estos tienen un nivel de severidad alto, 1 medio y 7 un nivel de severidad bajo. Así también, se encontró información sobre las deficiencias que están presentes en la muestra representativa (ver tabla 6).

Las deficiencias encontradas, efectivamente son las más comunes, según lo mencionado en el estudio de OWASP. Se observa también que 11 de los 24 sitios Web son susceptibles a ataques de Cross-Site Scripting, 7 de ellos son vulnerables a ataques de inyección de SQL y 2 más son susceptibles a ataques de XPath (Las tres corresponden a la categoría de inyección de comandos). También se observa que los 24 sitios Web tienen una deficiencia de enlaces rotos, lo cual no es de severidad alta. Sin embargo, esto puede indicar que no existe un adecuado mantenimiento a los servicios Web por parte de los propietarios en el momento de realizar una actualización de dichos servicios. La Tabla 7 muestra el tipo de servidores Web que son utilizados en la muestra representativa.

Vulnerabilidades encontradas	Número de sitios Web con estas vulnerabilidades
Cross Site Scripting (XSS)	11
SQL Injection	7
Blind SQL / Xpath Injection	2
Broken links	24
Password type input with autocomplete enabled	12
TRACE Method Enabled	10
Application error message	9
User credentials are sent in clear text	6
Files listed in robots.txt but not linked	3
Possible sensitive directories	3
Backup files	1
File inputs accepted	1
Directories with write permissions enabled	1
Source code disclosure	1
URL redirection	1

Tabla 6. Número de vulnerabilidades encontradas

Tipos de servidores Web	Servidores con esta versión
Sun GlassFish Enterprise Server v2.1.1	1
Apache	4
Microsoft-IIS/7.0	1
Apache/2.2.13 (Unix) PHP/5.2.11	1
Apache Tomcat/4.0.6 HTTP/1.1 Connector	1
Apache/2.0.59 (Unix) PHP/5.2.1	1
Apache/2.2.6 Fedora	1
Apache/2.2.3 CentOS	1
Microsoft-IIS/6.0	5
IBM HTTP Server/6.0.2.31 Apache/2.0.47 Unix	1
Apache/2.2.0 Fedora	1
Apache/2.2.9 Debian PHP/5.2.13-0.dotdeb.0 with Suhosin-Patch	1
Apache/2.2.8 Linux/SUSE	1
Apache/1.3.20 Sun Cobalt Unix	1
Apache/2	3

Tabla 7. Tipo de servidores Web

Se observa que existe una clara preferencia sobre servidores web de código libre.

Factores Explotables de las Aplicaciones Web

Como se ha observado, las deficiencias de Inyección de Comandos son el resultado de errores de programación por parte de los desarrolladores de las aplicaciones. Estas deficiencias son en sí mismas peligrosas debido a que son fáciles de encontrar, fáciles de explotar, permiten a los atacantes tomar control de la aplicación, robar información o impedir que la aplicación se utilice de una manera adecuada y normal [5].

VI. Recomendaciones de Mitigación

Las siguientes contramedidas se dividen entre recomendaciones para usuario y recomendaciones para desarrolladores y han sido planteadas de acuerdo a las recomendaciones del NIST SP 800-42 (Guidelines on Securing Public Web Servers), y NIST SP 800-95 (Guide to Secure Web Services).

Para los usuarios, ya que las vulnerabilidades de XSS y SQL Inyection son ampliamente difundidas, se recomienda seguir las siguientes acciones:

i. Cerrar la sesión inmediatamente después de utilizar una aplicación web.
ii. No permitir al navegador guardar el usuario/contraseñas, y no permitir a los websites recordar tu información de login.
iii. No utilizar el mismo navegador para acceder a aplicaciones web sensibles que para navegar libremente por Internet. Si tiene que hacer las dos cosas en la misma máquina, hágalo con navegadores diferentes.

Con respecto a los desarrolladores, estos deben validar lo siguiente respecto a las peticiones y respuestas:

Peticiones

i. Identificar dónde se utilizan las peticiones GET y dónde las POST.
ii. Identificar todos los parámetros utilizados en la petición POST (se encuentran en el cuerpo de la petición)
iii. Para el caso de peticiones POST, se debe prestar especial atención a cualquier parámetro oculto. Cuando se envía una petición POST, también se envían a la aplicación todos los campos de formulario (incluyendo los parámetros ocultos) en el cuerpo del mensaje HTTP. Generalmente no es posible acceder a ellos a no ser que sea utilizando un proxy o viendo el código fuente HTML. Además, la siguiente página a la que se accede, al igual que su contenido o tipo de acceso puede ser diferente dependiendo del valor de los parámetros ocultos.
iv. Identificar todos los parámetros utilizados en la petición GET (por ejemplo, la URL), sobretodo en forma de cadenas (generalmente aparecen después de un símbolo de "?").
v. Identificar todos los parámetros de la cadena, generalmente aparecen como pares de valores. Por ejemplo, foo=bar. También se debe destacar que muchos parámetros pueden aparecer en una petición. Por ejemplo, separados por un &, o cualquier otro carácter especial o codificado.
vi. Destacar el saber diferenciar, cuando se identifican múltiples parámetros en una cadena o dentro de una petición POST, si son necesarios algunos o todos los parámetros para llevar a cabo el análisis. Es necesario obtener todos los parámetros (incluso estando codificados o cifrados) e identificar cuáles de ellos son procesados por la aplicación.
vii. También prestar atención a cualquier cabecera adicional o personalizada que no sean comunes (como por ejemplo debug=false).

Respuestas

i. Identificar dónde se establecen nuevas cookies (mediante la cabecera Set-Cookie), o dónde se modifican o se añaden.
ii. Identificar dónde existen redirecciones (con código HTTP 300), códigos HTTP de tipo 400, por ejemplo el de prohibición, 403 Forbidden, o errores internos durante peticiones normales, como son los 500 (por ejemplo, peticiones no modificadas)
iii. También comprobar dónde se utilizan ciertas cabeceras. Por ejemplo, la cabecera "Server: BIG-IP" indica que el sitio se encuentra balanceado. Por lo tanto, si un sitio se encuentra balanceado y un servidor está configurado incorrectamente, entonces quizás deban realizarse múltiples peticiones para acceder al servidor vulnerable, dependiendo del tipo de balanceador de carga que se esté utilizando.

Adicionalmente, obtención de la firma digital de un servidor web es una tarea esencial para la persona que realiza una prueba de intrusión. Saber el tipo y versión del servidor en ejecución le permite determinar vulnerabilidades conocidas, y los programas (exploits) de explotación de vulnerabilidades apropiados a usar durante la prueba.

VII. Conclusiones

La naturaleza de los ataques informáticos se caracteriza por una rápida y constante evolución. Es por ello que es necesario que los desarrolladores de las aplicaciones Web, se familiaricen con la seguridad y apliquen medidas preventivas para evitar que un atacante o incluso un usuario dentro de la organización obtenga información sensible aprovechando las deficiencias de seguridad.

En este artículo se planteó la utilización de una metodología que relaciona la forma de evaluar la calidad de los productos de un lote a partir de una muestra representativa y adecuarla a las necesidades de la seguridad informática para sentar un precedente sobre la condición que guardan los servicios Web dentro de un dominio objetivo, el cual constituye el lote observable como un lote de producción fabril.

De acuerdo a los resultados obtenidos, se concluye lo siguiente: "El universo de los más de 5000 sitios Web que se encuentran en el dominio objetivo se rechaza, lo que significa que su seguridad es deficiente, de acuerdo con los resultados obtenidos en la muestra considerada". Esta seguridad deficiente es el producto de una mala o nula evaluación de las aplicaciones por parte de los desarrolladores de software, especialistas de seguridad y verificadores de la funcionalidad (software testers) antes de que estos operen en un ambiente productivo.

Es importante que los dueños de las aplicaciones y desarrolladores tomen conciencia de la importancia de las aplicaciones web, ya que muchas de ellas están expuestas públicamente en la internet; que al ser inseguras, podrían poner en riesgo a la organización o a las personas que en ella laboran.

La muestra evaluada sugiere que es necesario un trabajo intenso que contribuya a mejorar la seguridad de los sitios web del dominio objetivo. Este trabajo debe considerar un plan de conciencia de seguridad para administradores y desarrolladores de tecnología.

Reconocimientos

Al IPN por el apoyo económico otorgado en el Programa Institucional de Formación de Investigadores con el Proyecto SIP-20102510.

Al CONACYT por el apoyo económico otorgado al primer autor como becario 300946.

Referencias

1. OWASP Top 10 – 2010: "The Ten Most Critical Web Application Security Risks".
2. NIST SP800-61 Computer Security Incident Handling Guide
3. NIST SP800-115 Technical Guide to Information Security Testing and Assessment
4. NIST SP800-95 Guide to Secure Web Services
5. OWASP Testing Guide v3

APENDICE I: REFERENCIAS

[1] Vázquez, Jesús. Junio 2008. "Inseguridad de los sistemas". ACIS, Bogotá, Colombia.

[2] Mandeep, Khera. Marzo 2010. "Web Application Security Trends Report Q3-Q4, 2009". Cenzic Inc.

[3] Pérez, Martín. "Inversiones en TI", http://sociedaddelainformacion.wordpress.com/2010/01/22/la-inversion-en-tecnologias-de-la-informacion-crecera-un-46-por-ciento-en-2010-en-el-mundo/, Fecha de consulta: 2 de Febrero de 2010.

[4] ITespresso, "Se aumentan los presupuestos para el desarrollo de aplicaciones", http://www.mundo-contact.com/enlinea_detalle.php?recordID=14242. Fecha de consulta: Noviembre de 2009

[5] Gasser, Morrie. 1988. "BUILDING A SECURE COMPUTER SYSTEM". Editorial Van Nostrand Reinhold. EUA.

[6] SANS, "Vulnerabilidades de las aplicaciones", http://www.sans.org/top-cyber-security-risks/trends.php, Fecha de consulta: Noviembre 2009.

[7] Fernández de Lara, Carlos. "Urge proteger aplicaciones Web", http://www.netmedia.info/security/urgen-a-proteger-aplicaciones-web. Fecha de consulta: Noviembre 2009.

[8] Mandeep Khera. Noviembre 2009. "Web Application Security Trends Report Q1-Q2, 2009". Cenzic Inc.

[9] Feiman, Joseph. "Building Secure Applications". Gartner.

[10]Sommerville, Ian. 2005. "Software Engineering". http://books.google.com.mx/books?id=gQWd49zSut4C&printsec=frontcover&hl=es#v=onepage&q&f=false. Fecha de consulta: Agosto 2010.

[11] Espinoza, Fernando. "20-SISTEMAS_INFORMACION_PRESENTACION", http://ing.utalca.cl/~fespinos/20-SISTEMAS_INFORMACION_PRESENTACION.pdf , Fecha de consulta: Agosto 2010.

[12] Gutiérrez, Carlos M. William Jeffrey. Marzo 2006. "FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems". NIST.

[13] Red Escolar Nacional de Venezuela, "Sistemas de Información", http://www.rena.edu.ve/cuartaEtapa/Informatica/Tema10.html, Fecha de consulta: Agosto 2010.

[14] Ciber Habitad, Ciudad de la Informática, INEGI, "Seguridad Informática", http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/seguridad/intro.htm, Fecha de consulta: Agosto 2010.

[15] Villarrubia Jiménez, Carlos. "Seguridad y Alta Disponibilidad". Universidad de Castilla-La Mancha.

[16] ISO/IEC, "Estándar ISO/IEC 27002, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información". Publicación 2007.

[17] CARO M.,COBA L. 2004. "Manual de procedimientos enfocados al sistema de gestión de calidad ISO 9001:2000 del área de control de calidad de laboratorios Pronabell Ltda", Tesis de grado. Microbiología industrial. Pontificia Universidad Javeriana. Bogotá.

[18] Peltier, Thomas R. "Informatión security and procedures ", Editorial Auerboon Pulications.

[19] Santes Galván, Lucio. "Propuesta de una metodología de análisis forense para dispositivos de telefonía celular". Tesis de grado. Microelectrónica. IPN, ESIME Culhuacan. México, DF.

[20] The Royal Pharmaceutical Society of Great Britain (RPSGB), "Developing and implementing standard operating procedures for dispensing", http://www.pharmacycouncil.org.nz/sops, Fecha de consulta: Enero 2010.

[21] MUÑOZ Razo, Carlos. "Auditoría de Sistemas computacionales". Editorial Pearson, Prentice Hall.

[22] SOBRINOS Sánchez, Roberto. "Planificación y Gestión de los Sistemas de Información". Universidad de Castilla – La Mancha.

[23] LOBOS Barrera, Evelyn. "AUDITORÍA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES". Tesis de grado. Ingeniería en Ciencias y Sistemas. Universidad de San Carlos de Guatemala.

[24] RODRIGUEZ Pérez, Antonio y Olga Lidia León Burguera. "La seguridad informática y el control interno en Cuba. Experiencias de la división Copextel Villa

Clara", http://www.gestiopolis.com/administracion-estrategia/seguridad-informatica-y-su-control.htm, Fecha de consulta: Agosto 2010.

[25] PIATTINI, Mario y Emilio del Peso. 2003. "Auditoría Informática, Un enfoque práctico". Editorial RA-MA.

[26] BSI, "Standard", http://www.bsieducation.org/Education/about/what-is-a-standard.shtml, Fecha de consulta: Agosto 2010.

[27] GONZALEZ Báez, Imelda. Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI), "Mejores Prácticas", http://www.amereiaf.org.mx/congresodeverano2009/material/miercoles_tecnologia.pdf, Fecha de consulta: Agosto 2010.

[28] RUIZ Francisco, Macario Polo. UPM, "Mantenimiento de Software", http://personales.unican.es/ruizfr/is2/doc/teo/1/is2-t01-apuntes_masterupm.pdf, Fecha de consulta: Agosto 2010.

[29] IT Governance Institute. COBIT 4.1. EUA, 2007.

[30] ISSA, "ISO/IEC 15408-Evaluation criteria for IT security", http://issaperu.org/?p=381, Fecha de consulta: Agosto 2010.

[31] LOCKE, Gary y Patrick D. Gallagher, "NIST SPECIAL PUBLICATION SP 800-53. Recommended Security Controlsfor Federal Information Systems and Organizations". Tercera Revisión. NIST. Enero 2010.

[32] HERZOG, Pete, "OSSTMM 2.1. Manual de Metodología abierta de testeo de seguridad". Versión 2.1. ISECOM. Agosto 2003.

[33] MEUCCI, Mateo. "Guía de Pruebas OWASP V. 3.0". OWASP. Noviembre 2008.

[34] VAN Veenendaal, Erik y Julie McMullan. "Achieving Software Product Quality", http://www.cse.dcu.ie/essiscope/sm2/9126ref.html, Fecha de consulta: Septiembre 2010.

[35] ABUD Figueroa, M. Antonieta. "Calidad en la Industria del Software. La Norma ISO"-9126", revista UPIICSA enero-marzo 2004, http://www.revistaupiicsa.20m.com/Emilia/RevEneAbr04/Antonieta1.pdf, Fecha de consulta: Septiembre 2010.

[36] SANDERS, Joc & Eugene Curran. "Software Quality. A Framework for Success in Software Development and Support", Editorial Addison Wesley.

[36-1] Universidad de Ginebra, "ISO 9126", http://www.issco.unige.ch/en/research/projects/ewg96/node13.html, Fecha de consulta: Enero 2010.

[37] MILANO, Pablo."Seguridad en el ciclo de vida de desarrollo de software", http://www.prensariotila.com/pdf/TutorialCybsec_0710.pdf, Fecha de consulta: Agosto 2010.

[38] Microsoft. "Simplified Implementation of the Microsoft SDL". Febrero 2010.

[39] GRANCE, Tim, Joan Hash y Marc Stevens. "NIST SPECIAL PUBLICATION SP 800-64. Security Considerations in the Information System Development Life Cycle". NIST. Octubre 2003.

[40] CWE/MITRE. "Vulnerabilidades de los SI", http://cwe.mitre.org/top25/#Brief, Fecha de consulta: Agosto 2010.

[41] ISO/IEC. "ISO/IEC 17799. Tecnología de la Información – Técnicas de seguridad- Código para la práctica de la gestión de la seguridad de la información". Segunda Edición. Junio 2006.

[42] Mozilla Inc., "MFSA 2010-74", http://www.mozilla.org/security/announce/2010/mfsa2010-74.html. Fecha de consulta= Enero 2011.

[43] Mozilla Inc., "MFSA 2010-75", http://www.mozilla.org/security/announce/2010/mfsa2010-75.html. Fecha de consulta= Enero 2011.

[44] Mozilla Inc., "MFSA 2010-76", http://www.mozilla.org/security/announce/2010/mfsa2010-76.html. Fecha de consulta= Enero 2011.

[45] Mozilla Inc., "MFSA 2010-77", http://www.mozilla.org/security/announce/2010/mfsa2010-77.html. Fecha de consulta= Enero 2011.

[46] Mozilla Inc., "MFSA 2010-78", http://www.mozilla.org/security/announce/2010/mfsa2010-78.html. Fecha de consulta= Enero 2011.

[47] Mozilla Inc., "MFSA 2010-79", http://www.mozilla.org/security/announce/2010/mfsa2010-79.html. Fecha de consulta= Enero 2011.

[48] Mozilla Inc., "MFSA 2010-80", http://www.mozilla.org/security/announce/2010/mfsa2010-80.html. Fecha de consulta= Enero 2011.

[49] Mozilla Inc., "MFSA 2010-81", http://www.mozilla.org/security/announce/2010/mfsa2010-81.html. Fecha de consulta= Enero 2011.

[50] Mozilla Inc., "MFSA 2010-82", http://www.mozilla.org/security/announce/2010/mfsa2010-82.html. Fecha de consulta= Enero 2011.

[51] Mozilla Inc., "MFSA 2010-83", http://www.mozilla.org/security/announce/2010/mfsa2010-83.html. Fecha de consulta= Enero 2011.

[52] Mozilla Inc., "MFSA 2010-84", http://www.mozilla.org/security/announce/2010/mfsa2010-84.html. Fecha de consulta= Enero 2011.

[53] TechMediaNetwork, "2011 Internet Browser Software Review Product Comparisons", http://internet-browser-review.toptenreviews.com/. Fecha de consulta= Enero 2011.

[54] Mozilla Inc., "Reporte de Vulnerabilidades para Mozilla Firefox®" http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.13 . Fecha de consulta= Enero 2011.

APENDICE J: ACRONIMOS

CAT	Cambio a través del tiempo
CVDS	Ciclo de Vida de Desarrollo de Software
CVDS Seguro	Ciclo de Vida de Desarrollo de Software Seguro
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
POBC	Procedimientos Organizacionales Bien Conocidos
SANS	SysAdmin, Audit, Network, Security Institute
SI	Sistema de Información
SP	Special Publication