	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
Universidad Francisco de Paula Santander Ocaña - Colombia Vigilada Mineducación	Documento: FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Código: F-AC-DBL-007	Fecha: 10-04-2012	Revisión: A
	Dependencia: DIVISIÓN DE BIBLIOTECA	Aprobado: SUBDIRECTOR ACADEMICO		Pág.: i(64)

RESUMEN – TRABAJO DE GRADO

AUTORES	**JOSE LUIS PEÑARANDA SUAREZ**
FACULTAD	**FACULTAD DE INGENIERIA DE SISTEMAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**YESICA MARIA PEREZ PEREZ**
TÍTULO DE LA TESIS	**DIAGNOSTICO DE SEGURIDAD AL SISTEMA INFORMÁTICO DE GESTIÓN DE CONTRATOS DE PRESTACIÓN DE SERVICIOS (CPS) DE LA UNIVERSIDAD DEL ROSARIO**

RESUMEN
(70 palabras aproximadamente)

EL DESARROLLO TECNOLÓGICO HA SIDO EL MÁS GRANDE DE LA HISTORIA, HA EVOLUCIONADO DE FORMA RADICAL Y VISIBLE, CAMBIANDO COMPLETAMENTE EL ESTILO DE VIDA DE LAS PERSONAS. SE PUEDE EVIDENCIAR QUE PARA CASI CUALQUIER ACTIVIDAD QUE REALICE EL SER HUMANO ES NECESARIO EL USO DE UN COMPUTADOR.

EN LOS NEGOCIOS, SE HA CONVERTIDO EN EL MAYOR ACTIVO QUE PUEDE TENER UNA ORGANIZACIÓN, SE ENCUENTRA AL ALCANCE GRACIAS A LA CONEXIÓN DE INTERNET, SUS SISTEMAS DE INFORMACIÓN SE VUELVEN VULNERABLES A ATAQUES DE EXTRAÑOS; POR ESTA RAZÓN ES FUNDAMENTAL IMPLEMENTAR PROTOCOLOS DE SEGURIDAD INFORMÁTICA.

CARACTERÍSTICAS

PÁGINAS: 64	PLANOS:	ILUSTRACIONES:	CD-ROM:1

DIAGNOSTICO DE SEGURIDAD AL SISTEMA INFORMÁTICO DE GESTIÓN DE CONTRATOS DE PRESTACIÓN DE SERVICIOS (CPS) DE LA UNIVERSIDAD DEL ROSARIO

Autor:

JOSE LUIS PEÑARANDA SUAREZ

Trabajo de Grado presentado para optar por el título de Especialista en Auditoria de Sistemas

Directora:

YESICA MARIA PEREZ PEREZ

MDE(C). ESP. Ingeniería de Sistemas.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERIA DE SISTEMAS

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

Ocaña, Colombia. Marzo, 2019

Tabla de contenido

LISTADO DE FIGURAS

LISTADO DE TABLAS

GLOSARIO

A –

Activo – cualquier cosa que tiene valor para la organización.

Amenaza – es la posibilidad de ocurrencia de cualquier tipo de evento o acción.

Ataque – Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

B –

BPM. - es una metodología corporativa y disciplina de gestión, cuyo objetivo es mejorar el desempeño (eficiencia y eficacia) y la optimización de los procesos de negocio de una organización, a través de la *gestión de los procesos* que se deben diseñar, modelar, organizar, documentar y optimizar de forma continua. Por lo tanto, puede ser descrito como un proceso de optimización de procesos.

C –

Confidencialidad. – propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

D. -

Disponibilidad. – se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos.

E –

Evaluación del riesgo. – proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

I –

Inteligencia artificial. - En ciencias de la computación, una máquina "inteligente" ideal es un agente racional flexible que percibe su entorno y lleva a cabo acciones que maximicen sus posibilidades de éxito en algún objetivo o tarea.

Incidente de seguridad de la información. – Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información. - Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para sus actividades diarias, operaciones de su trabajo, para cumplir con sus funciones, el

cual puede equivocarse o no, o hacer el bien o el mal. La información tiene estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

S –

Sistema de información. - es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Seguridad de la información. – La información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

G –

Gestión del riesgo. – Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

INTRODUCCION

En los últimos años, el desarrollo tecnológico ha sido el más grande de la historia, la tecnología ha evolucionado de forma radical y visible, cambiando completamente el estilo de vida de las personas. Se puede evidenciar que para casi cualquier actividad que realice el ser humano es necesario el uso de un computador.

En el ámbito de los negocios, la información se ha convertido en el mayor activo que puede tener una organización, esta se encuentra al alcance gracias a la conexión de internet; sin embargo, cuando las redes corporativas se conectan a internet, sus sistemas de información se vuelven vulnerables a ataques de extraños; por esta razón es fundamental implementar protocolos de seguridad informática, el cual tendrá como principal objetivo proteger la información.

Por lo general la mayoría de las empresas no comprenden la magnitud del problema al que se enfrentan por no tener implementado un proceso de seguridad informática, dejando este ítem como algo secundario, sin embargo, es tan importante reconocer el papel que juega la seguridad informática hoy en día.

Aunque las empresas se niegan a invertir en seguridad debido a que no está relacionada directamente a sus resultados operativos, es necesario realizar el proceso de concientización de la necesidad de implementar auditorias de sistemas, las cuales son de vital importancia para el buen desempeño de los sistemas de información, debido a que proporcionan los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Con el fin de garantizar la integridad, confiabilidad y disponibilidad de la información se busca ejecutar el proceso de auditoría de sistemas bajo la Guía OWASP edición 3.0 del 2008, que permita evaluar los riesgos inherentes al sistema informático de Gestión de Contratos de Prestación de Servicios (CPS) de la Universidad del Rosario, el cual será desarrollado en los siguientes capítulos de este documento.

Capítulo 1. Diagnóstico de seguridad al sistema informático de gestión de contratos de prestación de servicios (cps) de la universidad del rosario

1.1 Planteamiento del problema

La Herramienta Gestora de Contratos de Prestación de Servicios hace parte del sistema de información de Contratación muy importante para la Universidad del Rosario, teniendo en cuenta que administra información susceptible para esta entidad. Esta herramienta esta modelada en una plataforma orientada a la Web, expuesta a ataques malintencionados inherentes al uso de la Internet.

1.2 Formulación del problema

¿Cómo garantizar la confidencialidad, la integridad y la disponibilidad de la información administrada en la herramienta Gestora de Contratos de Prestación de Servicios CPS de la Universidad del Rosario?

1.3 Objetivos

1.3.1 Objetivo General

Realizar el diagnóstico de seguridad al sistema informático de Gestión de Contratos de Prestación de Servicios de la Universidad del Rosario basado en la Guía de pruebas OWASP 3.0/2008

1.3.2 Objetivos específicos

Levantar información inherente al Sistema informático de Gestión de Contratos de prestación de Servicios de la Universidad del Rosario de ahora en adelante CPS.

Documentar el resultado de la auditoria informática pasiva al sistema informático CPS.

Identificar las amenazas y vulnerabilidades del sistema informático CPS.

1.4 Justificación

El bien más preciado en una institución es la información, la cual debe tener los controles adecuados que garanticen la confidencialidad, disponibilidad e integridad de la información, siendo estos los pilares esenciales en la seguridad informática. El sistema informático CPS, administra información susceptible a ataques malintencionados, por solo estar en un ambiente Web. Adicional a esto, CPS maneja información crítica y confidencial para los procesos de la Organización, por lo tanto, se requiere asegurar que este activo este totalmente protegido. Para garantizar lo anterior, se quiere desarrollar un análisis de seguridad al sistema informático CPS, que evidencie las oportunidades de mejora.

Por otra parte, es importante mencionar que para el cumplimiento de la ley habeas data definido como: “el derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada”[i], existen dos principios de gran importancia que cualquier entidad que

administre información de personas naturales o jurídicas debe garantizar, el principio de seguridad el cual impone que la información contenida en los bancos de datos, así como aquella que resulte de las consultas que se realicen, se deben implementar las medidas técnicas necesarias para garantizar la seguridad de la información; el principio de confidencialidad, que consiste en que la Universidad del Rosario como administrador de la información está obligada en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación contractual con el usuario. (Ministerio de las tecnologias y de las comunicaciones, s.f.)

Capítulo 2. Marco Referencial

2.1 Marco Histórico

La Seguridad Informática ha experimentado un profundo cambio en los últimos años. Inversiones aisladas llevadas a cabo con el objetivo de fortalecer la seguridad en puntos muy concretos han dado paso a inversiones para asegurar el bien más valioso de la empresa, la información, enfocando la seguridad hacia los procesos de negocio de la empresa.

Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos.

Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls. Es decir, la posibilidad tecnológica de “estar conectados” llevaba implícita la aparición de nuevas vulnerabilidades que podían ser explotadas, la exposición de información crucial para el negocio que podía ser accesible precisamente gracias a esa conectividad.

El perfil de atacante de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos de un atacante o hacker podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar, o infectar un sistema mediante algún tipo de virus, pero sin ningún tipo de ánimo de lucro), en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede ser. Se trata de grupos organizados que aprovechan las vulnerabilidades de los sistemas informáticos y las redes de telecomunicaciones para acceder a la información crítica y sensible de la empresa, bien a través de personal especializado en este tipo de ataques, o bien comprando en el mercado negro kits de explotación de vulnerabilidades para obtener información muy específica.

2.1.1 Antecedentes a Nivel Mundial

Por medio de revisiones documentales de fuentes digitales, se constató que, a nivel mundial en el mes de abril de 2007, el gobierno de Estonia sufrió el que es considerado el mayor ataque cibernético de la historia, en el cual se vieron afectados la presidencia, el parlamento, la mayoría de los ministerios, los partidos políticos y dos de sus grandes bancos. Este ataque desató una gran crisis que requirió la intervención de la comunidad internacional y alertó a la Organización del Tratado del Atlántico Norte (OTAN), la cual en agosto de 2008, puso en marcha el Centro de Excelencia para la Cooperación en Ciberdefensa(CCD), con el fin de proteger a sus miembros de este tipo de ataques y entrenar a personal militar, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad.

Vale la pena mencionar otros dos ataques cibernéticos representativos. El primero, fue en contra de los Estados Unidos en el mes de julio de 2009, cuando una serie de ataques afectaron la Casa Blanca, el Departamento de Seguridad Interna (DHS), el Departamento de

Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio. Otro suceso fue el que reportó la Guardia Civil española en marzo de 2010, cuando desmanteló a una de las mayores redes de computadores "zombies", conocida con el nombre de "BotNetMariposa", compuesta por más de 13 millones de direcciones IP infectadas, distribuidas en 190 países alrededor del mundo. (Gonzales, 2012)

2.1.2 Antecedentes a Nivel Nacional

En Colombia se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones elevando su nivel de exposición a amenazas cibernéticas. El número de usuarios de internet aumentó en 354% entre el 2005 y el 2009. El número de suscriptores a internet se incrementó en 101% entre el 2008 y el 2010 alcanzando un total de 4.384.181 suscriptores de internet fijo y móvil. De estos, el 39% corresponde a suscriptores de Internet fijo y el 61% a suscriptores internet móvil.

En relación con seguridad cibernética, Colombia también ha sido objeto de ataques. Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet".

Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se cuentan PayPal, el banco suizo Post Finance, MasterCard, Visa y páginas web del gobierno suizo.

2.2 Marco Teórico

2.2.1 Antecedentes a Nivel Local

Por medio de revisiones documentales de fuentes digitales, se constató que a nivel local existen diferentes propuestas sobre la aplicabilidad de la guía la Guía OWASP edición 3.0 del 2008, de las cuales se pueden citar:

Ivan Camilo Gómez González, propone, para optar por el título de Ingeniero de Telecomunicaciones, un proyecto titulado "Diseño de Metodología para verificar la seguridad en aplicaciones web contra inyecciones SQL", el cual tuvo como objetivo diseñar una metodología para el análisis de vulnerabilidades de acuerdo a parámetros de comparación utilizados en ataques denominados inyecciones por código SQL en aplicaciones web que manejen bases de datos multidimensionales, dentro de las conclusiones que presentó este proyecto fue la de concientizar a las organizaciones de las implicaciones y de los alcances que tienen los ataques de inyección SQL. (Daniel Santiago Garzon, s.f.)

Daniel Santiago Garzón, Juan Carlos Ratkovich Gomez y Alejandro Vergara Torres, redactaron un artículo efectuado en la Universidad Javeriana, titulado "Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña escala", en el cual se definió como objetivo el desarrollo de una metodología la cual diera a conocer una serie de pasos que abarcan temas como lo son: planeación, políticas de seguridad, aseguramiento de los recursos de la compañía entre otros, los cuales contribuyan al mejoramiento de la seguridad de la información, haciendo que un sistema permanezca cubierto y preparado ante

eventualidades que puedan interrumpir el desarrollo normal de las actividades de la organización. (Seguridad, s.f.)

Francy Janeth Ramirez Parra, propone, para optar por el título de Ingeniera de Sistemas, proyecto titulado “Modelo de Estándares de Desarrollo Seguro en Aplicativos Web”, cuyo objetivo fue el de implementar un estándar en todos los procesos del desarrollo de un aplicativo web, el cual mejorará el resultado y la seguridad del aplicativo; como conclusión la autora relata que sobre los hallazgos encontrados debe darse una atención especial debido a que pueden afectar seriamente la disponibilidad, integridad y confidencialidad de la información contenida en los servidores evaluados, y para lo cual se hace necesario el uso de ciclos de mejoramiento continuo.

2.2.2 Aplicación Web

En la ingeniería de software se denomina aplicación web a aquellas herramientas que los usuarios pueden utilizar accediendo a un servidor web a través de Internet o de una intranet mediante un navegador. En otras palabras, es una aplicación software que se codifica en un lenguaje soportado por los navegadores web en la que se confía la ejecución al navegador.

Las aplicaciones web son populares debido a lo práctico del navegador web como cliente ligero, a la independencia del sistema operativo, así como a la facilidad para actualizar y mantener aplicaciones web sin distribuir e instalar software a miles de usuarios potenciales.

Existen aplicaciones como los webmails, wikis, weblogs, tiendas en línea y la propia Wikipedia que son ejemplos bastante conocidos de aplicaciones web.

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

2.2.2.1 Estructura de las aplicaciones web

Aunque existen muchas variaciones posibles, una aplicación web está normalmente estructurada como una aplicación de tres-capas. En su forma más común, el navegador web ofrece la primera capa y un motor capaz de usar alguna tecnología web dinámica, por ejemplo: PHP, Java Servlets o ASP, ASP.NET, CGI, ColdFusion, embPerl, Python o Ruby on Rails que constituye la capa intermedia. Por último, una base de datos constituye la tercera y última capa.

El navegador web manda peticiones a la capa intermedia que ofrece servicios valiéndose de consultas y actualizaciones a la base de datos y a su vez proporciona una interfaz de usuario.

2.2.2.2 Lenguajes De Programación

Existen numerosos lenguajes de programación empleados para el desarrollo de aplicaciones web en el servidor, entre los que destacan:

PHP

Java, con sus tecnologías Java Servlets y JavaServer Pages (JSP)

Javascript en su modalidad SSJS: Server Side Javascript (Javascript del lado del servidor).

Perl

Ruby

Python

C# y Visual Basic con sus tecnologías ASP/ASP.NET

También son muy utilizados otros lenguajes o arquitecturas que no son propiamente lenguajes de programación, como HTML o XML.

Se utilizan para servir los datos adecuados a las necesidades del usuario, en función de cómo hayan sido definidos por el dueño de la aplicación. Los datos se almacenan en alguna base de datos estándar. (Bradanovic, s.f.)

2.2.2.3 Ventajas

Ahorra tiempo: se pueden realizar tareas sencillas sin necesidad de descargar ni instalar ningún programa.

No hay problemas de compatibilidad: basta tener un navegador actualizado para poder utilizarlas.

No ocupan espacio en nuestro disco duro.

Actualizaciones inmediatas: como el software lo gestiona el propio desarrollador, cuando nos conectamos estamos usando siempre la última versión que haya lanzado.

Consumo de recursos bajo: dado que toda (o gran parte) de la aplicación no se encuentra en nuestra computadora, muchas de las tareas que realiza el software no consumen recursos nuestros porque se realizan desde otra computadora.

Multiplataforma: se pueden usar desde cualquier sistema operativo porque solamente es necesario tener un navegador.

Portables: es independiente de la computadora donde se utilice (PC de sobremesa, portátil) porque se accede a través de una página web (solamente es necesario disponer de acceso a Internet). La reciente tendencia al acceso a las aplicaciones web a través de teléfonos móviles requiere sin embargo un diseño específico de los ficheros CSS para no dificultar el acceso de estos usuarios.

La disponibilidad suele ser alta porque el servicio se ofrece desde múltiples localizaciones para asegurar la continuidad del mismo.

Los virus no dañan los datos porque están guardados en el servidor de la aplicación.

Colaboración: gracias a que el acceso al servicio se realiza desde una única ubicación es sencillo el acceso y compartición de datos por parte de varios usuarios. Tiene mucho sentido, por ejemplo, en aplicaciones en línea de calendarios u oficina.

Los navegadores ofrecen **cada vez más y mejores funcionalidades** para crear "aplicaciones web enriquecidas" (*Rich Internet application* o RIA)

2.2.2.4 Inconvenientes

Habitualmente ofrecen menos funcionalidades que las aplicaciones de escritorio. Se debe a que las funcionalidades que se pueden realizar desde un navegador son más limitadas que las que se pueden realizar desde el sistema operativo.

La disponibilidad depende de un tercero, el proveedor de la conexión a internet o el que provee el enlace entre el servidor de la aplicación y el cliente. Así que la disponibilidad del servicio está supeditada al proveedor.

2.2.3 Seguridad informática.

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. (Owasp, s.f.)

2.2.3.1 Objetivos de la Seguridad Informática.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, sabotajes, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

La información: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios. (Directrices para la seguridad del sistema y redes de informacion , 2012)

2.2.3.2 Amenazas.

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema desde un troyano, pasando por un programa descargando de forma gratuita que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro

sistema permitiendo la entrada a espías hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad; se pueden clasificar por tanto en amenazas provocadas por **personas, lógicas y físicas**. A continuación, se presenta a una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. La primera son las personas, la mayoría de los ataques a nuestro sistema van a provenir de forma intencionada o inintencionada de personas y pueden causarnos enormes pérdidas. (Ministerio de las telecomunicaciones y redes , s.f.)

2.2.3.4 Tipos de amenazas.

Aquí se describen brevemente los diferentes tipos de personas que pueden constituir un riesgo para nuestros sistemas. (Portal derecho informatico , s.f.)

2.2.3.4.1 Personas.

Personal (se pasa por alto el hecho de la persona de la organización incluso a la persona ajeno a la estructura informática, puede comprometer la seguridad de los equipos)

Ex-empleados (generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran la organización)

Curiosos (son los atacantes juntos con los crackers los que más se dan en un sistema)

Hackers (una persona que intenta tener acceso no autorizado a los recursos de la red con intención maliciosa, aunque no siempre tiende a ser esa su finalidad)

Crackers (es un término más preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa)

Intrusos remunerados (se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la organización)

2.2.3.4.2 Amenazas lógicas

Software incorrupto (a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.)

Herramientas de seguridad (cualquier herramienta de seguridad representa un arma de doble filo de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos, herramientas como NESUS,SAINT o SATAN pasa de ser útiles a peligrosas cuando la utilizan Crackers.)

Puertas traseras (durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se está diseñando.) Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial.)

Canales cubiertos (son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.)

Virus (un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a sí mismo en otros programas.)

Gusanos (es un programa capaz de ejecutarse y propagarse por si mismo a través de redes en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos a ser difíciles de programar su número no es muy elevado pero el daño que causa es muy grave.)

Caballos de Troya (son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera del pero que realmente ejecuta funciones ocultas.), Programas conejo o bacterias (bajo este nombre se conoce a este programa que no

hace nada útil si no que simplemente se delimitan a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación del servicio.

2.2.3.5 Amenazas Físicas.

Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales.

2.2.4 Amenaza Informática del Futuro

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

Se puede afirmar que “la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas”.

Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

"La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas", La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital".

Obtención de perfiles de los usuarios por medios, en un principio, lícitos: seguimiento de las búsquedas realizadas, históricos de navegación, seguimiento con geoposicionamiento de los móviles, análisis de las imágenes digitales subidas a Internet, etc. (Oswap, s.f.)

2.2.5 Información

Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para sus actividades diarias, operaciones de su trabajo, para cumplir con sus funciones, el cual puede equivocarse o no, o hacer el bien o el mal. La información tiene estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

2.2.6 Pilares básicos de la seguridad de la Información.

2.2.6.1 Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información

confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

2.2.6.2 Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) *Grosso modo*, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

La integridad también es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes que son parte de la información.

La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

2.2.6.3 Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir

con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

2.2.6.4 Ingeniería Social

Existen diferentes tipos de ataques en Internet como virus, troyanos u otros; dichos ataques pueden ser contrarrestados o eliminados, pero hay un tipo de ataque, que no afecta directamente a los ordenadores, sino a sus usuarios, conocidos como *"el eslabón más débil"*. Dicho ataque es capaz de conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos. Además, es un ataque más eficiente, debido a que es más complejo de calcular y prever. Se pueden utilizar infinidad de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

2.2.7 Incidente de seguridad de la información

Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer operaciones del negocio a amenazar la seguridad de la información.

2.2.8 Análisis del riesgo

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

2.2.9 Técnicas de respaldo y los sistemas redundantes

Los sistemas de respaldo (backup) y los sistemas redundantes son dos técnicas para proteger los datos contra pérdida por borrado accidental o desastres fortuitos, ambos sistemas son complementarios en cuanto a la seguridad que ofrecen ya que tanto los respaldos como la redundancia por si solos tienen problemas.

2.2.10 Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP)

Es una comunidad abierta dedicada a permitir a las organizaciones realizar el desarrollo, adquisición y mantenimiento de aplicaciones fiables. Todas las herramientas, documentos, foros y delegaciones del OWASP son libres y abiertas a cualquier interesado en mejorar la seguridad de las aplicaciones.

2.2.11 Guía OWASP edición 3.0.

La guía de pruebas OWASP, es un documento desarrollado para cubrir los procedimientos y herramientas diseñados para probar la seguridad de las aplicaciones.

2.2.12 Modelo PHVA

La aplicación del modelo PHVA también reflejará los principios establecidos en las directrices OCDE (2002) que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

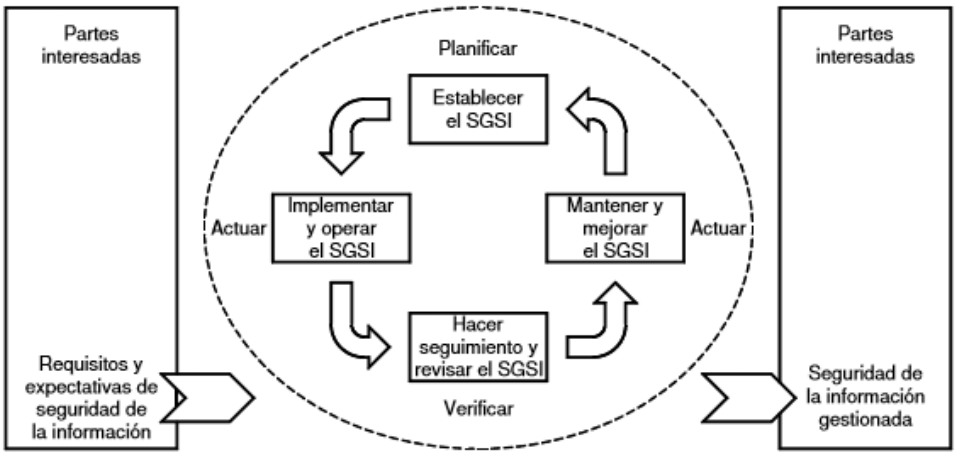

figura 1. **Modelo PHVA aplicado a los procesos SGSI.** Recuperado de *http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf*

Tabla 1. Modelo PHVA.

Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Recuperado de

http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

2.3 Marco Legal

2.3.1 CONPES 3701 de 2011 – Lineamientos Ciberseguridad y Ciberdefensa

Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

2.3.2 LEY 1266 de 2008 – Habeas Data financiera y seguridad en datos personales.

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

2.3.3 LEY 1581 de 2012 – Ley Estatutaria de Protección de datos personales.

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

2.3.3.1 Aspectos claves de la normatividad.

Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

Crea una especial protección a los datos de menores de edad.

Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

Crea el Registro Nacional de Bases de Datos.

Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

2.3.4 Decreto 1377 De 2013

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

2.3.5 LEY 527 de 1999 – Validez Jurídica y probatoria de la información electrónica.

Por medio del cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

2.3.6 LEY 594 de 2000 – Ley General de Archivos – Criterios de Seguridad

La presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.

2.3.7 LEY 1273 de 2008 – Delitos informáticos y protección del bien jurídico tutelado que es la información.

Esta ley crea un nuevo bien jurídico tutelado – denominado "la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios

mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales,

datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.3.7.1 LEY 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad.

Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones -TIC- se crea la agencia nacional del espectro y se dictan otras disposiciones.

2.3.8 LEY 603 DE 2000 – Derechos de autor.

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

2.3.9 LEY 1712 de 2014 – Transparencia en acceso a la información pública.

El objeto de esta ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

2.3.10 DECRETO 1360 de 1989.

Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor.

2.3.11 DECRETO 1727 de 2009.

Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

2.3.12 Código Penal.

Art. 199. Espionaje

Art. 258. Utilización indebida de información

Art. 418. Revelación de Secreto

Art. 419. Utilización de asunto sometido a secreto o reserva

Art. 420. Utilización indebida de información oficial

Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública

Capítulo 3. Metodología De La Investigación

3.1 Tipo de investigación

El foco de investigación de este proyecto es la realización de un diagnóstico de seguridad al sistema informático de Gestión de Contratos de Prestación de Servicios de la Universidad del Rosario basado en la Guía de pruebas OWASP 3.0/2008, el cual será de carácter descriptivo.

3.2 Población

La población tomada para este proyecto son los usuarios involucrados en el manejo del sistema informático CPS, de la Universidad del Rosario

3.3 Técnicas e instrumentos de recolección de información

El enfoque de esta auditoria es de Caja Blanca, donde el usuario dueño o responsable del Sistema Gestor CPS, nos da el acceso y la información necesaria para iniciar con la auditoria, pero adicional a esto, se debe recabar información que el mismo usuario desconoce y se deben ejecutar otras metodologías para tener dicha información

Entrevistas con usuarios administradores

3.3.1 En esta entrevista se solicitó la información relevante al objeto a auditar.

Ip del servidor

Sistema operativo

Versión del BPM

Usuarios de acceso al servidor

3.4 Herramientas tecnológicas.

A través de la implementación de estas herramientas recolectaremos información que los usuarios desconocen, pero es importante para objetivo de la auditoría.

Capítulo 4. Presentación de resultados

4.1 Primer objetivo Específico

Con la colaboración del Área de Nomina y Contratación de la Universidad del Rosario, se da inicio a la auditoria informática con la Autorización del Jefe de Desarrollo e Innovación de Tecnología. Esta auditoria informática tiene como objetivo garantizar la confidencialidad, disponibilidad e integridad de la información administrada y almacenada en la Herramienta Web de Gestión de Contratos de Prestación de Servicios CPS.

Este análisis se llevó a cabo en las siguientes Fases:

4.2 Reconocimiento.

El objetivo de esta etapa es recabar toda información relevante, tanto al proceso de contratación de prestación de servicios, como del mismo aplicativo.

En este caso el auditado nos proporcionó un ambiente clone de producción donde realizaremos nuestras verificaciones o pruebas necesarias para recabar información.

Información suministrada por el Auditado

Tabla 2. Información básica suministrada por el auditado

Nombre del Aplicativo a auditar	Gestión de Contratos de Prestación de Servicios CPS
URL	http://10.10.10.39/sysTestPM/es/urosario/setup/main (clone de producción)
Tipo de aplicación Web	BPM 2.5.2.8 Enterprise Edition
IP privada	201.234.181.86
IP privada	**********
SO	Linux
Distribución	Red Hat
Versión	6.8
Usuario ssh	**********
Contraseña usuarios ssh	**********

Ya disponemos de información suministrada por el cliente auditado, a partir de este momento se hizo una recopilación adicional a través de herramientas hechas para una auditoria informática. Es importante tener la mayor cantidad de información posible.

4.2.1 Información de DNS

A través de la herramienta WHOIS, podemos averiguar información detallada de los DNS, como quien o quienes son los propietarios, información de contacto. Para ello ingresamos a la url http://whois.domaintools.com/ y digitamos el dominio al que queremos recabar información:

– Whois & Quick Stats

Email	luis.amaya@urosario.edu.co is associated with ~2 domains luis.castiblanco@urosario.edu.co is associated with ~2 domains — Reverse Whois
Registrant Org	UNIVERSIDAD DEL ROSARIO is associated with ~6 other domains
Dates	Created on 1998-09-02 - Expires on 2016-12-31 - Updated on 2015-06-23
IP Address	201.234.181.59 - 4 other sites hosted on this server
IP Location	- Distrito Capital De Bogota - Bogota - Level 3 Colombia S.a.
ASN	AS3549 LVLT-3549 - Level 3 Communications, Inc., US (registered Mar 21, 2000)
Whois History	89 records have been archived since 2010-01-09
Whois Server	whois.nic.co

– Website

Website Title	Universidad del Rosario - Bogotá Colombia - Universidad del Rosario
Server Type	Microsoft-IIS/7.5
Response Code	200
SEO Score	76%
Terms	341 (Unique: 227, Linked: 264)
Images	22 (Alt tags missing: 4)
Links	82 (Internal: 68, Outbound: 12)

figura 2. Respuesta del Whois

En este primer contacto tenemos información de ip publica, ubicación, nombres de los propietarios y correos electrónicos de contacto.

```
Domain Name:                            UROSARIO.EDU.CO
Domain ID:                              D616823-CO
Sponsoring Registrar:                   .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID:           111111
Registrar URL (registration services):  www.cointernet.com.co
Domain Status:                          clientTransferProhibited
Registrant ID:                          4655-REG
Registrant Name:                        Luis Antonio Amaya
Registrant Organization:                UNIVERSIDAD DEL ROSARIO
Registrant Address1:                    CALLE 14 # 6-25
Registrant City:                        BOGOTA
Registrant State/Province:              Bogota
Registrant Postal Code:                 11001
Registrant Country:                     Colombia
Registrant Country Code:                CO
Registrant Phone Number:                +57.12970200
Registrant Email:                       luis.amaya@urosario.edu.co
Administrative Contact ID:              4655-ADMIN
Administrative Contact Name:            Luis Eduardo Castiblanco
Administrative Contact Organization:    UNIVERSIDAD DEL ROSARIO
Administrative Contact Address1:        Av. Jimenez 4.09
Administrative Contact Address2:        Calle 14 6-25
Administrative Contact City:            Bogota
Administrative Contact State/Province:  Bogota
Administrative Contact Postal Code:     11001
Administrative Contact Country:         Colombia
Administrative Contact Country Code:    CO
```

figura 3. Respuesta del Whois 2.

```
Name Server:                                  JUNO.IMPSAT.NET.CO
Name Server:                                  NS1.IMPSAT.NET.CO
Name Server:                                  SERVER1.UROSARIO.EDU.CO
Created by Registrar:                         NEULEVELCSR
Last Updated by Registrar:                    .CO INTERNET S.A.S.
Domain Registration Date:                     Wed Sep 02 00:00:00 GMT 1998
Domain Expiration Date:                       Sat Dec 31 23:59:59 GMT 2016
Domain Last Updated Date:                     Tue Jun 23 22:57:41 GMT 2015
DNSSEC:                                       false
```

figura 4. Respuesta del Whois 3.

4.2.2 Documentación de tipo de aplicación.

El sistema Gestor CPS, es un macro proceso que esta modelado en una plataforma que utiliza la tecnología BPM llamada ProcessMaker. Este macro proceso cuenta con siete procesos modelados:

figura 5. Procesos de CPS

Cada proceso tiene su flujo de aprobación, principal característica para ser modelado en un BPM.

Como ya tenemos el acceso al sistema gestor, es importante tener más información de la aplicación BPM, en Información del sistema:

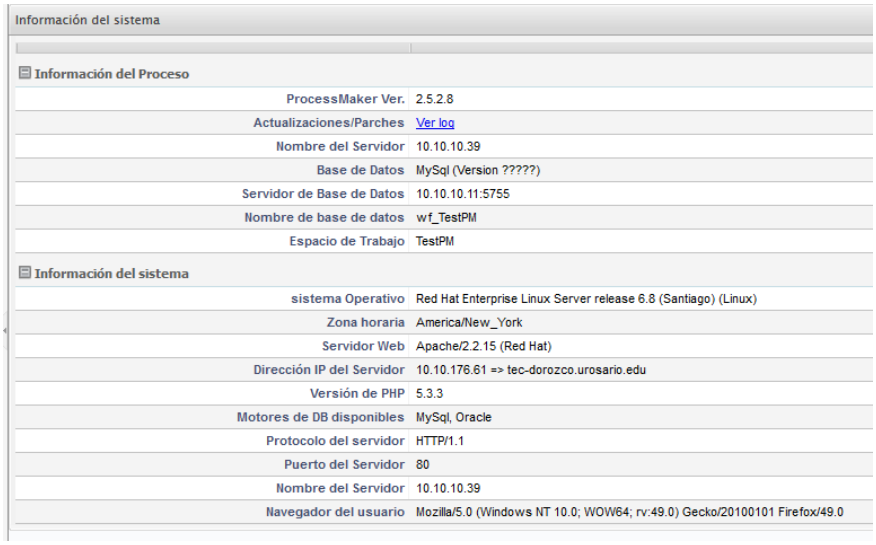

figura 6. Información del Aplicativo

Como podemos observar en la imagen, la versión del BPM es la 2.5.2.8, instalado en un servidor Linux Red Hat Enterprise Server reléase 6.8.

En la página oficial de ProcessMaker, encontramos que la última versión estable es la 3.1.2 (fecha de revisión, 05/06/2016). Este es un hallazgo de oportunidad de mejora, que se da en la etapa de reconocimiento. Es necesario iniciar un proyecto de migración y actualización del BPM ProcessMaker.

4.2.3 Escaneo de puertos y versiones

Cada máquina tiene un máximo de 65.535 puertos TCP, y otros tantos UDP, desde los que se comunica con las otras máquinas de la red, lo óptimo y más seguro es tener cerrado los puertos que no se estén utilizando y este escaneo se utiliza precisamente para revisar que puertos están abiertos y cerrados.

Al ejecutar el NMAP al servidor clonado 10.10.10.39 tenemos el siguiente resultado:

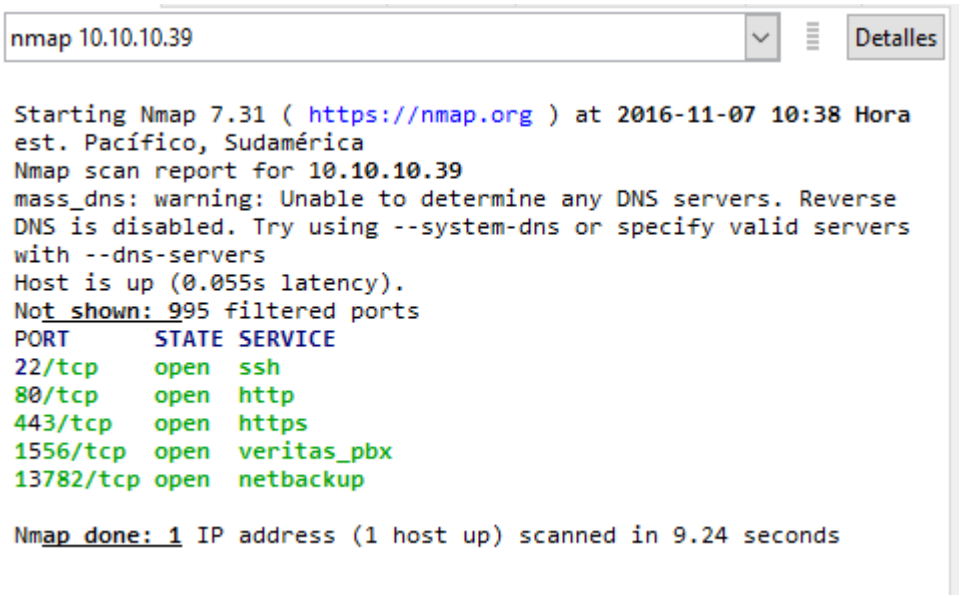

figura 7. Información del servidor clonado

Cinco puertos abiertos.

DNS deshabilitado.

Con este análisis logramos identificar los servicios que pueden tener afectación.

Nota: en este análisis tenemos una pregunta que hacer al responsable de la seguridad. ¿Para qué se está utilizando el puerto 13782?

4.2.4 Análisis SSL

En este análisis vamos a resolver los siguientes interrogantes:

¿El servidor soporta SSL?

¿Las versiones de SSL soportadas son seguras?

¿Cuál es el tamaño de las claves y los tipos de cifrado soportados por el servidor?

¿El certificado del servidor es aceptado por todos los navegadores o muestra algún tipo de error?

Para ello ejecutamos por consola los siguientes comandos:

tlssled cps.urosario.edu.co 80

El resultado que arroja es el siguiente:

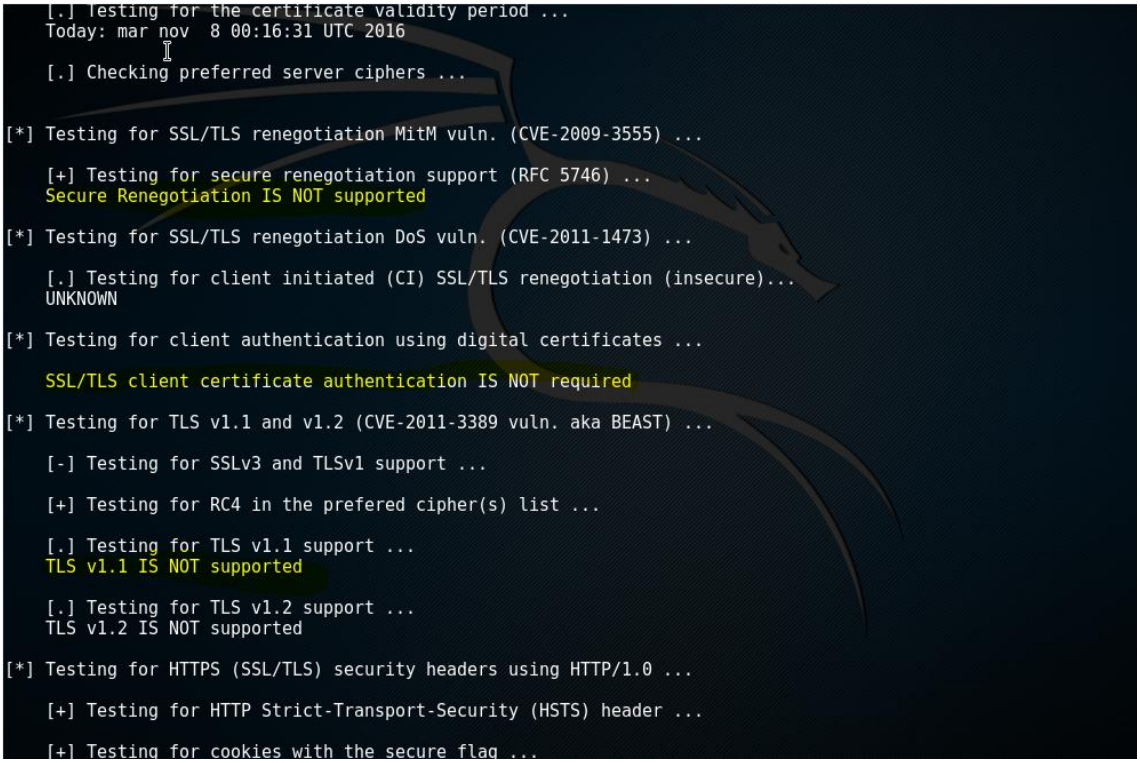

figura 8. Resultado del comando tlssled

En este caso se realizan muchas pruebas, pero ninguna de ellas da ningún resultado.

Concluimos que la comunicación TCP no soporta ningún tipo de SSL.

Ahora revisamos y hacemos la prueba, pero esta vez con el puerto 443.

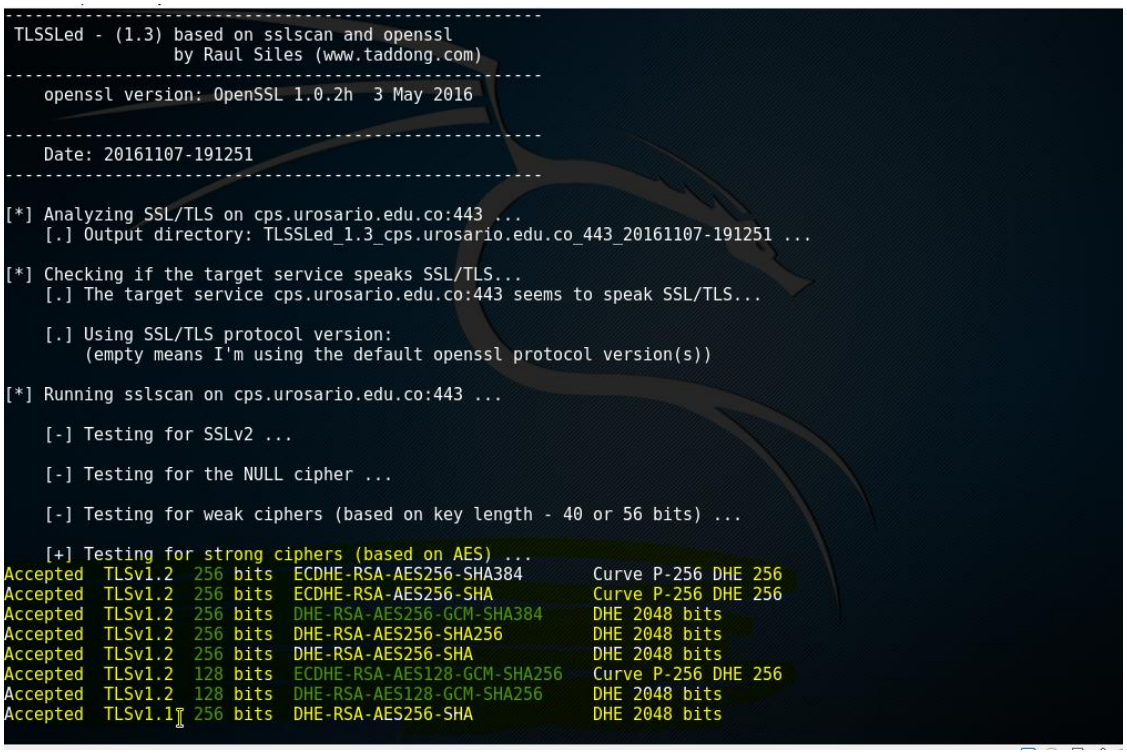

figura 9. Resultado del análisis puerto 443

Como vemos en la imagen vemos que el servidor pasa la prueba soportando algoritmos de cifrado fuertes.

Análisis de configuración del aplicativo.

A través de una herramienta que nos brinda nuestro sistema operativo Kali Linux, podemos averiguar información detallada del aplicativo en sí. Quizá información que el cliente desconoce y para el objetivo de nuestro proyecto es necesario recabar, quizá para el cliente es importante tenerla.

Para ello ejecutaremos el siguiente comando:

nikto -host cps.urosario.edu.co

El resultado de la ejecución de este comando es:

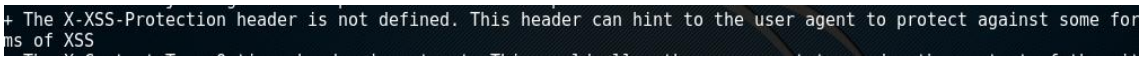

figura 10. Resultado del comando nikto

Lo que observamos en la imagen, es que el servidor tiene instalado un servidor de aplicaciones Apache con la versión 2.2.15 en un sistema Operativo Red Hat. Adicional a esto encontramos unas posibles vulnerabilidades:

El **clickjacking**, es una técnica maliciosa utilizada para engañar a usuarios suplantando los clics y enrutándolos a otras páginas. Por lo general este tipo de técnicas se utilizan para fines publicitarios.

También encontramos que el servidor de aplicaciones no está protegido frente a los filtros XSS. Para ello OWASP recomienda utilizar los HTTP headers que empiezan por X-, las cuales son variables extendidas que se pueden encontrar en el siguiente enlace: https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#X-Frame-Options_Header_Types

4.3 Segundo Objetivo Específico

Adicional al análisis pasivo, utilizando diferentes herramientas de origen Open Source, se implementó, junto con el usuario DBA (Administrador de la Base de datos por sus siglas en Ingles) una revisión de la Base de Datos del Sistema CPS.

Se le solicitó al DBA acceso a la base de datos donde se implementó la siguiente lista de chequeo a la tabla USERS de la base de datos WF_WORKFLOW.

Tabla 3. Check List integridad y redundancia de datos

Lista de chequeo - Integridad y redundancia de los datos			
NOMBRE DE LA TABLA O ENTIDAD: wf_workflow - USERS			
DESCRIPCION DE LA PRUEBA	**Cumple**		**Observación**
	Si	**No**	
Existe llave primaria	**X**		El sistema utiliza como llave primaria el campo APP_UID como llave primaria.
¿La llave primaria esta duplicada?		**X**	Se hizo la revisión y no se encontró duplicidad
¿La llave primaria cumple con los criterios para ser llamada llave primaria?	**X**		
¿Existen campos nulos en la llave primaria?		**X**	
¿El tipo de dato es el indicado para cada campo de la tabla o entidad?	**x**		
¿Los tamaños son los justos para cada campo?	**x**		
¿La tabla tiene un campo con registros consecutivos?		**x**	Aunque la llave primaria es único e irrepetible no existe un campo consecutivo donde indique que no se han borrado datos
¿Existe un campo de tipo Date donde se registre la fecha y hora del registro?	**x**		El nombre del campo es USER_DATE_CREATE de tipo datetime

Tabla 4. Check List Controles de acceso a la BD

Lista de chequeo - Controles de acceso a la BD			
NOMBRE DE LA TABLA O ENTIDAD: wf_workflow - USERS			
DESCRIPCION DE LA PRUEBA	**Cumple**		**Observación**
	Si	**No**	
Existe algún archivo de tipo Log donde se almacene los eventos u operaciones que se realizan en la Base de Datos		**X**	no existe un log de eventos donde se verifique cada cambio o acciones de las operaciones de cada usuario
Existe un (solo uno) DBA o responsable con permisos de administrador	**x**		
existe un usuario con privilegios de consulta o actualización, si permisos de administrador	**X**		
existe varios usuarios con privilegios de consulta o actualización, si permisos de administrador	**X**		
¿Existe un documento inventario con la información detallada de cada usuario?		**X**	Aunque la base de datos no tiene un inventario, el mismo sistema tiene un sistema de usuarios bien estructurado.
¿Existe un procedimiento de monitoreo permanente de la disponibilidad del servidor donde se aloja la base de datos?	**X**		el área de servidores utiliza una herramienta llamada SolarWinds, donde se lleva el control de cada uno de los servidores de la institución
Existe un procedimiento de respaldo o recuperación	**x**		El sistema tiene un crontab, o tarea programada todos los días en la madrugada, donde ejecuta un backup de la base de datos

Después de la revisión de la base de datos, se encontró que la base de datos es de tipo transaccional, es decir, que tablas tienen movimientos constantes en la mayoría, y el tipo de motor de MySQL es MyIsam, la cual no es la correcta para bases de tipo transaccional. Para estas bases de datos se recomiendo utilizar el Motor InnoDB.

Se recomienda utilizar un campo consecutivo de tipo auto-increment, en las tablas más importantes como son: USERS, APPLICATION. Este campo evita el borrado indiscriminado de un registro y a la detección de una irregularidad.

4.4 Tercer Objetivo Específico

Conclusiones

Después del análisis de la información recabada y suministrada por el usuario, se encontró que el Sistema Informático De Gestión De Contratos De Prestación De Servicios (CPS) se encuentra en Buen estado en cuanto a la estructura de la base de datos, una administración en el manejo de la base de datos con solo algunas recomendaciones a ser tenidas en cuenta:

La implementación de campos autoincrement consecutivos que identifiquen si hubo un borrado injustificado de algún registro.

El control de eventos donde se registre algún cambio y su justificación. Si en las tablas hubo algún borrado del registro, este debe ser registrado en el Control de eventos.

El cambio de tipo de motor MyIsam a InnoDB, debido a que la mayoría de las tablas tienen un alto índice de movimientos o transacciones, esto ayudaría al performance de la base de datos.

En cuanto a la seguridad del aplicativo web, se encontraron algunas vulnerabilidades que pueden exponer la integridad de la información almacenada y observaciones adicionales:

La versión instalada del ProcessMaker es la 2.5.2.8 y última versión es la 3.0.5 la cual tiene solucionada muchas de las vulnerabilidades de seguridad que tiene la versión instalada, por tanto, se recomienda su actualización.

La versión actual, no es compatible con los dispositivos móviles, no es Responsive. Aunque no es una vulnerabilidad, es un requisito opcional si se quiere aumentar la experiencia de usuario.

En los hallazgos encontrados en la etapa de reconocimiento y exploración de información se encontró que el sistema no tiene medidas para evitar el clickjacking. Técnica maliciosa utilizada para engañar a los usuarios suplantando el destino y enrutarlos a páginas desconocidas.

También encontramos que el servidor de aplicaciones no está protegido frente a los filtros XSS (***Cross-site scripting***). Este último es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar. Se recomienda utilizar los HTTP headers que empiezan por X-, las cuales son variables extendidas que se pueden encontrar en el siguiente enlace: https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#X-Frame-Options_Header_Types

Referencias

Bradanovic, T. (s.f.). *asesorias y proyectos.* . Obtenido de http://www.bradanovic.cl/pcasual/ayuda3.html

Daniel Santiago Garzon. (s.f.). Obtenido de http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

Directrices para la seguridad del sistema y redes de informacion . (julio de 2012). Obtenido de www.oecd.org.

Gonzales, I. C. (2012). Obtenido de http://repository.unimilitar.edu.co/bitstream/10654/7212/2/GomezGonzalezIvanCamilo2012.pdf

http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf. (s.f.).

Ministerio de las tecnologias y de las comunicaciones. (s.f.). Obtenido de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Ministerio de las telecomunicaciones y redes . (s.f.). Obtenido de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Oswap. (s.f.). Obtenido de https://www.owasp.org/index.php/Clickjacking

Owasp. (s.f.). Obtenido de https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

Portal derecho informatico . (s.f.). Obtenido de http://derechoinformatico.co/legislacion-que-protege-la-informacion-en-colombia/

Seguridad. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica