MR – SPEL. MARCO DE REFERENCIA PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE PAGOS EN LÍNEA DE UNIVERSIDADES OFICIALES EN COLOMBIA

YOHANA ANDREA TRUJILLO CAIPE
FIDEL CAMILO HIDALGO ZAMBRANO

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
ÁREA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN
2010

MR – SPEL. MARCO DE REFERENCIA PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE PAGOS EN LÍNEA DE UNIVERSIDADES OFICIALES EN COLOMBIA

YOHANA ANDREA TRUJILLO CAIPE
FIDEL CAMILO HIDALGO ZAMBRANO

TRABAJO DE GRADO

Director: Ing. SILER AMADOR DONADO

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS
ÁREA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA
POPAYÁN, JUNIO DE 2010

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRÓNIMOS

ACH: Automatic Clearing House (Cámara de Compensación Automática).
BSI: British Standards Institute (Instituto de Estándares Británico).
CENIT: Compensación Electrónica Nacional Interbancaria
CNUDMI: Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.
DNS: Domain Name Server (Servidor de Nombres de Dominio)
IEC: International Electrotechnical Commission (Comisión Internacional Electrotécnica).
ISO: International Organization for Standarization (Organización Internacional para la Normalización).
NACHA: National Automated Clearing House Association (Asociación Nacional de Cámaras de Compensación Automatizadas).
OSSIM: Open Source Security Information Management (Gestión de Seguridad de Información de Código Abierto).
OSSTMM: Open Source Security Testing Methodology Manual (Manual de la Metodología Abierta de Testeo de Seguridad).
OWASP: The Open Web Application Security Project (Proyecto Abierto de Seguridad de Aplicaciones Web).
PSE: Proveedor de Servicios Electrónicos
RAV: Risk Assessment Values (Valores de la Evaluación del Riesgo)
SDLC: Software Develop Life Cicle (Ciclo de Vida del Desarrollo de Software).
SGSI: Sistema de Gestión de Seguridad de la Información
SI: Seguridad de la Información.
SMS: Short Message Service (Servicio de Mensaje Corto)
SPEL: Sistema de Pagos en Línea
SOAP: Simple Object Acess Protocol
SSL: Secure Sockets Layer (Protocolo de Capa de Conexión Segura)
TI: Tecnología de la Información
TIA: Telecommunications Industry Association
TOE: Target of Evaluation (Objetivos de Evaluación).
WSE: Web Services Enhancement

INTRODUCCION

La evolución de las tecnologías de la información y la comunicación (TIC) ha posibilitado nuevas formas en cómo las personas se relacionan, se comunican y cómo se establecen relaciones comerciales. Cuando Internet dejo de ser el medio que servía como fuente de información y paso a ser el medio que permitió ofrecer servicios y obtener resultados (productos) con los beneficios de mayor disponibilidad, en tiempo real, con diversidad de mercados, más agiles y más cómodos, el comercio electrónico y principalmente el pago en línea tomaron importancia en todos las formas de hacer negocios y por ende en la economía mundial.

Todas las empresas, entidades o comercios tiene un mercado al cual ofrecen determinado producto ya sea bien o servicio y por el cual los clientes deben pagar el costo del mismo; en este proceso de distribución o de compra venta de un producto y en el que interviene las TIC, se puede hablar de comercio electrónico. En este contexto se evidencian tres momentos en cómo se puede realizar la venta del producto y cómo las TIC, principalmente internet impactaron directamente en la forma de hacer negocios o de comercializar los productos. En un primer paso las TIC se utilizan para dar a conocer o presentar información acerca del bien o del servicio que se ofrece, esto por medio de documentos, comunicados, anuncios, catálogos de servicios; aquí el cliente solo es receptor de información, conoce lo que va a comprar. Luego un segundo paso es cuando el usuario puede interactuar, generalmente con un servicio web donde puede diseñar, escoger y solicitar el producto que desea. Un tercer paso es donde se puede realizar el pago en tiempo real por el producto, transferir dinero electrónicamente desde la cuenta del usuario a la cuenta de la empresa. Un cuarto paso que es la recepción del producto o servicio, que depende del producto que se comercializa; si el servicio se puede trasmitir por internet se realiza la entrega y si no, se envían los productos por los medios tradicionales de entrega y con esto se complementa el ciclo de compra venta. Estos pasos son consecutivos e incrementales ya que la empresa tiene que ir mejorando la infraestructura tecnológica que le permita ofrecer el servicio de comercio electrónico con calidad en cualquiera momento de su proceso.

Considerando a las Universidades oficiales como las entidades que desean ofrecer el sistema de pago en línea como el medio para el recaudo del dinero que perciben por los servicios que presta a estudiantes, docentes y otros beneficiarios de la entidad como: el valor de la matricula, costo de exámenes supletorios, constancias, certificados y demás servicios que implican recibir dinero. En el contexto de la Universidad del Cauca, con el recaudo de la matricula y a manera de ejemplo se puede representar los tres pasos mencionados anteriormente, primero solo se permitió consultar el valor de la matricula y la fecha de pago (sistema como proveedor de información), luego fue posible consultar el recibo e imprimirlo para pagarlo en el banco (sistema como generador de información) y por último se habilito el botón de pago en línea para el recibo de matrícula. Antes el

proceso del pago de la matricula se llevaba a cabo en medio día en el mejor de los casos y con el sistema de pago en línea se puede realizar en un espacio de 10 minutos.

A medida que estos pasos son soportados en sistemas de información, también se exponen a diferentes amenazas informáticas que pueden afectar un activo de información asociado al servicio, teniendo en cuenta que un activo es el valor económico que tiene algo para su dueño, en el primer y segundo paso solo se comprometen los activos de la empresa que ofrece el servicio de pago. Pero el momento del pago en línea involucra información sensible de los clientes directos de la empresa como identificaciones personales e información de acceso a dinero real, debido a esta característica la empresa que ofrece el servicio de pago en línea, debe garantizar a sus clientes que el servicio esta soportado en un sistema de gestión de la seguridad de la información (SGSI) que le permite tener un respaldo de confianza para los usuarios del sistema de pagos.

Los sistemas de información en la actualidad se concentran en los servicios que deben ofrecer, descuidando la gestión de los riesgos informáticos. Existen varias normas como la ISO/IEC 27001, ISO 9000, ISO/IEC 13335, TIA 942, ISO 25000 e ISO 15408 que se encargan de la seguridad de la información, sin embargo cada una de ellas presenta fortalezas y debilidades en el momento de aplicarlas, además en la fase de pruebas de seguridad que en muchas de ellas se contempla, no se hace referencia a una metodología de pruebas de seguridad específica, siendo algunas de ellas OSSIM, ISSAF, OSSTMM y OWASP.

El proyecto de investigación MR-SPEL, tiene como propósito generar un marco de referencia referente al proceso de gestión de seguridad de la información, asociada al sistema de pago en línea que utilizan o utilizarían las universidades oficiales de Colombia; el SPEL se implementa bajo la arquitectura tecnológica del servicio de botón de pagos PSE de ACH Colombia.

El interés de proponer un marco de referencia para gestionar la seguridad de la información del SPEL, es brindar garantías de confianza a los usuarios de la comunidad universitaria al utilizar un medio de pago que permite tener comodidad y agilizar el proceso de pagos a la Universidad; ya que es un servicio que involucra el manejo de información sensible, está asociada al manejo de dinero, lo que representa un compromiso para la Institución velar por el correcto procesamiento de este tipo de información.

Metodológicamente el desarrollo de este trabajo se soporta en el Modelo Integral para el profesional en Ingeniería [1] y dos de sus submodelos el Modelo para la Investigación Documental y el Modelo para la Construcción de Soluciones, el primero en sus 4 fases y el segundo en la etapa 4 la validación.

Los objetivos específicos que se lograron se ven reflejados en el contenido de los capítulos uno, dos y tres, como se explica a continuación.

En primera instancia se elabora una base de conocimientos que tiene como propósito adquirir la información suficiente en las temáticas que son objeto de análisis, de esta forma la investigación tiene como tema central de estudio la “Gestión de seguridad de la información en el SPEL de las Universidades Oficiales”. Este tema está conformado por los siguientes subtemas o núcleos temáticos: gestión de seguridad de la información, sistema de pago en línea y contexto de las universidades oficiales. La estructura del capítulo 1 refleja la síntesis de los núcleos temáticos y la construcción teórica global de los mismos. Aunque las fichas descriptivas de los referentes seleccionados no se describen en este trabajo, se realizó un análisis de las mismas para la construcción teórica global y por ende para el desarrollo de la base de conocimiento.

La Universidad de Nariño, Universidad del Cauca y Universidad del Valle son las universidades oficiales colaboradoras con el proyecto de investigación, que actúan como fuentes de información en relación a la forma cómo se llevó o se llevaría a cabo el proceso de implementar el botón de pagos PSE y cómo hacen para garantizar la seguridad de la información del SPEL dentro de su Universidad.

Con la base de conocimientos elaborada, y el conocimiento del contexto de las Universidades Estatales, en el capítulo 2 se proponen los lineamientos que le permitirán a una Universidad Oficial, implantar un SGSI para el SPEL. Algunos lineamientos generados se desarrollaron para el SPEL de la Universidad del Cauca que es el caso de estudio real, el resultado de estos desarrollos se encuentran en el capítulo 3.

Adicional al documento se presentan algunos anexos que complementan la información descrita, así:

El Anexo A contiene las actividades que propone ACH COLOMBIA, para llevar a cabo el proyecto de desarrollo del botón de pagos PSE.

El Anexo B es una propuesta de un acuerdo de confidencialidad, dirigido a los funcionarios de la División de Sistemas de la Universidad del Cauca encargados del SPEL.

El Anexo C es un documento que se propone para llevar un registro de control del ingreso y operaciones que se ejecutan en una sala de servidores.

El Anexo D contiene el diseño de la encuesta que se aplico en la Universidades colaboradores, para obtener información relacionada a la seguridad de la información y el posible SPEL de cada una de ellas.

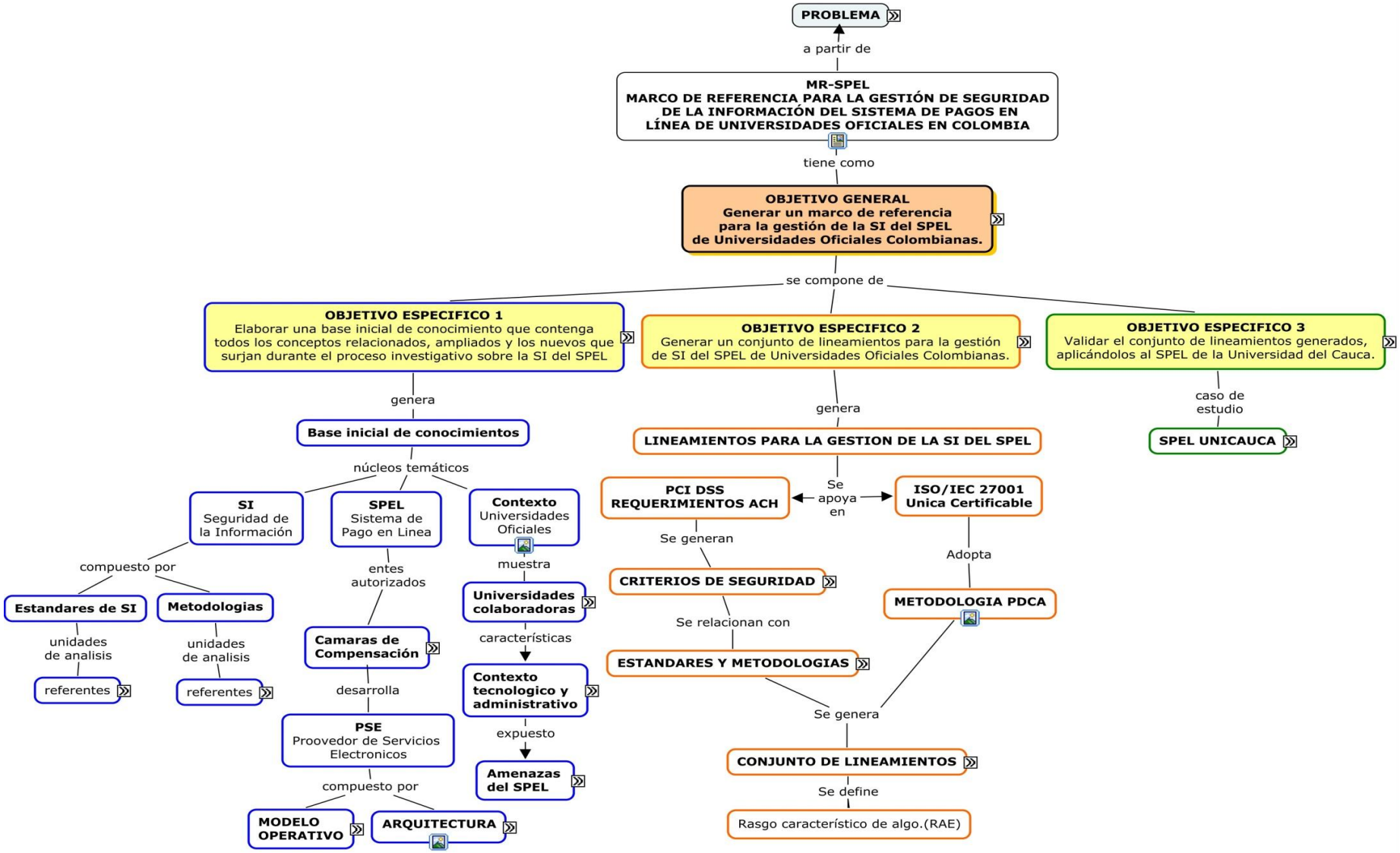


Figura 1. Diagrama General MR-SPEL

Capítulo 1 DISEÑO Y ELABORACION DE LA BASE INICIAL DE CONOCIMIENTO

“La base de conocimientos determina el estado del conocimiento en la temática seleccionada y por lo tanto da cuenta de la investigación que se ha realizado sobre dicha temática. Esta temática se desglosa en núcleos temáticos (subtemas), cada uno de los cuales delimita un campo de conocimiento y está constituido por investigaciones afines”. [1].

El tema central de este trabajo de investigación es la gestión de la SI del SPEL de Universidades Oficiales de Colombia, para lo cual se tomaron tres núcleos temáticos: Seguridad de la Información, Sistema de Pagos en Línea y Contexto de las Universidades Oficiales de Colombia.

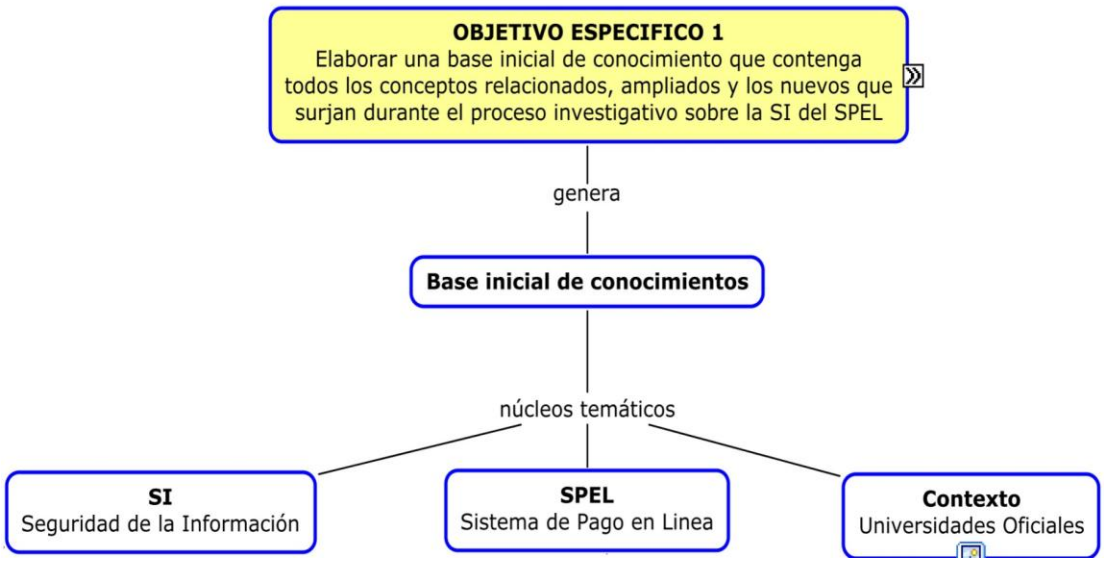


Figura 2. Diagrama Objetivo Específico 1

1.1 Seguridad de la Información

1.1.1 Definición

Los orígenes de internet se fundamentan con la evolución y construcción de las primeras redes de datos: pequeñas y privadas; donde se identificaba físicamente a los usuarios y se conocía la cantidad de los mismos, así no era necesario el proceso de autenticación en la red y dada la confianza de los usuarios interconectados, generalmente grupos de trabajo, se esperaba el uso adecuado de la misma, donde todos velaran por el buen funcionamiento y el aprovechamiento ideal de los recursos en red, donde por lo anterior

eran innecesarios antivirus, firewalls, sistemas de detección de intrusos o sistemas que evitaran las acciones mal intencionadas ya sea contra la infraestructura de red o la información disponible. Con el crecimiento de las redes, las interconexiones mundiales, el uso de empresas privadas, gubernamentales y del público en general; las fallas o vulnerabilidades intrínsecas al origen de las redes, fueron descubiertas y mal utilizadas. Es así como desde la década de los 90 cuando empiezan a surgir los virus y amenazas a la información y a los sistemas informáticos, nace también la necesidad de protegerse ya que se crea conciencia del peligro, y esto representa pérdida de dinero. Es así como se crea el concepto de *"Seguridad de la Información (SI)"*.

Según la ISO/IEC 27001:2005 define la SI como: "*Preservación de la confidencialidad, integridad, y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio, y confiabilidad."* [2]

La ISO/IEC 17799:2005 la define como: "*La protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales."* [3]

De estas definiciones es importante resaltar que buscan preservar características importantes que debe tener la información dentro de una organización como: disponibilidad, integridad, no repudio, autenticidad y confidencialidad [4].

- Disponibilidad: Se debe tener acceso a la información cada vez que se requiera.
- Integridad: La información debe permanecer completa.
- No repudio: Responsabilidad absoluta del origen o fuente de la información.
- Autenticidad: La información debe permanecer exacta.
- Confidencialidad: Solo pueden acceder a la información las personas autorizadas.

La SI debe ser un proceso integral, para ello es necesario gestionarla.

Según la Real Academia Española [5] gestionar significa *"Hacer diligencias conducentes al logro de un negocio o de un deseo cualquiera".* Enfocándolo en el área de interés la gestión de la SI sería la realización de las tareas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

En este sentido un sistema de gestión de la seguridad de la información (SGSI) es el sistema que basado en el análisis de riesgos, establece, opera, monitoriza, revisa, mantiene y mejora la SI [2].

El SGSI es el concepto central sobre el cual se construye la norma ISO/IEC 27001, la cual se ha tomado como base para la realización de este trabajo.

1.1.2 Generalidades

La arquitectura propuesta por la ISO en 1984 de las siete capas: aplicación, presentación, sesión, transporte, red, enlace de datos y física de El *modelo* de Interconexión de Sistemas Abiertos (*OSI*, Open System Interconnection) [6], ha sido como referente teórico y como punto de partida para que la información viaje adecuadamente desde su origen a su destino (transportar información); teniendo en cuenta que al atravesar las siete capas se acceden o manipulan los datos por diferentes protocolos, dispositivos y medios, como también se los puede acceder o manipular mal intencionadamente aprovechándose de vulnerabilidades intrínsecas a cada capa.

Por otra parte y como complemento necesario, la información en sí misma y su seguridad involucra más campos incluso que contienen a los sistemas informáticos, por el hecho de que la información nace y es importante para las personas, así es como existen las relaciones o interacción de la información, las personas y los sistemas informáticos, lo que acarrea vulnerabilidades propias de este medio como la *Ingeniería Social* [7] y en este sentido las soluciones preventivas vienen dadas en la construcción de hábitos asociados en la creación de cultura de la seguridad de la información.

En el marco de las leyes colombianas que hacen relación a la seguridad de la información y los delitos informáticos, se encuentran las leyes de la república: 527 de 1999 [8], 1273 de 2009 [9] y diferentes artículos relacionados a las anteriores.

La ley No. 527 del 18 de Agosto de 1999 refleja la ley de Comercio Electrónico propuesta por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) [10][10], como modelo general y único que debe ser apropiado en cada país, para lograr tener en el mundo una legislación uniforme respecto de las transacciones de comercio electrónico que son globalizadas en su naturaleza. La anterior ley regula y define el uso y acceso de los mensajes de datos, el comercio electrónico, las firmas digitales y las entidades de certificación; componentes vitales para garantizar la seguridad de la información de un SPEL.

La ley No. 1273 del 5 enero de 2009 [9] complementa el Código Penal, con el Titulo VII BIS denominado “De la protección de la información y de los datos”. En su contenido tipifica delitos y prácticas conocidas por los delincuentes informáticos o crackers, que venían siendo utilizadas hasta la fecha, valiéndose de la ausencia de normas claras y penas severas en nuestra República; ahora las personas que incurran en estos delitos pueden tener penas de prisión que van desde los treinta y seis (36) a los ciento veinte (120) meses y en multas de cien (100) a mil quinientos (1500) salarios mínimos legales mensuales vigentes, dependiendo del delito, que en los decretos derogados solo se constituían como multas menores.

Cabe resaltar cómo la ley tipifica el delito, incluso con características técnicas del proceso, por ejemplo, se puede relacionar directamente el *Pharming* [11] o también conocido como ataque de hombre en el medio con el contenido del Artículo 269G: Suplantación de Sitios

Web Para Capturar Datos Personales: "*… el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza …*", como se entiende del texto se refiere a la alteración del Servidor de Nombres de Dominio (DNS Domain Name Server).

Teniendo en cuenta que es una ley técnicamente nueva, se deja abierto el debate en preguntas como: ¿La aplicación de esta ley es explicita al texto o subjetiva a la situación?, ¿Quedan por fuera de esta norma otras formas (técnicas) de efectuar fraudes?, ¿Cómo se dará respaldo al uso de estos delitos en espacios académicos y de investigación?, ¿Existen términos técnicos ambiguos al contenido?, ¿Cómo evolucionarán las prácticas de fraude informático, para encontrar nuevos vacios constitucionales?.

Las leyes anteriores son el respaldo normativo, tanto para ciudadanos e instituciones públicas o privadas, dentro de la República de Colombia, que pretenden garantizar la seguridad de la información en general. Además, posibilita a las Universidades Oficiales ajustar las políticas de seguridad y sistemas de información a los requerimientos nacionales (respecto de normas) y principalmente poder proceder jurídicamente dado el caso necesario.

1.1.3 Estándares

Dada la necesidad en el mundo de buscar mecanismos y estrategias que brinden seguridad informática y a los continuos riesgos a los que se encuentra expuesta la información, surgieron estándares y metodologías que sugieren criterios, prácticas y lineamientos que guíen a la obtención de la SI no solo basado en la parte técnica y/o tecnológica sino también en la parte de organización y control. Cubren áreas como desarrollo de aplicaciones, riesgo, autenticación, administración y evaluación de SI, control de acceso, entre otras.

Dada que la SI se tornó en una necesidad básica dentro de una empresa, cada día se realiza más inversión en este tema, por lo tanto es importante para los responsables de la SI apoyarse en estándares y/o metodologías que han sido aprobadas en consenso por grandes organizaciones líderes en el mundo en seguridad informática y tomarlas como base ajustadas a sus necesidades propias.

El proceso de estandarización de la SI ha permitido poner orden dada la diversidad de fabricantes de productos hardware y software, sistemas, redes y aplicaciones, ya que proponen una solución neutral teniendo en cuenta los intereses de fabricantes y usuarios generando mayor seguridad, fiabilidad e interoperabilidad.

1.1.3.1 ISO/IEC 15408 *Information technology - Security techniques – Evaluation criteria for IT security* (Tecnología de la Información – Técnicas de Seguridad – Criterios de Evaluación para la seguridad de las TI)

ISO/ IEC 15408 [12][11] es una guía de criterios comunes para la evaluación de productos o sistemas con funciones de seguridad de TI, de tal forma que se pueda identificar si estos cumplen o no con sus requerimientos.

La primera parte, en su segunda edición del año 2005, plantea una introducción que define principios y conceptos generales de la evaluación de la seguridad y presenta un modelo general de ésta.

La segunda parte, establece un conjunto de componentes funcionales como una manera estándar de expresar los requisitos funcionales por los Objetivos de Evaluación (*TOE - Target of Evaluation*), los cuales son los objetivos que se van a evaluar, por ejemplo redes, sistemas distribuidos y aplicaciones.

La tercera parte, establece un set de 8 componentes de confiabilidad basados en la confianza en la aplicación de las funciones de seguridad así como la efectividad de éstas.

1.1.3.2 ISO/IEC 13335: *Information technology – Guidelines for the management of IT security* (GMITS) (Tecnología de la Información – Lineamientos para la gestión de la seguridad de TI)

La ISO/IEC TR 13335-1:1996 y la ISO/IEC TR 13335-2:1997 fueron reemplazadas, después de una revisión técnica por la primera edición de ISO/IEC 13335-1 del año 2004, la cual menciona conceptos y modelos generales de la gestión de la seguridad de la información.

La ISO/IEC 13335-2:2004 cuando fue publicada, canceló y reemplazó a la ISO/IEC TR 13335-3:1998 y a la ISO/IEC TR 13335-4:2000, debido a que provee una guía operacional sobre la seguridad de las TI, esbozando técnicas de gestión y medidas preventivas.

La ISO/IEC 13335 [13], puede ser usada como una guía para abordar problemas específicos de seguridad, relacionados a la pérdida de confidencialidad, integridad y disponibilidad de la información y servicios en las organizaciones, lo que genera un impacto negativo en éstas, es por esto que se hace necesario que se mantengan apropiados niveles de seguridad, para lo cual es indispensable la gestión de la misma.

1.1.3.3 RFC 2196. *Site Security Handbook* (Manual de Sitios Seguros)

La RFC 2196 [14], es un trabajo colectivo donde contribuyeron numerosos autores, creada en 1997, es una guía para el desarrollo de procedimientos y políticas de seguridad para sistemas informáticos que se conecten a Internet.

Su objetivo es proteger la información y los servicios, de tal forma que conserven las características principales de disponibilidad, confidencialidad e integridad. Para esto, esta guía identifica claramente qué es una política de seguridad, cuál es su propósito, quién debe establecerlas y quién debe seguirlas, así define una arquitectura concisa para la realización de adecuadas políticas de seguridad.

Dentro de los temas que más se destacan en esta guía son: formación y contenido de políticas, seguridad de redes y sistemas, manejo y respuesta a los incidentes de seguridad y análisis del riesgo.

Esta guía es muy útil para todos aquellos administradores de red que deseen implementar políticas de seguridad que se ajusten a sus sistemas o redes.

1.1.3.4 BS 7799 Sistema de gestión de seguridad de la información, lineamientos para gestión de riegos de seguridad de información

Normas creadas por el Instituto de Estándares Británico (BSI por sus siglas en ingles). Su origen se debe a la necesidad de las organizaciones en general de tener un referente común para gestionar de forma adecuada la seguridad de la información.

La primera parte (BS 7799-1) creada en 1995 como Código de Buenas Prácticas y revisada en 1999, es un conjunto de controles de seguridad y de metodologías para su correcta aplicación. En el año 2000 la ISO adopta y establece la norma como ISO/IEC 17799:2000, que desde entonces ha tenido reconocimiento a nivel mundial y posteriormente revisada y nombrada (BS 7799-1:2005) [15].

La segunda parte (BS 7799-2) creada en 1999 para ser certificable y auditable; posteriormente revisada en el 2002 (BS 7799-2:2002), contiene los principios para establecer un SGSI debidamente documentado y relacionado con los controles y objetivos de control dados en la primera parte. En el año 2005 la norma es revisada técnicamente y renombrada como BS 7799-2:2005 [16] e ISO/IEC 27001:2005 norma internacional certificable.

Luego de la publicación de la ISO27001:2005, en el 2006 BSI publicó la BS7799-3:2006 [17], centrada en la gestión del riesgo de los sistemas de información.

1.1.3.5 ISO/IEC 27001: 2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

El objeto de esta norma [2] es definir los requerimientos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La implantación de un SGSI bajo la guía de esta norma, permite a cualquier organización descubrir los activos de información de su negocio, para poder gestionar el riesgo y garantizar la seguridad de la información.

La norma tiene un enfoque en procesos; donde el resultado de una pequeña actividad en la organización sirve como insumo para realizar otra, esto permite la fácil adopción incremental del SGSI al entorno, requerimientos y objetivos de seguridad, propios de la organización cualquiera que sea el tamaño y tipo de negocio.

La norma se considera como una herramienta de gestión para la alta gerencia, es compatible con otros sistemas de gestión, es aceptada internacionalmente y es la única certificable. Además de ser el eje central de la familia de normas ISO 27000.

1.1.3.6 ISO/IEC 27002: 2005 (antes 17799: 2005) Tecnología de la Información Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

La primera edición (ISO/IEC 17799:2000) fue revisada técnicamente en el 2005, año donde es remplazada por la norma conocida como ISO/IEC 17799:2005 y que a su vez desde el 1 de Julio de 2007 se renombra como ISO 27002:2005 [3]; manteniendo el contenido y año de publicación formal de la revisión.

Esta norma está enfocada en servir como una guía general de buenas prácticas para crear, diseñar y seleccionar los objetivos de control y controles de seguridad. No es certificable.

Con la adecuada implementación de los controles, que incluyen políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware, la norma busca preservar los principios de confidencialidad, integridad y disponibilidad sobre la información.

1.1.3.7 ISO 9000 Sistemas de gestión de la calidad — Conceptos y vocabulario

Especifica los requisitos para la gestión de la calidad del producto o servicio que se ofrece. Este estándar internacional pretende que las organizaciones busquen el mejoramiento continuo, con el fin de ofrecer mejores productos o servicios y con ello aumentar la satisfacción del cliente [18].

1.1.3.8 TIA-942 Infraestructura de Telecomunicaciones – Estándar para centros de Procesamiento de Datos

Se encarga de brindar los requisitos que debe cumplir un centro de procesamiento de datos, en relación con la seguridad física de la información. La infraestructura global se divide en cuatro subsistemas: telecomunicaciones, arquitectura, eléctrico y mecánico; para los cuales se recomienda en detalle el diseño, la instalación, el sistema de cableado, factores de rendimiento, redundancia de equipos, independencia de fuentes de energía, gestión de alarmas entre otros [19].

Según el grado de disponibilidad de funcionamiento, el estándar clasifica a los centros de procesamiento de datos en cuatro tipos (tier I, tier II, tier III y tier IV). El aumento en el grado de disponibilidad implica que la información está protegida frente riegos humanos, del negocio, ambientales y catástrofes; a sí mismo el costo de construcción aumenta a mayor tier. El grado de tier es independiente a cada subsistema así que es posible evolucionar a una implementación más segura; teniendo en cuenta que la construcción de un centro de datos tipo 4 se concibe desde la planeación y construcción del edifico contenedor.

En complemento de los procesos de gestión de seguridad, el TIA-606ª propone un sistema de etiquetas para todos los componentes del centro de procesamiento de datos, tales como: cables, conectores, gabinetes, sensores, sistema eléctrico, racks entre otros.
La implementación de este estándar busca tanto proteger a los equipos de procesamiento de información, como también la integridad del personal y las instalaciones de la organización, ya que existen controles preventivos y correctivos; en caso de un desastre las vidas humanas prevalecen sobre los equipos y la información contenida en ellos. Para el caso anterior las copias de respaldo ya deberían estar protegidas en otro lugar.

1.1.3.9 Agenda Global de Ciberseguridad (GCA - *Global Cybersecurity Agenda*)

Iniciativa que surge en el desarrollo de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) respecto de la línea de acción C5 “Construir confianza y seguridad en

el uso de las TIC" [20]. La ITU es la organización que lidera el trabajo sobre esta línea de acción, por lo que en 2007 creó El Grupo de Expertos de Alto Nivel (HLEG - The High-Level Experts Group), personas de diferentes sectores y regiones, encargados de desarrollar un framework para cooperación internacional en ciberseguridad. La GCA fue publicada en el 2008 y propone el trabajo integrado alrededor de cinco áreas: medidas jurídicas, medidas técnicas y de procedimiento, la estructura organizacional, la capacidad de creación y la cooperación internacional [21], esto con el objeto de construir confianza y seguridad en la sociedad de la información.

1.1.3.10 PCI DSS. *Payment Card Industry. Data Security Standard* (Industrias de Tarjetas de Pago. Normas de Seguridad de datos)

PCI DSS [22] fue generada por el Security Standards Council el cual es conformado por American Express, Discover Financial Services, JCB, MasterCard Worldwide y Visa Inc. Las DSS de PCI definen requerimientos para la gestión de la seguridad, políticas, procedimientos y diversas medidas cuyo fin es reducir el fraude y aumentar la protección de los datos relacionados con la información de tarjetas de crédito o débito; las deben cumplir los bancos, comercios y proveedores de servicio que almacenan, procesan o transmiten datos de los usuarios que realizan pagos por estos medios.
En Julio de 2009 se encontraba en su versión 1.2.1 y define 12 requisitos indispensables en 6 áreas: desarrollar y mantener una red segura, proteger los datos del titular de la tarjeta, desarrollar un programa de administración de vulnerabilidad, implementar medidas sólidas de control de acceso, supervisar y probar las redes con regularidad y mantener una política de seguridad de la información.

1.1.4 Metodologías

1.1.4.1 OSSTMM *Open Source Security Testing Methodology Manual* (Manual de la Metodología Abierta de Testeo de Seguridad)

EL OSSTMM [23] es una metodología de referencia para la realización de pruebas de seguridad, incluye lineamientos de acción, legislación sobre testeo de seguridad, un conjunto integral de pruebas y las normas éticas del evaluador.

El objetivo de este manual es crear un método aceptado para ejecutar una prueba de seguridad minuciosa, cabal, de forma ordenada y con calidad profesional, para ello menciona una serie de pasos y aspectos claves que se deben tener en cuenta en la realización de las pruebas desde el exterior hasta el interior del área de testeo de seguridad.

Plantea seis secciones: Seguridad de la Información (SI), Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física, además provee una serie de reglas y lineamientos que dan claridad sobre cuándo, qué y cuáles eventos deben ser analizados en cada una de estas secciones.

En la revisión 2.5 del OSSTMM se incluyó los Valores de la Evaluación del Riesgo o RAVs (*Risk Assessment Values*) por sus siglas en inglés, que se definen como la evaluación del riesgo sobre un ciclo de vida específico para pruebas periódicas, es decir, es posible realizar pruebas específicas en periodos de tiempo determinados que se tornan cíclicos minimizando los riesgos.

Es importante contar con una metodología como ésta, que se basa en las mejores prácticas y en un conceso a nivel mundial, lo que reduce tener supuestos y por consecuencia pruebas mal elaboradas, que pierden de vista los detalles importantes que generalmente son los que llevan a fallas de seguridad.

1.1.4.2 OSSIM *Open Source Security Information Management* (Gestión de Seguridad de Información de Código Abierto)

Cuatro españoles que se autodenominaban hackers éticos, crearon una herramienta de seguridad de licencia libre llamada OSSIM [24].

OSSIM es una herramienta de monitorización de seguridad para administradores de red, agrupa más de 15 programas de código abierto con la tecnología necesaria que permite realizar control sobre la red, gestionando la información desde un punto central; al integrar programas libres no es necesario preocuparse por el desarrollo de estos, puesto que cada uno de ellos cuenta con una comunidad que los perfecciona.

Las tres características más relevantes de OSSIM se mencionan a continuación:

Abstracción: Implementa procesos de abstracción que convierten millones de pequeños eventos de difícil comprensión en decenas de alarmas totalmente comprensibles.

Reducción de Falsos Positivos: La correlación permite chequear todos los eventos, de esta forma se encuentran los falsos positivos y se asegura de cuáles son ataques reales y cuáles no.

Gestión del Riesgo: Todas las respuestas se encuentran basadas en parámetros del riesgo, así el riesgo es calculado y almacenado para cada evento individual.

De esta forma es como OSSIM cubre el ciclo de vida completo de la Gestión de Seguridad.

1.1.4.3 Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP)

El proyecto OWASP [25] en general está constituido como una fundación sin ánimo de lucro, donde sus miembros se unen libremente a la comunidad y los aportes de trabajo o conocimiento son voluntarios. El objetivo de interés es crear documentos, guías, manuales, metodologías, herramientas y en general soluciones que permitan detectar y corregir las causas que hacen una aplicación web insegura.

Las prácticas bajo los principios de OWASP, son reconocidas y recomendadas, ya que el trabajo de calidad e impacto es un aporte a la actividad académica y productiva del mundo. Dentro de los proyectos más importantes y que apoyan el objeto de investigación están:

Proyecto OWASP Top Ten (OWASP *Top Ten*)
Este proyecto ha publicado en dos ocasiones en el 2004 y el 2007 [26] la lista de las diez vulnerabilidades de seguridad más críticas de las aplicaciones web. La estadística se basa en los eventos analizados y recolectados durante el periodo de estudio y la clasificación del anterior año. Cada vulnerabilidad se estudia, se detecta su causa o causas y se propone las estrategias de solución.

El objetivo de la lista es informar e ilustrar principalmente a diseñadores y desarrolladores, las prácticas comunes que generan estas vulnerabilidades, como el impacto de sus consecuencias al pasarlas por alto y las mínimas medidas de protección frente a éstas.

Proyecto Guía de Pruebas OWASP (OWASP *Testing Guide*)
Propone el framework [27] de pruebas de OWASP, que tiene como fin abordar la seguridad de las aplicaciones web en todo el ciclo de vida del desarrollo de software (SDLC siglas en inglés), para detectar en tiempo presente vulnerabilidades de la aplicación y evitar en el futuro pérdidas de tiempo y recursos. La metodología propuesta explica en detalle el alcance, los principios y las técnicas de evaluación.

Esta guía de pruebas da a las organizaciones un marco de trabajo para crear y a su vez probar sus aplicaciones web de forma segura, como también diseñar nuevas pruebas de evaluación o uso, acordes a sus necesidades y lógica propia del negocio; que es a partir de donde se originan las nuevas vulnerabilidades. No está propuesto para ser una lista de comprobación.

Proyecto Guía Para Construir Aplicaciones Web Y Servicios Web Seguros (*A Guide to Building Secure Web Applications and Web Services*)

Proyecto [28] dirigido a desarrolladores, jefes de proyecto, equipos de seguridad y personal relacionado con el desarrollo de aplicaciones web. Esta guía pretende enseñar a

corregir las malas prácticas de codificación, mostrando los procesos de seguridad que se deben tener en cuenta para evitar las vulnerabilidades más comunes, modelar amenazas correctamente, revisar código y elaborar pruebas. El contenido de cada temática contiene objetivos, teoría, buenas prácticas, análisis de vulnerabilidad y medidas de protección. Es un documento centrado en el desarrollo que utiliza los leguajes de programación J2EE, PHP, ASP.NET como muestra de los más conocidos.

1.1.4.4 Marco de Evaluación de Seguridad de Sistemas de Información (ISSAF)

Es un marco de trabajo para evaluar la seguridad de la información en las empresas, respecto de sus requerimientos organizacionales. Como metodología abierta trabaja con voluntarios del mundo especialistas en seguridad de la información. La evaluación de seguridad quiere ser completa y eficiente detectando las posibles vulnerabilidades y dando a entender los riegos que se tiene antes de tomar medidas de gestión; para que estas mismas medidas se ajusten a los escenarios reales de impacto [29].

Se utilizan Criterios de evaluación definidos para cada sección o área que se está analizando. Estos criterios tienes objetivos a cumplir, prácticas comunes, tareas adicionales, precauciones y mejores prácticas.

1.2 Sistemas de Pagos en Línea

1.2.1 Definición

Un SISTEMA DE PAGOS es *"Un conjunto organizado de políticas, reglas, acuerdos, instrumentos de pago, entidades y componentes tecnológicos, tales como equipos, software y sistemas de comunicación, que permiten la transferencia de fondos entre los participantes, mediante la recepción, el procesamiento, la transmisión, la compensación y/o la liquidación de órdenes de transferencia y recaudo"* [30]. El sistema de pago en línea forma parte del comercio electrónico y es el que permite transferencias de dinero a través de Internet. La OECD define una transacción electrónica como "*la compra/venta de bienes/servicios, ya sea entre empresas, familias, individuos, gobiernos u otras organizaciones, públicas o privadas, realizadas a través de medios telemáticos*" [31].

En Colombia para estos sistemas de pago se crearon dos cámaras de compensación [30], CENIT Y ACH Colombia S.A, el responsable de la primera es el Banco de la República y se utiliza para pagos de bajo valor del sector público, a través de éste se realizan los pagos a proveedores del gobierno central [32]; la segunda fue implementada en 1997 por los intermediarios financieros afiliados, opera a través de una red privada y se utiliza para

pagos entre individuos y empresas [33]. CENIT y ACH Colombia abrieron en el país la posibilidad de realizar transacciones electrónicas como pago de nóminas, pensiones y proveedores y bienes y servicios en general. Los pagos por Internet son intrabancarios, es decir los fondos se toman de la cuenta de ahorros o corriente del usuario y se transfieren a la cuenta bancaria de la empresa, en Colombia se han desarrollado iniciativas para fortalecer este campo, todas enmarcadas en ACH único autorizado en el país para dichas transacciones, es por ello que ACH desarrolló el SOI (Servicio Operativo de Información) de acuerdo en lo establecido en el Decreto Ley 1465 de Mayo 10 de 2005 [34], como un servicio de pago electrónico integrado de aportes a la seguridad social y parafiscales donde el aportante puede realizar la liquidación de su pago y a la vez descontarlo de su cuenta bancaria.

Dentro del sistema de pago en línea se pueden efectuar pagos y recaudos, esto dependiendo de los actores que intervienen, de esta forma se tomará como sistema de pago la transacción realizada por el usuario para realizar un pago a la empresa y como sistema de recaudo las operaciones realizadas por la empresa para recibir el dinero.

1.2.2 Generalidades

Dentro del comercio electrónico existen dos modalidades: indirecto y directo, el primero es cuando el pedido se hace electrónico y la entrega del bien o servicio de manera física, indiferentemente de la forma de pago. El segundo es cuando el pedido, el pago y la entrega se hacen en línea [35].

Además, según los actores que intervienen en la transacción electrónica de compra y venta de bienes y o servicios, el comercio electrónico se clasifica en [36]:

- Empresa-Empresa (B2B *Business to Business*): Transacciones de compra venta de bienes/servicios entre empresas. Comúnmente denominado venta al por mayor.
- Empresa-Consumidor (B2C *Business to Consumer*): Es el más popular y se trata de transacciones de compra venta de bienes/servicios entre la empresa y el consumidor final.
- Empresa-Gobierno (B2G *Business to Government*) y Consumidor-Gobierno (C2G *Consumer to Governmnet*): Comercio que se realiza desde el gobierno a empresas o particulares como trámites administrativos, declaración y pago de impuestos, entre otros.
- Empresa-Empleado (B2E *Business to Employer*): Relación que establece la empresa con sus empleados para transacciones como facturación de ventas, de comisiones, gastos de desplazamiento, entre otros.
- Consumidor-Consumidor (C2C *Consumer to Consumer*): Son las transacciones privadas de consumidores, se pueden realizar por ejemplo por correo electrónico o tecnologías p2p.

Entre las ventajas del pago en línea para los usuarios se destacan la flexibilidad de horarios, se pueden realizar transacciones las 24 horas durante los 7 días de la semana desde cualquier lugar que tenga conexión a Internet, por lo que no es necesario desplazarse al banco, hacer largas filas, ahorrando así tiempo y dinero en gasolina o transporte. Desde la comodidad de la casa u oficina se puede realizar compras y pagos con confirmación en línea de la transacción y con acceso a millones de establecimientos de comercio en todo el mundo en donde se puede hacer compras de forma segura. El sistema de recaudo para las empresas genera ventajas competitivas ya que brinda a sus usuarios una posibilidad más para realizar los pagos lo que genera mayor comercialización de sus productos y/o servicios, mayor velocidad e información en línea de los recaudos, eficiencia en sus procesos productivos, seguridad en el manejo de la información y el dinero y reducción de costos.

Uno de los retos más importantes del sistema de pago en línea es generar confianza en los usuarios para que ellos realicen cada vez más transacciones sin miedo a sufrir un robo o desfalco, para esto también es necesario aumentar la seguridad pues es la desventaja más significativa de los sistemas de pago en línea, ya que este tipo de transacciones se encuentran expuestas a diferentes amenazas que se describirán más adelante en este capítulo.

Las tecnologías de la información y a su vez el comercio electrónico son cada vez más usadas como estrategias de negocio que aumentan la productividad y las ventajas competitivas, es por ello importante mirar algunas estadísticas de la penetración y evolución de éstas en Colombia y el mundo.

Los usuarios de Internet por regiones del mundo según la *Internet World Stats* [37] se muestran en la siguiente tabla:

Tabla 1. Usuarios de Internet por Regiones del Mundo
Fuente: Internet World Stats

Regiones	Usuarios 2009	% Población (Penetración)	Crecimiento 2000 – 2009	% de Usuarios
África	991.0052.342	6.7%	1359.9%	3.9%
Asia	3.808.070.503	18.5%	516.1%	42.2$
Europa	803.850.858	50.1%	282.9%	24.2%
Medio Oriente	202.687.005	23.7 %	1360.2%	2.9%
Norte América	340.831.831	73.9%	132.9%	15.1%
América Latina / Caribe	586.662.468	30.0%	873.1%	10.5%
Oceanía / Australia	34.700.201	60.1%	173.4%	1.2%
TOTAL	6.767.808.208	24.7%	362.3%	100.0%

En Colombia según el DANE [38] y tomando una muestra de 13.600 hogares aproximadamente se tuvieron los siguientes resultados.

En 2003 y 2008 Bogotá registró el mayor porcentaje de hogares con conexión a Internet y la Región Pacífica el menor (Figura 3).

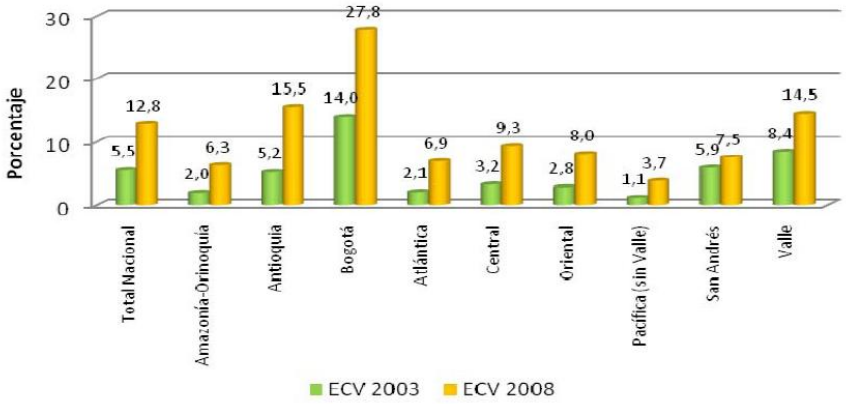


Figura 3. Porcentaje de hogares con conexión a Internet.
Encuesta de Calidad de Vida 2003 y 2008.
Total Nacional y Regiones
Fuente: DANE – Encuesta de Calidad de Vida 2003 y 2008

rango de edades las personas que más usaron el computador entre julio y diciembre de 2008 están entre los 12 años y los 24 años de edad, observándose además que el nivel educativo es directamente proporcional con el uso del computador (Figuras 4 y 5). Estos rangos se comportan de una forma similar para el uso de Internet (Figuras 6 y 7). Es importante resaltar que las personas que se encuentran dentro de estos rangos, son los usuarios potenciales para el mercado del SPEL.

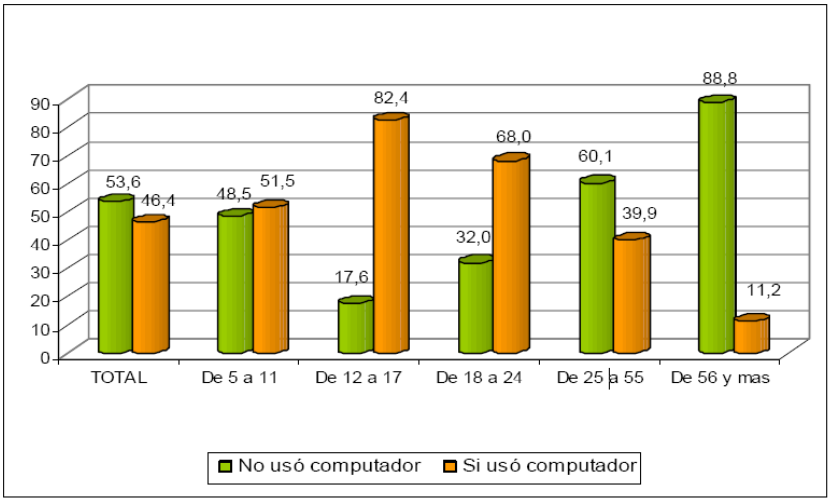


Figura 4. Caracterización de las Personas que usaron / no usaron computador por rangos de edad, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

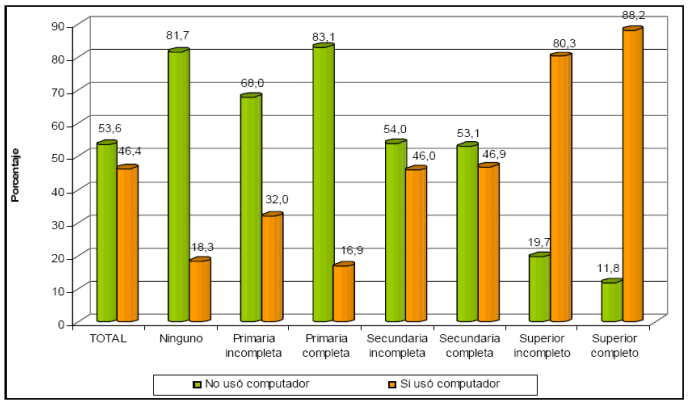


Figura 5. Caracterización de las Personas que usaron / no usaron computador por nivel educativo. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

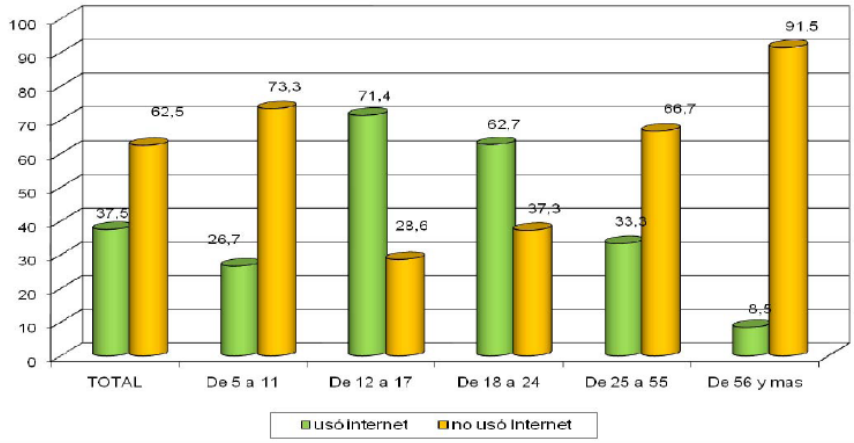


Figura 6. Porcentaje de Personas que usaron Internet (en cualquier lugar) por rangos de edad, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

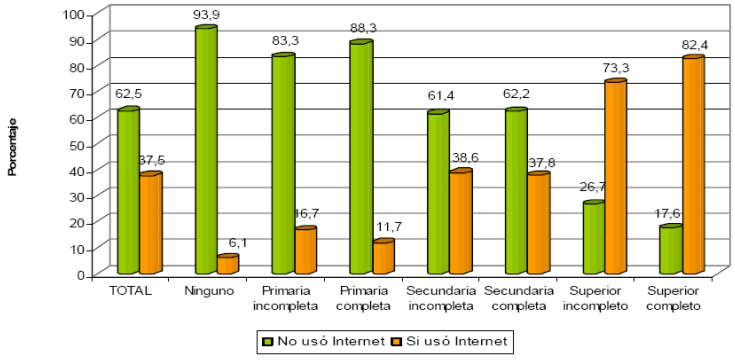


Figura 7. Porcentaje de Personas que usaron Internet (en cualquier lugar) según nivel educativo, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

Los lugares de acceso a Internet más utilizados fueron los de acceso público (Figura 8) y la actividad principal para la cual se utilizó Internet fue la búsqueda de información con un 92% (Figura 9), la banca electrónica un 10.9% y compra de productos y servicios el 5.9 %. Cartagena (10.3), San Andrés y Bucaramanga fueron las ciudades donde más se utilizó Internet para este propósito (Figura 10), Popayán tan solo tiene un 2.4%.

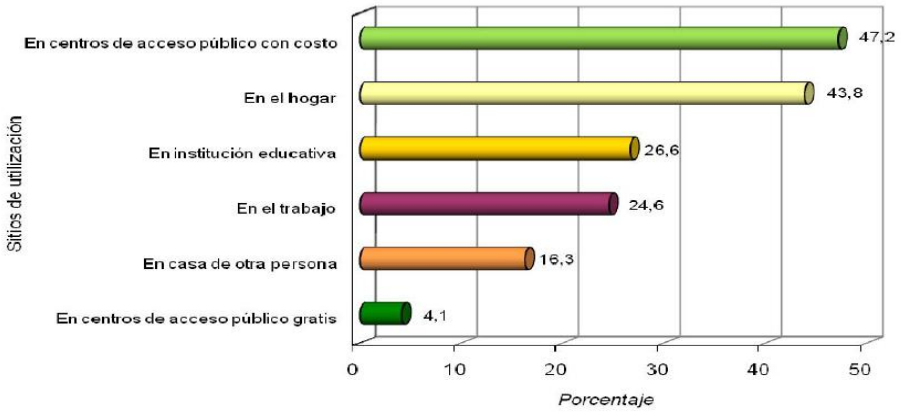


Figura 8. Porcentaje de Personas que usaron Internet según su sitio de utilización, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

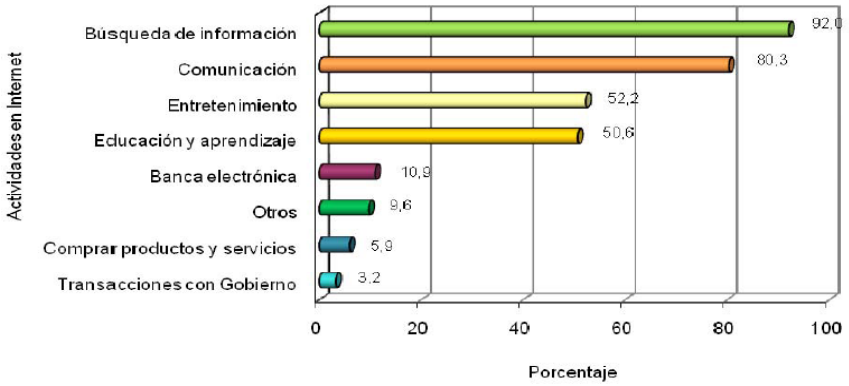


Figura 9. Porcentaje de Personas que usaron Internet según los servicios o actividades para los cuales lo utilizaron, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

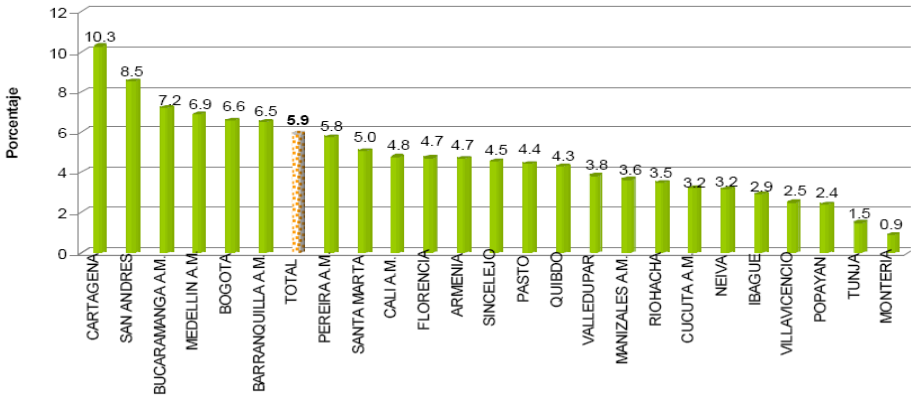


Figura 10. Porcentaje de Personas que usó Internet para comprar u ordenar productos o servicios, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

Para banca electrónica las ciudades donde más utilizaron estos servicios fueron Medellín (14.1 %) y Bogotá (12.9%), Popayán tuvo un 2.7%, es decir que la utilización de Internet para compra de productos y banca electrónica es muy baja.

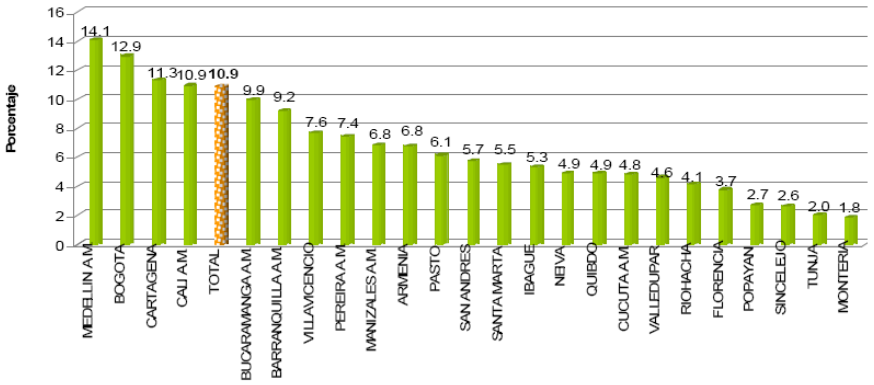


Figura 11. Porcentaje de Personas que usó Internet para banca electrónica u otros servicios financieros, 24 ciudades y áreas metropolitanas. Julio - Diciembre 2008
Fuente: DANE – Gran Encuesta Integrada de Hogares

De acuerdo a las figuras anteriores se puede notar que el auge del uso del computador e Internet ha ido creciendo paulatinamente, esto demuestra que las personas cada vez más hacen uso de estos medios ya sea para diversión, consulta de información o transacciones bancarias. En Colombia los pagos en línea han tenido un crecimiento moderado (Figura 12), una de las causas principales de esto es la cultura colombiana, las personas se encuentran acostumbradas a realizar sus compras y pagos físicamente, además desconfían de la seguridad del sistema de pagos. Para que el comercio electrónico crezca en el país, se debe generar confianza al colombiano para que se sienta seguro de que una compra o pago electrónico puede ofrecer las mismas garantías que

uno físico, infortunadamente los bancos nacionales no hablan de forma positiva en los medios de comunicaciones de este tipo de transacciones, se habla del virus, de la nueva modalidad de robo, suplantación de identidad, entre otros, pero no de las mejoras en el sistema o de los nuevos comercios que ahora ofrecen más y mejores servicios para los clientes que compren en línea. Se debe crear la conciencia de que el comercio electrónico promueve la competitividad, inversiones en innovación y crecimiento en la industria lo cual trae progreso al país.

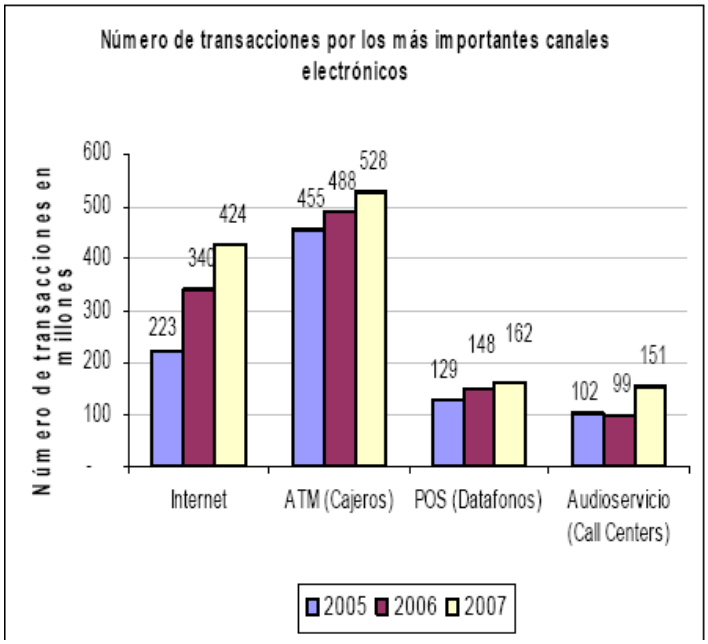


Figura 12. Número de Transacciones por los más importantes canales electrónicos
Fuente: Asobancaria. [39]

1.2.3 SPEL - PSE

1.2.3.1 Descripción General

El Proveedor de Servicios Electrónicos PSE [40],[31] desarrollado por ACH Colombia S.A.[33], es un sistema centralizado y estandarizado que permite a las empresas ofrecer a los usuarios la posibilidad de realizar pagos, accediendo a sus recursos desde la entidad financiera donde tienen su dinero.

ACH Colombia S.A es la única red autorizada en Colombia para efectuar los pagos entre individuos y empresas, por tanto el SPEL debe basar su funcionamiento en el PSE, para ello es necesario que la empresa, en este caso las Universidades Públicas, tengan un convenio con ACH para ofrecer el servicio de pagos en línea y así utilizar la red ACH.

1.2.3.2 Modelo Operativo PSE

El modelo de operación del PSE se encuentra dividido en 4 partes [41]: Registro, Pago en línea, Aplicación y Compensación de Fondos y Conciliación

A. Componente de Registro

Para poder operar el pago en línea, las Empresas y las Entidades financieras deben firmar acuerdos con el PSE donde establezcan todas las reglas de negocio, por tanto el objetivo de este componente es permitir la inscripción de estos actores.

Este componente tiene dos procesos: un procedimiento operativo donde se firman los acuerdos y uno electrónico donde las empresas y las entidades financieras se registran en el PSE dando la información necesaria para administrar todos los procesos del pago en línea.

B. Componente Pago en Línea

El objetivo de esta transacción es realizar en línea procesos como: identificación y autenticación del usuario ante su entidad financiera, aceptación o rechazo del pago, información a los actores del resultado de la transacción.

En el pago en línea interactúan cuatro elementos (Usuario, PSE, Entidad Financiera y Comercio) como se muestra en la figura 13:

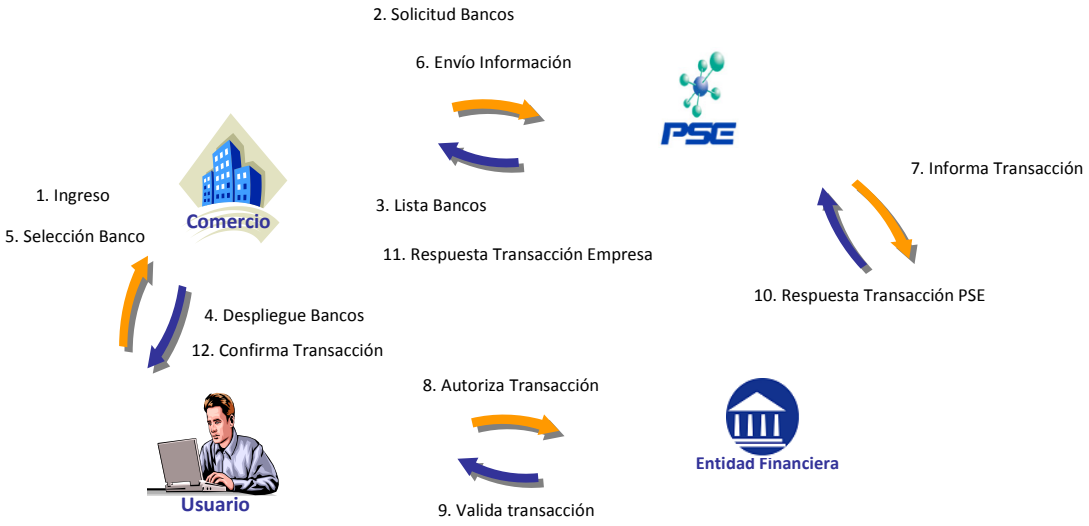


Figura 13. Proceso de Pago en Línea
Fuente: ACH Colombia S.A. [33]

1. El usuario (estudiante o padre de familia que realiza el pago) entra al sitio de la Empresa (Universidad), escoge el servicio o producto y selecciona la opción pagar. La liquidación del pago y el valor a pagar es responsabilidad de la empresa quien determina si se pueden hacer pagos parciales o no.
2. La empresa solicita al PSE mediante un Servicio Web, la lista de Entidades Financieras afiliadas al PSE.
3. El PSE retorna la lista de Entidades Financieras afiliadas al PSE.
4. La empresa presenta al usuario la lista de Entidades Financieras.
5. El usuario selecciona el banco del cual desea realizar el pago**.**
6. La empresa llama al Servicio Web del PSE para iniciar la transacción y envía la información del pago y el banco seleccionado.
7. El PSE registra en su base de datos esta transacción y envía mediante un Servicio Web la información a la Entidad Financiera.
8. La Entidad financiera con esta información inicia una transacción y asigna un identificador único con el cual la empresa direcciona al usuario a una dirección URL donde encuentra la información exacta de la transacción que inicio y la efectúa.
9. La Entidad Financiera realiza la autenticación y validación del Usuario, efectúa la verificación del saldo de la cuenta y aprueba o niega la transacción. La autenticación del usuario y la autorización del pago es responsabilidad de la Entidad Financiera.
10. La Entidad Financiera retorna el Servicio Web al PSE con el resultado de la transacción.
11. El PSE envía el Servicio Web a la empresa que envió la solicitud con la respuesta de éxito o fracaso de la transacción.
12. El usuario migra al sitio Web de la Empresa la cual le confirma el resultado de la transacción.

La entidad financiera que da la autorización debe afectar el saldo disponible del cliente y se hace responsable de hacer la compensación ante ACH COLOMBIA y transferir el dinero a la entidad financiera recaudadora. El pago es exitoso ante el usuario y la empresa si se cumple el proceso descrito en la figura 13.

Si durante el proceso del pago en línea se pierde la comunicación antes de la confirmación de la transacción, el PSE después de un tiempo predeterminado solicitará al Web Service de la Entidad Financiera por el estado de la transacción y así actualizar su base de datos.

El PSE utiliza un servicio Web desarrollado en .NET (*ASP.NET Web Service*) [42], contiene WSE (*Web Services Enhancements*) para la seguridad, además tiene *tokens* (llaves privadas generadas a partir del certificado digital) para asegurar el contenido de los Servicios Web.

C. Componente Aplicación y Compensación de Fondos

El objetivo de este modelo es la compensación de fondos que hace ACH COLOMBIA debido a los pagos en línea exitosos. Dentro de este modelo se realizan dos procesos: Cobro a las Entidades Financieras Autorizadas y Pago a las Entidades Financieras Recaudadoras.

El Cobro a las Entidades Financieras Autorizadas lo hace ACH COLOMBIA a cada una de los bancos donde el usuario hizo la transacción, le envía un archivo en formato NACHA-m[1] [43] para descontar de la Entidad Financiera el valor de la transacción y transferirlo a ACH COLOMBIA.

El Pago a las Entidades Financieras Recaudadoras lo hace ACH COLOMBIA mediante un archivo en formato NACHA-m, donde se transfiere el valor de la transacción del pago en línea desde ACH COLOMBIA a la Entidad Financiera donde la Empresa tiene la cuenta.

D. Componente de Conciliación

Es un proceso de conciliación que le permite a las Empresas y a las Entidades Financieras verificar la realización correcta de los pagos en línea; para eso el PSE genera dos archivos de conciliación uno donde detalla cada una de las transacciones realizadas (conciliación transaccional) y otro por totales (conciliación financiera).

El archivo de conciliación para las Empresas contiene la información de la totalidad de las transacciones realizadas y para las Entidades Financieras detalla cada una de las transacciones realizadas y su estado, es decir, si fueron exitosas, fallidas o están pendientes.

Las empresas o entidades financieras pueden en cualquier momento consultar información de las transacciones y monitorear los procesos.

[1] Formato adoptado al contexto Colombiano del Formato Nacha, el cual es un formato establecido por la Asociación Nacional de Cámaras de Compensación Automatizadas de Estados Unidos y establece los procedimientos para un pago en línea.

1.2.3.3 Arquitectura del PSE

La infraestructura de red necesaria para el SPEL se ve en la siguiente figura:

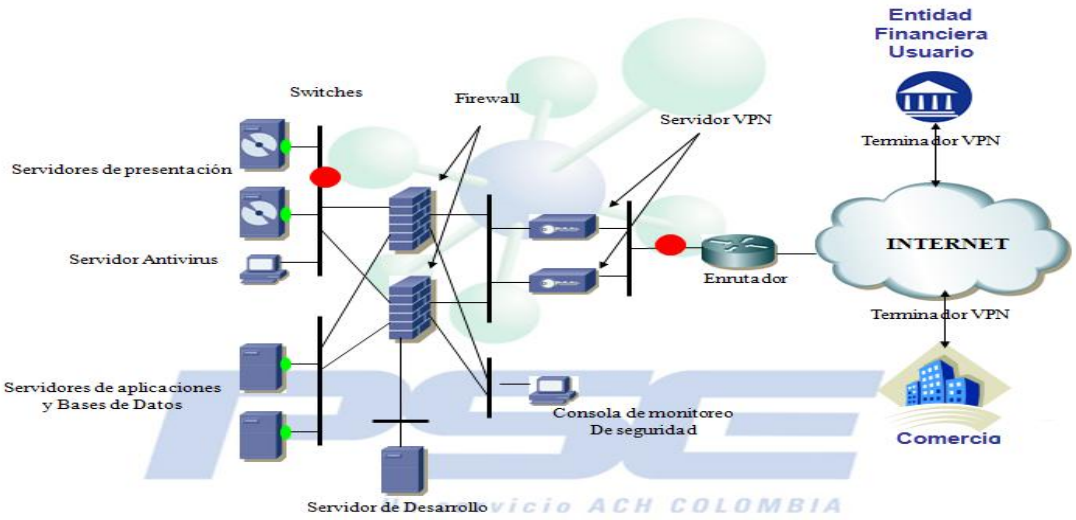


Figura 14. Arquitectura PSE
Fuente: ACH Colombia S.A. [33][41] [41]

A. Componentes Hardware

Para tener comunicación con el PSE es necesario contar con:

Terminador, Router o Firewall de VPN's
Terminador que permite establecer un par de VPN's hacia el nodo de PSE (una principal y otra de backup), además permite las conexiones seguras a través de Internet entre las empresas y las entidades financieras. Inicia y negocia la comunicación de los túneles encriptados que terminan en el concentrador de VPN's del PSE el cual recibe las conexiones de Internet que requieran comunicarse con él. El terminador debe contar con las características estándares de seguridad y confiabilidad.

Firewall
Fundamental para el aseguramiento de redes y comunicaciones de la Entidad Financiera, la seguridad física, de red y aplicaciones es responsabilidad de las empresas y entidades financieras.

Enlace a Internet
Es necesario para acceder a los servicios del PSE ya que por este medio viajara toda la información encriptada. Debe contar con una dirección pública en Internet para poder conectar el servidor Web donde se encuentra su sitio.

Métodos de Autenticación
Se puede usar dos métodos: Autenticación por medio de PRE-SHARED KEY o Autenticación por medio de Certificados Digitales emitidos por Certicámara.

Además la empresa debe contar con:

- Direcciones IP públicas de terminador VPN.
- Dirección IP del servidor Cliente de PSE en la Empresa
- Dirección IP de navegación a Internet de la Empresa
- URL del portal de la Empresa
- Formato de Registro ante PSE diligenciado.
- Plataforma a trabajar (Sistema Operativo, Servidor Web, Servidor de Aplicaciones, Lenguaje de Desarrollo)

B. Componentes Software

El PSE implementa varios recursos para garantizar la seguridad de todos sus procesos como:

- Autenticación basada en IP/Certificado.
- WS-Security – extensión de seguridad para mensajes SOAP.
- VPN – para conectarse al PSE a través de un VPN criptografiado.
- SSL – https, que suministra seguridad en nivel de transporte (TCP).

Autenticación basada en IP Certificado
Este certificado es usado por el PSE para autenticar cual empresa o entidad financiera es la que está haciendo la llamada al PSE. Cada debe institución debe tener una lista de las direcciones IP con las que va a acceder al servicio web y el mensaje debe contener el certificado seleccionado, por lo tanto el PSE solo acepta llamadas de estas IP y que contengan certificados validos.

WS-Security

WS-Security (WSS) [44] fue originalmente desarrollado por IBM, Microsoft y Verisign, ahora este protocolo es desarrollado por el comité Oasis Open [45], contiene especificaciones sobre cómo debe garantizarse la integridad y seguridad en mensajería de Servicios Web.

WS-Security es una capa de software que suministra mecanismos de seguridad como firma digital y criptografía en nivel de mensajes SOAP [46], esto permite la integridad y confidencialidad de los mensajes, además se puede incluir tokens de seguridad en ellos. Se implementa en el ambiente .NET, en el paquete WSE.

SSL

Desarrollado por Netscape, en 1995 sale la versión SSL 3.0 [47], la cual desde entonces se ha caracterizado por ser un estándar seguro para las comunicaciones cliente servidor que trabaja sobre el protocolo TCP ya que proporciona autenticación y privacidad de la información en los extremos de la comunicación.

1.3 Contexto de las Universidades Oficiales de Colombia

1.3.1 Definición

Tanto por la ley 115 de 1994 “Por la cual se expide la Ley General de Educación”, artículo 35 [48] y la ley 30 de 1992 "Por la cual se organiza el servicio público de la educación superior", artículo 16 [49], las instituciones de educación superior según el carácter académico se clasifican en:

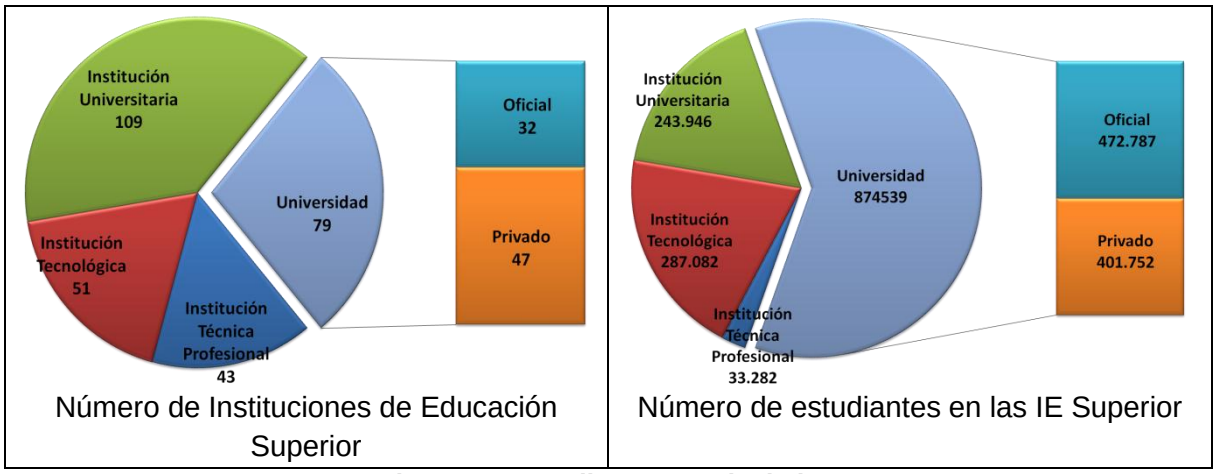
Tabla 2. Clasificación Instituciones de Educación Superior

	Definido en:
a. Instituciones técnicas profesionales.	Ley 30 de 1992 articulo 17 [49]. Ley 749 de 2002 articulo1[50].
b. Instituciones tecnológicas.	Ley 749 de 2002 articulo2 [50].
c. Instituciones universitarias, o, escuelas tecnológicas.	Ley 30 de 1992, articulo 18 [49]. Ley 115 de 1994, articulo 213 [48].
d. Universidades.	Ley 30 de 1992, articulo 19 [49].

Y según la razón de su origen las instituciones de educación superior se clasifican en: estatales u oficiales, privadas y de economía solidaria (ley 30 articulo 23) [49].

Para el desarrollo de este trabajo de grado el grupo de interés de instituciones de educación superior son las Universidades Oficiales del país, las que conforman el Sistema Universitario Estatal (SUE).

Según el Sistema Nacional de Información de Educación Superior (SNIES) en Colombia existen 32 Universidades Oficiales con aproximadamente 472.787 estudiantes matriculados en el 2008.



Número de Instituciones de Educación Superior

Número de estudiantes en las IE Superior

Figura 15. Estudiantes Matriculados
Fuente: MEN-SNIES. [51]

Por otra parte, el fin fundamental de una Universidad es promover el desarrollo de la región y por ende del país a partir de la formación integral de las personas que asisten a ella y más el fin de una Universidad Pública es permitir este beneficio a las personas de bajos recursos para mejorar la calidad de las mismas.

1.3.2 Contexto administrativo y tecnológico

Administrativamente las Universidades Estatales son entes autónomos y que pertenecen a un régimen especial (Art 57 Ley30 de 92) que les otorga personería jurídica (son empresas) y que el régimen financiero entre otros está sujeto a los acuerdos de ley estatal.

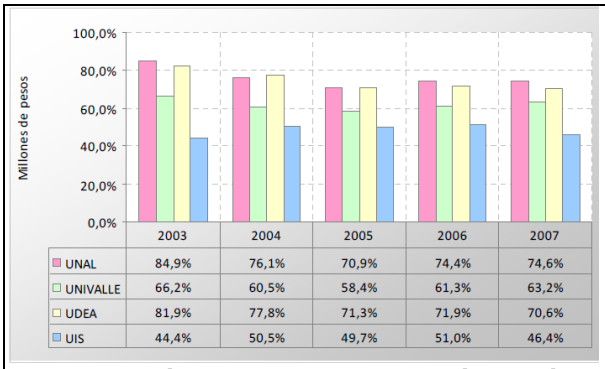
Económicamente la Universidad Publica sustenta sus gastos de funcionamiento: por las partidas asignadas del presupuesto nacional, los valores por matriculas, cursos y derechos y los bienes mueble e inmuebles que posee y los que adquiera así como sus frutos y rendimientos (Art 85 Ley30 de 92).

Teniendo en cuenta que a partir de la aplicación de la ley 30 de 1992 los aportes de la nación se hacen a pesos constantemente y que por normas establecidas por el Congreso de la Republica se obliga a las Universidades Oficiales a cubrir de sus propios recursos aspectos como: descuentos en matriculas para sufragantes, prestaciones sociales de

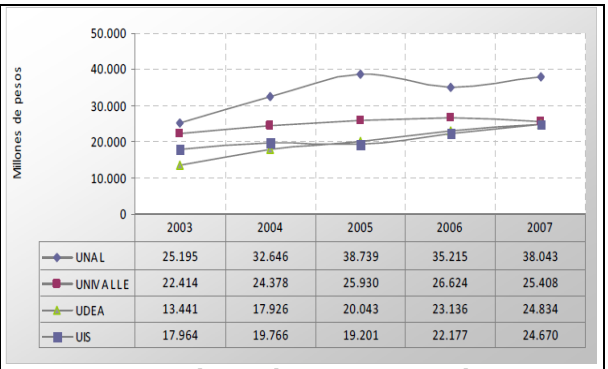
docentes ocasionales, de cátedra y personal supernumerario, procesos de acreditación y certificación, gastos general con ítems por encima del IPC y sostenibilidad de la infraestructura física y tecnológica [52] y por otra parte la política educativa estatal propone mejorar la calidad de la educación incrementado el número de estudiantes de pregrado, generando nuevos grupos de investigación, docentes cualificados y generando impacto en el contexto regional empresarial.

Cabe resaltar como los procesos de gestión institucional se han ajustado y refinado para ser más eficientes en el aprovechamiento de los recursos, permitiendo mantener las universidades estatales y mejorar los aspectos de los indicadores de evaluación institucional, pero a pesar de este esfuerzo como lo han dado a conocer y sentir los miembros del SUE, el sistema educativo estatal esta en el límite, donde técnicamente no se puede ofrecer mejores condiciones a la educación de los universitarios sin deteriorar la calidad de la misma.

Las cuatro universidades estatales con el mayor número de estudiantes y las más complejas también son: Universidad Nacional de Colombia (UNAL), Universidad de Antioquia (UDA), Universidad Industrial de Santander (UIS) y Universidad del Valle (UNIVALLE). En la siguiente figura comparativa lo que es de interés resaltar es el aspecto económico de las mismas, fuentes de ingresos como son los aportes de la nación y las matriculas [53] y no el hecho de que estas universidades son diferentes a las que se pretende analizar la información del SPEL (Las tres universidades oficiales que participaron como fuentes información son: Unicauca, Udenar y Univalle).



Porcentaje De Los Aportes Del Estado Respecto Al Total De Ingresos



Ingresos Financieros Generados Por Matriculas (Millones De Pesos Corrientes)

Figura 16. Comparación Ingresos Financieros Universidades Públicas
Fuente: Universidad del Valle. [53]

Así es como a pesar de que por ley los recursos destinados a las universidades deben ir en aumento, realmente los aportes del estado respecto del total de los ingresos de una universidad de forma general van en decremento; por lo menos en 3 de las 4 universidades de la figura. Y los ingresos por conceptos de matriculas del estudiantado se incrementa con los años.

La realidad es que existen recursos limitados y la política estatal busca el auto sostenimiento de la empresa universidad. Además que la anterior debe propiciar los espacios para el acceso a la sociedad del conocimiento e información; de principio en la dotación de salas de computadores con acceso a internet en su gran mayoría y principalmente asignar los recursos para la gestión de los recursos informáticos. Así es como las inversiones en la infraestructura tecnológica se realizan, pero pocas veces se piensa en su sostenimiento y los riesgos asociados sobre la información que se transporta sobre ella.

Dentro de cada universidad existe por lo menos una oficina o lugar que se encarga de todo lo relacionado con las tecnologías de información y comunicación TIC, como un servicio para su funcionamiento. Estas dependencias de la universidad existen o se crean según las funciones y responsabilidades que se necesiten en la institución, como por ejemplo: el área encargada de hacer mantenimiento físico a los equipos tecnológicos de la universidad pude ser computadores, equipos de comunicación, equipos de laboratorio, el área que mantiene las redes informáticas en correcto funcionamiento, el área encargada de los sistemas de información administrativa, el área encargada del desarrollo software adecuado a la universidad, el área que da el servicio de internet, correo electrónico entre otros a los estudiantes. Como se evidencia son diversas las necesidades respecto de la infraestructura tecnológica de una universidad, esto depende de la estructura administrativa interna asociada a su complejidad y cantidad de estudiantes.

En el caso de la Universidad del Cauca existe la División de Sistemas que es el ente centralizado para la distribución del trabajo en las diferentes áreas. Por otro lado en la Universidad de Nariño existen 2 dependencias una que se encarga de los servicios relacionados a los estudiantes y otra de los servicios administrativos de la universidad. En el caso de la Universidad del Valle cuenta con una Oficina de Informática y Telecomunicaciones la cual da soporte en este tema a toda la Universidad.

El gran número de computadores y más el número de usuarios (estudiantes, docentes y administrativos) hace que las redes internas de las universidades se comporten como una plataforma para el despliegue de infecciones y también en un laboratorio de ataques informáticos, convirtiéndose la intranet en una amenaza en sí misma para el bienestar informático institucional si no se gestiona adecuadamente. La universidad debe entender la apropiación de los recursos públicos como una comunidad universitaria donde el sostenimiento depende del buen uso cada persona le dé a los recursos en cargo.

Las oficinas de TIC se concentran en garantizar el correcto funcionamiento de los equipos que soportan los servicios de importancia para la universidad por lo general los servidores que se encuentran dentro del área desmilitarizada. La anterior zona se configura para proteger la red interna de la información que entra por los enlaces de internet. La seguridad de la red es flanqueada por los equipos de la intranet donde por ejemplo los estudiantes intercambian información entre los equipos institucionales y los equipos personales o externos que dependen de otro servicio de intranet y por ende con responsabilidad de los mismos usuarios. Así que los servicios de la universidad deben protegerse no solo de la cara a internet sino también de su propia red interna.

1.3.3 Sistemas de pago en línea en Universidades oficiales

Para recopilar información sobre SI y SPEL de las Universidades Oficiales colaboradoras (Udenar, Univalle y Unicauca), se realizó una encuesta (Ver Anexo D) a los directores o encargados de la Infraestructura tecnológica. Además se acordó confidencialidad con la información por lo cual no se exponen los resultados individuales en este documento.

Se debe tener en cuenta que al decir SPEL de Universidades Oficiales, se refiere a un SPEL que ha sido desarrollado por la Universidad misma y no como un servicio que la Institución pude contratar a un tercero para su desarrollo, gestión y mantenimiento.

En el proceso significativo de hacer eficientes los procesos administrativos asociados al funcionamiento de la Universidad como: registro y control de las matriculas, notas, préstamos de libros en bibliotecas, reserva de aulas informáticas, gestión de correspondencia, bienestar universitario, directorio institucional, contabilidad, entre muchos otros. La universidad ha pasado de realizar estos procesos manualmente a ir adquiriendo o desarrollando e implementado SW y HW para realizar estos procesos agiles y dinámicos soportados en infraestructuras tecnológicas e informáticas. Es así como por ejemplo el proceso de matrículas implicaba que los estudiantes entregaran un formato con las materias que desean cursar, esta información debe ser validada presencialmente y seguidamente autorizada, luego se genera un recibo de matricula a cada estudiante según cada situación, el estudiante recibe su recibo, debe pagarlo, llevar los comprobantes de pago, las dependencias cruzar información de quien ha pagado quien debe y finalmente autorizar o no al estudiante para recibir sus clases. Siguiendo el proceso evolutivo del ejemplo se crean sistemas en principio de forma independiente para procesar la información de las matriculas, entonces un sistema se encarga del registro de las materias, otro sistema genera los recibos, otro permite su pago y finalmente un sistema le informa al estudiante el estado de su matrícula; como los sistemas son independientes la información se transporta en archivos planos o con formatos definidos para que sean insumos del siguiente sistema. Una tercera evolución del ejemplo se pueda dar cuando estos sistemas de información se correlacionan automáticamente

compartiendo la información necesaria para que el estudiante realice el proceso de matricula desde cualquier lugar y a cualquier hora por internet.

La necesidad de la Universidad en busca de agilizar el procesamiento de grandes volúmenes de información ha llevado a soportar diferentes procesos administrativos y académicos en sistemas de información, donde el objeto y la tendencia es poder contar en tiempo real, con diferentes tipos de información verídica y de cualquier parte de la organización. Esta tendencia viene impulsada por las políticas de estado donde se han implementado sistemas de información para tener a valor presente el estado de una institución, como en el sector educativo lo son el SIMAT para la educación básica y media y el SNIES para la educación superior, en el sector transporte el RUNT en línea, el la salud el SOI y PILA y la propuesta del programa Gobierno en Línea donde Colombia es uno líder de los países latinoamericanos.

En este entorno el SPEL es un componente de la interrelación de diferentes sistemas de información que tiene una Universidad, que busca aportar en la solución al problema generado en el recaudo de los dineros asociados a los diferentes servicios que se ofrecen. Como se mostró anteriormente la delicada situación financiera de la universidad no permite dejar de recibir ingresos porque simplemente los sistemas actuales de recaudo no se dan abasto o generan incomodidades y molestias entre los usuarios que realizan sus pagos; como por ejemplo largas filas en temporadas de pagar matriculas, o exámenes supletorios o habilitación, donde la población estudiantil se concentra alrededor de los lugares de pago, cajas de la Universidad y bancos. Es por esto que el SPEL busca beneficiar directamente a los usuarios, principalmente estudiantes que deben realizar sus pagos y que podrían hacerlo vía internet. La Universidad se beneficia directamente porque podrá disponer inmediatamente de los dineros percibidos por los pagos en línea, como también agilizar los procesos administrativos asociados a estos recaudos.

Las iniciativas para mejorar los servicios prestados como todo proceso de adaptación a nuevas posturas frente al uso de herramientas TIC, genera inconformidades y temores en los primeros ciclos de producción. Esto se vio reflejado en la cantidad creciente de pagos recibidos por el SPEL de Unicauca en cada periodo de matrículas desde 4 a 80 personas que utilizaron el servicio.

La visión para la prestación del servicio del SPEL es de 24x7 o siempre disponible, salvo obviamente la validación de un pago fuera de la fecha de vencimiento. Pero dado la criticidad del servicio respecto de la información que transita por él y la inmadurez de los procesos que respalden el servicio; solo se habilita la opción de pago en línea cuando se puede garantizar su gestión y correcto funcionamiento.

El SPEL desde su desarrollo cuenta por lo menos con un único ambiente de funcionamiento o sea el desarrollo, las pruebas y producción se ejecutan bajo el mismo

ambiente. En el mejor de los casos pueden existir dos ambientes de funcionamiento uno para el desarrollo y pruebas y el de producción, ya que por la limitación de los recursos no se puede dedicar equipos a un solo servicio.

La base de datos de la información que relaciona los estudiantes con las valores que se deben pagar funciona de forma centralizada, donde el acceso de información a la misma se puede realizar automáticamente partiendo de archivos planos que contiene la información y también manualmente para editar en detalle campos de información. Estos archivos se elaboran, se comparten y transportan bajo la responsabilidad de la persona a cargo generalmente sin medidas de seguridad que protejan la integridad de esta información.

El SPEL permite imprimir el resultado de la transacción, siendo esta la única forma de comprobar y respaldar las operaciones por parte del usuario. La universidad solo tiene respaldo en los archivos de conciliación generado por el PSE siendo esta la única fuente de comprobación de operaciones.

El SPEL no cuenta con un proceso para reportar eventualidades tanto de los usuarios directos como sus administradores, esto da cuenta de que no hay registro tanto del correcto o inadecuado funcionamiento del mismo.

1.3.4 Amenazas de los SPEL en las Universidades Oficiales

Con el nacimiento del comercio electrónico y a su vez las transacciones en línea, fueron apareciendo ataques informáticos que operan con sitios Web falsos y códigos maliciosos que buscan robar información confidencial de los usuarios dando lugar a estafas, robos y fraudes.

A continuación se mencionan las amenazas más comunes y su operación en el entorno del SPEL de las Universidades Oficiales.

1.3.4.1 Ingeniería Social

La Ingeniería Social es una acción o conducta social que busca conseguir información de las personas relacionadas con algún sistema. A través de engaños se logra que el usuario revele información importante y confidencial tanto personal como del sistema, de esta forma la ingeniería social se enfoca en lograr la confianza de las personas para persuadirlas, manipularlas y con un par de preguntas, una llamada telefónica, un mensaje

de texto o un correo electrónico hacer que caigan en la trampa y así acceder a información o incluso a la propia red, todo esto siempre con un fin económico [7].

El principio básico de esta modalidad es que el usuario es el eslabón más débil, es por esto que los atacantes hacen uso de la credibilidad, inocencia, desconocimiento y morbo de las personas para realizar sus engaños, por ejemplo circulan miles de correos electrónicos sobre noticias de catástrofes, fotos y videos de famosos lo cual realmente es un virus o troyano que se ejecuta en el momento de la descarga, también hacen uso de marcas y eventos conocidos que llevan a los usuarios a revelar su información.

Una modalidad muy sencilla, común y económica es realizar una llamada haciéndose pasar por alguien, por ejemplo el administrador pidiendo contraseñas de acceso [54]

Llamada a una compañía telefónica:

- ¿Quién es el supervisor hoy?
- Carmen
- Comuníqueme con Carmen
- Hola Carmen, ¿Tiene un mal día hoy?
- No, ¿Por qué?
- Su sistema parece estar caído
- No, funciona correctamente.
- Mmm, por favor salga e ingrese nuevamente
- No hemos notado ningún cambio, por favor hágalo de nuevo.
- Nada, trataré de entrar por acá, y mirar que está pasando, por favor dígame su usuario y contraseña.

Los fallos de seguridad generalmente se presentan no por los sistemas, su configuración o administración, sino por gente no entrenada, poco precavida o indiscreta, es importante comprender que no hay tecnología capaz de proteger contra la ingeniería social, ni usuarios o expertos que se encuentren exentos a este tipo de amenaza, así que la única forma de evitarlo es ser consciente y estar prevenido.

En el entorno del SPEL la Ingeniería Social puede ser realizada por cualquier persona haciéndose pasar por el administrador de la red de datos de la Universidad y solicitando al estudiante el usuario y contraseña de la cuenta bancaria, haciendo suponer algún error en el pago de la matricula. Otra modalidad es engañando a los administradores de la red de datos solicitando claves de acceso para ingresar al sistema y así modificar los valores a pagar por los estudiantes.

1.3.4.2 Phishing y Pharming

El Phishing es una técnica de Ingeniería Social y su fin es el robo de información personal a través de diversos medios como SMS (Short Message Service) donde se solicitan datos personales supuestamente para actualización de datos de su banco de confianza, también se puede realizar a través de llamadas telefónicas suplantando entidades, adquiriendo así los datos personales de quienes sin precaución los suministran, otra de las formas es cuando los delincuentes envían un correo electrónico simulando ser una entidad de confianza como un banco y piden al usuario acceder a un enlace que los lleva a un sitio Web falso cuya imagen es idéntica al original, solicitan todos los datos personales y confidenciales, de esta forma el atacante recolecta toda esta información y la tiene disponible para realizar todo tipo de transacciones. Generalmente suplantan entidades bancarias para robar contraseñas que les permitan realizar transacciones electrónicas y así robar a los usuarios [55]. En Colombia el phishing se presentó aproximadamente entre Noviembre de 2006 y Enero de 2007 cuando suplantaron la página de Bancolombia [56], En el mundo esta modalidad de robo presentó en el primer semestre de 2009 aproximadamente 5.698 ataques un poco menos que en el segundo semestre del 2008 en el cual se presentaron 56.969 [57].

Dado que las personas ya conocían acerca del phishing y eran consientes de que podían ser víctimas de un fraude a través de estos correos electrónicos, los delincuentes tuvieron que buscar nuevas formas de atacar, es así como a mediados del 2005 aparece el Pharming como una evolución del Phishing, este desvía el tráfico de Internet de un sitio Web hacia otro cuya apariencia es similar, de esta forma se pueden obtener nombres, contraseñas y diversos datos que quedaran guardados en la base de datos del sitio falso [11].

Los sitios Web de bancos, entidades financieras o de aquellos que permitan transacciones de pagos son los más suplantados, pues es de gran interés para el pirata informático [59] robar información personal para suplantación de identidad, fraudes y robo.

Para acceder a un sitio Web, se escribe la URL en el navegador de Internet la cual se convierte a su respectiva dirección IP, esto se hace a través de un servidor DNS. El pharming realiza su ataque en este tipo de servidores, su objetivo es cambiar la correspondencia numérica a todos los usuarios que lo utilicen, de tal forma que al escribir la URL los lleve a un sitio Web idéntico al original pero en realidad es un sitio falso creado por delincuentes [60].

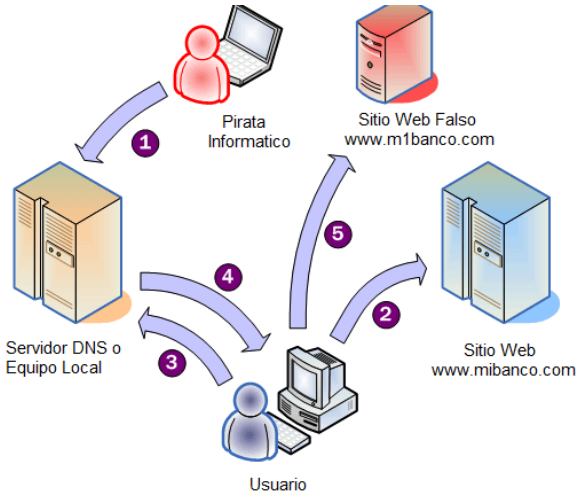


Figura 17. Funcionamiento del Pharming

1. El pirata informático entra al Servidor DNS y cambia la tabla de direcciones IP
2. El usuario escribe la URL del Sitio Web a la que desea acceder
3. Se realizar una petición de la dirección IP al servidor DNS
4. Devuelve la dirección IP falsa
5. El usuario accede sin saberlo al sitio Web Falso

En el caso de las Universidades Oficiales, un estudiante puede recibir en su correo electrónico institucional un supuesto mensaje de la red de datos informando el link por el cual pueden realizar su pago a través del SPEL, dando click lo direcciona a una página Web falsa de la entidad financiera en la cual después de digitar su usuario y contraseña aparece un mensaje de error y lo direcciona a la página real del banco. Los datos han sido guardados en un archivo y enviados a un correo electrónico, el delincuente posteriormente usa estos datos para realizar transacciones a su cuenta. Esta forma de robo también puede ser realizada haciendo modificaciones al DNS de tal forma que cuando se quiera acceder a una página Web de la entidad bancaria la direcciona a una falsa.

1.3.4.3 Denegación de servicio

La denegación de servicio, DoS (Denial of Service), se realiza enviando mensajes hacia un destinatario o hacia el canal de comunicación, se consumen los recursos de tal forma que en un corto periodo de tiempo se interfiera en su funcionamiento impidiendo acceder a sus servicios [61]. Las pérdidas económicas y el daño al buen nombre que sufre una empresa cuando es víctima de este ataque pueden llegar a ser más grande que el de una intrusión al sistema.

Los ataques DoS más comunes son [62]:

- Ataques Software: Se envía al destino mensajes o datagramas errados aprovechando alguna vulnerabilidad del sistema. Este tipo de ataques se pueden prevenir teniendo los sistemas actualizados o filtrando los paquetes erróneos. Hay diversas formas de realizarlos como:
  - Ping de la Muerte: Se envían numerosos mensajes ICMP muy pesados al destino hasta que colapse [63].
  - Teardrop (Lágrima): Se realiza mediante el envío de paquetes IP traslapados lo que dificulta que el receptor los organice y posibilita que el sistema colapse [62].
  - Land Attack: Consiste en enviar un paquete a algún puerto del servidor con la dirección origen y destino igual, después de algunos mensajes la máquina se cae [62].

- Inundación: Como su nombre lo indica se inunda un sistema con constante flujo de tráfico hasta que el ancho de banda o los recursos del sistema se consuman, hay varias modalidades entre ellas:
  - TCP SYN: Se satura el tráfico de la red aprovechando la negociación de tres vías del protocolo TCP. De esta manera, se hace una petición de conexión con una dirección origen falsa, el destino envía un paquete intentando establecer la conexión y esperando como respuesta un mensaje ACK (Acuse de recibo), pero dado que la dirección IP esta errada nunca lo va a recibir, los intentos de conexión disminuyen el rendimiento de la red hasta lograr que salga de funcionamiento [64].
  - Inundación ARP: Es una denegación de servicio por medio del envío de paquetes ARP, se envía direcciones MAC al azar asociadas a direcciones IP, o indicando un DNS o una Gateway con una MAC no existente, se genera un alto flujo de tráfico hasta que finalmente deja de funcionar [65].
  - Inundación de Red: Envío de demasiadas solicitudes de conexión de forma que se daña la conectividad a Internet de una red saturando los canales de comunicación e impidiendo que conexiones reales funcionen [62].
  - Inundación de Conexión: Los ISP tienen un número máximo de conexiones simultáneas, cuando se alcanza el límite no se admiten nuevas, el atacante manteniendo activas varias conexiones al tiempo puede lograr que el servidor no funcione [62].
  - Inundación ICMP: Envió de paquetes ICMP solicitud de eco (ping), dado que el destino debe realizar una respuesta de eco (pong) lo que sobrecarga la red [66].

- Denegación de Servicio Distribuido (DDoS) [67]: Es cuando varios orígenes distribuidos y sincronizados realizan un ataque a un mismo destino.
  - Trinoo: Se basa en un modelo jerárquico maestro/esclavo y se realiza en grandes empresas o universidades, cuando se accede a un equipo se instalan todos los programas Trinoo (snifers, puertas traseras, demonios), luego se escanean otros

equipos para infectarlos, así crece la red y se tiene control sobre muchos equipos [67].

- TFN. Tribe Flood Network: Los ataques se realizan mediante inundación SYN o ICMP. Se forma una red donde el atacante controla uno o más equipos (clientes), cada equipo controla varios demonios y estos reciben la orden de realizar los ataques [67].

Los atacantes pueden hacer uso de estas modalidades para dejar sin servicio al sitio Web de la Universidad solo por la satisfacción de vulnerar el sistema y que sea una situación crítica para los administradores sobre todo si lo realizan en los días de mayor congestión cuando es la época de pago de matrículas u otros servicios.

1.3.4.4 Spoofing

Se refiere a la suplantación de identidad de un tercero con fines maliciosos, entre los diferentes mecanismos existen:

- Ip Spofing: Se utiliza para acceder a un equipo de forma no autorizada, se realiza enviando paquetes TCP con una dirección IP de origen falsa y generalmente suplantando un equipo miembro de la red. El fin de acceder a los equipos es recopilar información del sistema como puertos abiertos, sistema operativo, aplicaciones, vulnerabilidades, entre otros. Esta amenaza es difícil controlarla ya que se debe a un problema en el diseño del protocolo TCP/IP, sin embargo se pueden aplicar algunos métodos sencillos para prevenirlo como filtros en el router, encriptación y autenticación. [68], [69].
- DNS Spoofing: Suplantación de identidad por nombre de dominio, hace referencia a la falsificación de la relación dirección IP – Nombre de Dominio, esto permite al atacante direccionar al usuario a sitios Web Falsos [70], [71].
- Web Spoofing: Suplantación de una página Web Real. El atacante modifica las páginas Web que accede un usuario a través del navegador. El delincuente puede crear una copia de toda la Web y monitorear todas las actividades del usuario como el ingreso de contraseñas, números de tarjetas bancarias, entre otros y es así como obtiene toda la información de la víctima. Una forma de evitar esta amenaza es verificar en el navegador que la dirección sea realmente a la cual se quiere acceder y desactivar acciones de Java y Active X [72].

La red de datos de la Universidad puede ser afectada por esta amenaza ya que se puede acceder a algún servidor o equipo de la red para rastrearlo y encontrar sus vulnerabilidades con el fin de tumbar al servidor, robar información, por ejemplo, para la modificación de valores a pagar en la matrícula, modificación de notas, capturar contraseñas para realizar transacciones bancarias a cuentas personales, entre otros.

1.3.4.5 Keylogger

Keylogger [73] es un programa que registra todas las pulsaciones que se hacen sobre el teclado las cuales se guardan en un archivo o se envían por Internet. Este registro se puede hacer a través de hardware utilizando pequeños dispositivos que pasan desapercibidos, se instalan entre el puerto del teclado y el teclado y guardan todas la pulsaciones del teclado en su memoria interna que puede estar entre 8Kb y 2 Mb; a través de software es el medio más común y el más utilizado ya que es un pequeño programa que se distribuye como un troyano, en la Web hay muchas páginas de las cuales se pueden descargar gratis.

Este programa espía es muy atractivo para cualquier delincuente puesto que de una forma muy sencilla y sin tener contacto con el usuario puede conocer contraseñas, información personal, conversaciones, documentos, números de tarjetas, en fin toda la información a su alcance para realizar cualquier tipo de delito. Algunas páginas utilizan teclados virtuales los cuales solo necesitan del mouse para escribir y así evitar que el usuario teclee y la información sea capturada por un keylogger, pero los programas más actuales capturan también los clicks del mouse, así que se pueden detectar con antivirus, algunos firewalls o con programas antikeylogger específicos, aunque no es cien por ciento seguro ya que muchos keylogger son indetectables.

Teniendo en cuenta la facilidad de esta modalidad y además que las personas aún no toman conciencia de la seguridad informática y realizan sus transacciones desde cualquier computador ya sea en un café internet o desde la misma universidad, un keylogger puede ser instalado en cualquier computador de la institución educativa y capturar toda la información cuando el estudiante esté realizando su matrícula, también si se encuentra instalado en algún equipo de la red se puede tomar información de contraseñas, procesos e información exclusiva de la Universidad.

1.3.5 Seguridad de los SPEL en las Universidades Oficiales

Los SPEL se realizan dentro de las Universidades como proyectos de desarrollo que se enmarcan dentro de los requisitos funcionales de los mismos, dejando de lado los requisitos no funcionales como lo son: la calidad, el rendimiento, la seguridad entre otros. Por esto no existe un sistema de gestión de seguridad de la información asociado al SPEL que respalde los procesos que realiza la aplicación desarrollada.

Las adecuaciones físicas de los centros de datos se han mejorado de acuerdo a las amenazas más frecuentes en el sitio y la comodidad de los espacios laborales, pero de forma general estas adecuaciones se han realizado de forma incremental ya que pocos de los lugares fueron diseñados estructuralmente para el funcionamiento de un centro de

datos. Las principales características de estos espacios frente a la seguridad física de las personas y equipos resguardados son: extintores de incendio adecuados, rutas marcadas de evacuación, control de temperatura del lugar, cableado estructurado, fuentes de alimentación de respaldo como ups y/o planta eléctrica. El perímetro de los centros de datos se compone de chapas de seguridad y en el mejor de los casos lectores de tarjetas inteligentes.

El SPEL se encuentra funcionando dentro del área de servidores de los centros de datos o en el peor de los casos desde el equipo donde se desarrollo la aplicación. Las protecciones de seguridad principales de los servidores de producción son: firewall a nivel físico y lógico y antivirus. Las configuraciones se revisan y se evalúan por lo menos una vez en el semestre; pero para el SPEL no existe un documento de respaldo de donde se pueda partir para reconfigurar el servicio en caso de una des configuración grave.

Dado que la implementación de una norma de seguridad implica costos y disposición de personal, recursos escasos por la condición económica crítica de la Universidad. El sector académico de la institución ha desarrollado trabajos de grado, pasantías o investigaciones en seguridad de la información de los sistemas de forma general o en temas puntuales. Estos trabajos sirven y son tomados como referencia para conocer el estado actual de la seguridad de la información manejada por la oficina de TIC. Este esfuerzo de utilizar el talento humano de estudiantes y docentes se queda en el planteamiento de soluciones y que pueden ser implementadas más adelante, dependiendo de funcionarios comprometidos con una política institucional clara para brindar seguridad en la información que almacena y procesa la universidad.

Uno de los activos importantes de los centros se datos de las universidades, es el talento humano que realiza la gestión de seguridad de información, ya que por iniciativa y por tener respaldo de su propio trabajo en primer lugar se han formado autodidácticamente en conocimientos de seguridad organizados dentro de metodologías o normas de referencia y en segundo lugar ha comenzado a documentar estos procedimientos para beneficio institucional.

Las universidades cuentan con políticas de seguridad de información establecidas que han surgido con la necesidad o a consecuencia de experiencias negativas. Pero en su mayoría no se tiene presente la seguridad de la información, se presume los riesgos a los que están expuestos por lo que se llevan a cabo prácticas de seguridad de información de una forma muy personal y no de forma sistemática apoyadas o soportadas dentro de un proceso de gestión de seguridad. El SPEL de la Universidad del Cauca no cuenta con políticas de seguridad de información.

Cuando se presentan problemas o fallos en el funcionamiento de los servicios, el éxito de depende de la madurez de los procedimientos en seguridad y en gran medida del talento humano que tiene que proceder reactivamente frente a la ocurrencia de un fallo.

Los planes de contingencia para el SPEL no existen, pero se considerarían asumiendo diferentes niveles de riesgo; o sea se espera a que exista un evento que realmente amenace la disponibilidad e integridad de la información para encaminar las acciones que procuren su desarrollo.

Dentro de las medidas implementadas de seguridad, se hace uso de certificados de seguridad y métodos de cifrado en algunos procesos muy particulares de los servicios. Aunque la existencia de un certificado de seguridad refleja el interés de la institución en invertir en seguridad para confianza de los estudiantes y en beneficio de su buen nombre. El uso del certificado se ve comprometido con la inapropiada generación o configuración dentro de los servicios que lo requieren; lo que permite al SPEL ser vulnerable frente a un ataque de suplantación de identidad combinado con el ataque de hombre en el medio.

La forma de autenticación de un usuario frente el servidor en un servicio como el SPEL es débil ya que no es necesario colocar una clave o contraseña que solo el usuario conozca y administre; principalmente se utiliza el código de estudiante. Aunque la forma de autenticación por contraseña se utiliza en otro tipo de servicios, queda pendiente hacer la integración de la funcionalidad de autenticación al SPEL.

Las pruebas del servicio, dependen y son responsabilidad de la Universidad, una vez el SPEL se encuentre en la etapa de producción. Estas pruebas se realizan por los responsables de la administración el servicio y pocas veces se realizan basándose en metodologías de pruebas de seguridad.

Capítulo 2 GENERACION DE UN CONJUNTO DE LINEAMIENTOS PARA LA GESTION DE SEGURIDAD DE LA INFORMACIÓN DE SISTEMAS DE PAGO EN LÍNEA DE LAS UNIVERSIDADES OFICIALES DE COLOMBIA

2.1 Análisis Comparativo de Estándares y Metodologías de Seguridad de la Información

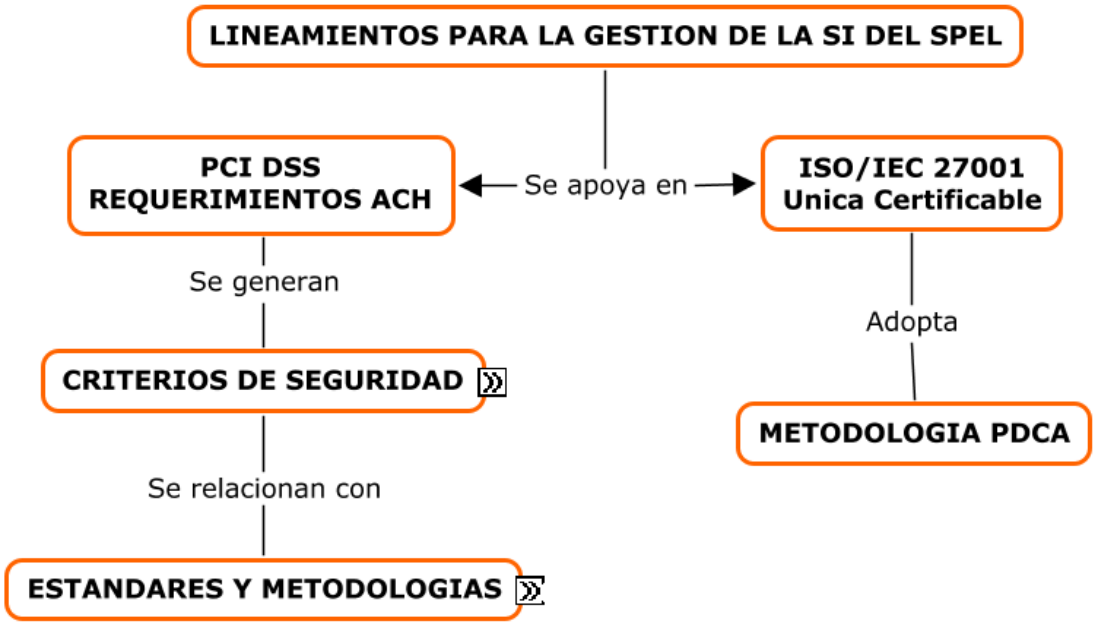


Figura 18. Diagrama Objetivo Específico 2

De acuerdo a los estándares y metodologías de seguridad sintetizadas en la base de conocimiento planteada en el Capítulo 1, se realiza un análisis comparativo, entre los estándares de SI y los componentes[2] que debería tener un SGSI para un SPEL.

Por lo anterior, teniendo en cuenta la PCI DSS [22] y los requisitos de ACH Colombia, se definen ocho componentes que todo SPEL debe cumplir para gestionar la seguridad y disminuir el riesgo. Los componentes son los siguientes:

1. Políticas de Seguridad: Define políticas de seguridad para el desarrollo, uso y administración del SPEL

[2] Que compone o entra en la composición de un todo [74].

2. Gestión de Riesgo: Establece un análisis de riesgo del sistema que permita identificar, estimar y valorar el riesgo y así determinar amenazas, vulnerabilidades e impactos.

3. Desarrollo y mantenimiento de aplicaciones y sistemas seguros: Define guías para un desarrollo seguro de las aplicaciones que intervienen en el SPEL y su mantenimiento.

4. Desarrollo y mantenimiento de una red segura: Establece las características de una red segura, su diseño, implementación y mantenimiento.

5. Seguridad Física: Define parámetros de seguridad en el entorno en que se encuentra el SPEL tales como seguridad perimetral, control de acceso físico, entre otros.

6. Protección de los datos de usuario: Gestiona la seguridad para la protección de los datos de usuario que procesa, transmite y almacena el SPEL.

7. Supervisión y Pruebas: Define procedimientos que permitan realizar una evaluación constante del SPEL para identificar que se debe corregir y mejorar.

8. Implementar acciones preventivas y correctivas: De acuerdo al resultado del componente anterior se debe realizar mantenimiento al SPEL y ejecutar acciones que prevengan o corrijan daños.

Los componentes planteados anteriormente se toman como criterios[3] de clasificación y comparación de las metodologías y estándares estudiados, para ello es necesario interrelacionarlos y establecer que estándares aplican a cada uno de estos y qué metodologías los complementan. De esta manera se obtiene la siguiente tabla.

Tabla 3. Criterios de Seguridad vs Estándares y Metodologías

CRITERIOS	***ISO 27001***	***RFC 2196***	***ISO 9001***	***ISO 27005***	***ISO 27002***	***ISO 15408***	***TIA 942***
Políticas de Seguridad	Cumple. Se comple-menta con OSSTMM	Cumple. Se complement a con OSSTMM	Cum -ple				
Gestión de Riesgo	Cumple			Cum-ple	Cumple. Se complement a con ISSAF OWASP		
Desarrollo y mantenimient o de	Cumple				Cumple. Se complement	Cumple	

[3] Juicio o Discernimiento [75].

aplicaciones y sistemas seguros					a con OWASP		
Seguridad Física					Cumple. Se complement a con OSSTMM		Cumpl e
Protección de datos de los usuarios					Cumple	Cumple. Se complement a con OSSTMM ISSAF	
Desarrollo y mantenimient o de una red segura					Cumple. Se complement a con OSSTMM		
Supervisión y Pruebas	Cumple. Se complement a con OSSTMM ISSAF OWASP OSSIM			Cum- ple		Cumple	
Implementar acciones preventivas y correctivas	Cumple						

La ISO/IEC 27001 aporta al primer componente *Políticas de Seguridad*, con su apartado 4.2.1 Establecer el SGSI, ya que en éste se define el alcance y los límites del sistema de gestión, así como las políticas de seguridad en términos de las características del negocio, la organización, ubicación, activos, tecnologías, entre otros, que se encuentren enmarcadas por requerimientos comerciales, gestión y evaluación del riesgo y que además sean aprobadas por la gerencia o entes responsables. LA RFC también aporta ya que define como se deben realizar las políticas y establece todo lo que se debe tener en cuenta para su diseño e implementación. Esto se complementa con el Trabajo de Grado Criterios para Establecer Políticas de Seguridad de la Información y Plan de Contingencia, Caso de Estudio El Centro de Datos de La Universidad del Cauca [76], y con la OSSTMM Sección C: Seguridad en las Tecnologías de Internet, Módulo 16. Evaluación de Políticas de Seguridad, el cual plantea evaluar que las políticas que se encuentran escritas realmente se están aplicando y que además se encuentran basadas en las justificaciones del negocio, de la organización y de los estatutos legales. La ISO 9001 aporta en sus ítems 5. Responsabilidad de la Dirección y 6. Gestión de los Recursos.

El segundo componente *Gestión de Riesgos*, es abordado por la ISO/IEC 27001, punto 4.2.1 Establecer el SGSI, literales c, d, e, f y g los cuales identifican, analizan y evalúan el

riesgo, determinan niveles aceptables de riesgo y las acciones a realizar para el tratamiento del mismo. La ISO/IEC 27002 aporta los controles que se deben implementar para realizar las acciones definidas en la ISO/IEC 27001. Se complementa con OWASP en su sección 5. Valorar el Riesgo Real, el cual identifica el riesgo, estima la probabilidad de ocurrencia y el impacto en el negocio, determina la severidad del riesgo y se ajusta al Modelo de Valoración del Riesgo. Todo esto se enmarca en la ISO/IEC 27005 que define la gestión del riesgo para la seguridad de la información. ISSAF aporta con su sección B, apartado 6. Evaluación del Riego que incluye metodología y herramientas de evaluación.

En el componente tres, *Desarrollo y mantenimiento de aplicaciones y sistemas seguros,* aporta la ISO/IEC 27001, 4.2.2 Implementar y Operar el SGSI, literales a, b, c, d, h los cuales sugieren implementar los tratamientos de riesgo aplicando los controles seleccionados de la ISO/IEC 27002, medir su efectividad y manejar las operaciones y recursos del SGSI. La ISO/IEC 15408 aporta con su clase FTA: Acceso al Sistema, que especifica los requerimientos funcionales del establecimiento de una sesión de usuario. Estas normas se complementan con OWASP. Entorno de Pruebas, que enuncia lo que se debe hacer antes de empezar el desarrollo, durante el diseño y la definición, durante el desarrollo, durante la implementación y mantenimiento.

El cuarto componente *Desarrollo y mantenimiento de una red segura,* se soporta en la ISO/IEC 27002 con los controles de Gestión de Seguridad de la Red que definen el Control de las Red el cual busca proteger la información en las redes y mantener la seguridad de los sistemas y aplicaciones utilizando la red y también la Seguridad de los Servicios de Red provisión de conexiones, servicios de redes privadas, redes de valor agregado, firewalls, sistema de detección de intrusos, entre otros. La OSSTMM la complementa en su Sección C, Modulo 1. Logística y Controles y Módulo 2. Sondeo de Red.

Al componente cinco *Seguridad Física*, le aportan la TIA 942 Sección 3, 4, 5, 6, 7, y 8 que menciona el diseño del Centro de Datos, sistemas de cableado, redundancia y topologías. La ISO/IEC 27002 define controles de Seguridad Física y Ambiental que contienen Áreas seguras (perímetros, controles de ingreso físico, aseguramiento de oficinas y habitaciones, protección contra amenazas externas e internas, áreas de acceso público), Equipo de seguridad (Ubicación y protección del equipo, servicios de soporte, seguridad del cableado, mantenimiento de equipo) y Seguridad de la eliminación o re-uso del equipo. OSSTMM complementa con la sección F: Seguridad Física con el Módulo 1: Revisión de Perímetro, que permite evaluar la seguridad física de la organización teniendo en cuenta el perímetro físico; Módulo 2: Revisión de Monitoreo, descubre puntos de acceso monitoreados; Módulo 3: Evaluación de controles de acceso, maneja privilegios de acceso físicos; Módulo 4: Revisión de respuestas de alarmas, descubre procedimientos y equipos de alarmas en una organización; Módulo 5: Revisión de Ubicación, métodos para obtener acceso a una organización, a través de puntos débiles en su ubicación; Módulo 6:

Revisión de Entorno, es un método para ganar acceso o dañar una organización a través de puntos débiles de su entorno.

El componente seis Protección de los Datos de Usuario le aporta la ISO/IEC 27002 con controles de Controles Criptográficos y Adquisición, desarrollo y mantenimiento de los sistemas de información (Requerimientos de seguridad, análisis y especificación de los requerimientos, procesamiento correcto en las aplicaciones, validación de la input data y de la output data, control del procesamiento interno, integridad del mensaje). La ISO/IEC 15408 con la clase FDP: Protección de los datos de usuario, especifican requerimientos y políticas de seguridad relacionadas a proteger los datos de usuario, la clase FIA: Identificación y Autenticación que define los requerimientos funcionales para establecer y verificar la identidad de un usuario. La complementa OSSTMM Sección A: Seguridad de la Información, Módulo 2: Revisión de Privacidad, la cual contiene el punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente y del empleado. Además, ISSAF la complementa con la sección Y: Evaluación de la seguridad de la base de datos.

El componente séptimo *Supervisión y Pruebas*, la ISO/IEC 27001 aporta en la sección 4.2.3, literales a, b, c, d, y e los cuales ejecutan los procedimientos monitoreo y revisión regulares de la efectividad del SGSI, revisión las evaluaciones del riesgo y realización de auditorías internas. También los apartados 6. Auditorías internas del SGSI y 7. Revisión gerencial del SGSI. La ISO/IEC 15408 con la clase FAU: Auditoría de Seguridad que permiten determinar qué actividades de seguridad son relevantes. La complementan las metodologías OSSTMM Sección C: Seguridad en las Tecnologías de Internet, Módulo 1: Logística y Controles, Módulo 3: Identificación de los Servicios de Sistemas, Módulo 7: Búsqueda y Verificación de Vulnerabilidades, Módulo 8: Testeo de Aplicaciones de Internet, Módulo11: Testeo de Control de Acceso, Módulo 12: Testeo de Sistemas de Detección de Intrusos, Módulo 13: Testeo de Medidas de Contingencia y Módulo 15: Testeo de Denegación de Servicio. OWASP maneja una Guía de Pruebas en su apartado 4. Pruebas de Intrusión de aplicaciones Web. OSSIM define cuatro etapas, sensores, servidores, consola y base de datos; a través de los sensores se monitoriza la actividad de la red y en los servidores se desarrolla la Correlación, Priorización, Valoración de riesgos que permite identificar los falsos positivos, priorizar eventos y la abstracción de las alarmas.

El octavo componente *Implementar acciones preventivas y correctivas,* se basa en la ISO/IEC 27001, apartados 4.2.4 Mantener y Mejorar el SGSI y 8. Mejoramiento del SGSI, que plantea Mejoramiento Continuo, Acciones Correctivas y Preventivas.

De acuerdo a la Tabla 3 y al análisis anterior, se identificar que la ISO/IEC 27001 es el estándar que más se ajusta a los criterios establecidos y además de que es el único estándar certificable, es por ello que en este Trabajo de Grado se escoge como referencia principal para el desarrollo de los lineamientos de seguridad el SPEL que serán mencionados más adelante en éste capítulo.

La ISO/IEC 27001 acoge el modelo del proceso PDCA (Planear, Hacer, Chequear, Actuar) [77], la cual es una estrategia que permite el continuo mejoramiento de la calidad y se puede aplicar a todos los procesos de un SGSI, es apropiado para la planificación, implementación, verificación y operación de estos sistemas, es por eso que la ISO lo ha tomado como base para organizar el contenido de sus normas internacionales tales como la ISO 9000, ISO 14000 e ISO 27000.

En la fase PLANEAR se definen los objetivos, se realiza un análisis de la situación actual y establecer los procesos que permitirán obtener el resultado deseado.

En la fase HACER se aplica lo que se ha determinado en la fase anterior, se implementan los procesos.

En CHEQUEAR, se verifica si lo que se ha definido se desarrolla correctamente

ACTUAR, en esta fase se establecen todas las condiciones que permitan mantener o mejorar los procesos implementados.

En el caso de un SGSI las fases se enfocan de la siguiente manera:

PLANEAR: Diseño del SGSI, análisis de riesgos y selección de controles de seguridad.

HACER: Implementación y operación de los controles.

CHEQUEAR: Evaluar la eficiencia del SGSI

ACTUAR: Se realizan todos los cambios que conlleven a un SGSI eficiente.

Esta metodología se adopta en este trabajo de investigación, de esta manera se establecen los componentes de seguridad definidos, en cada una de las fases de la siguiente manera.

Tabla 4. Metodología PDCA para la gestión de seguridad del SPEL

FASE	COMPONENTES DE SEGURIDAD	LINEAMIENTOS DE SEGURIDAD	ACTIVIDADES
PLANEAR	- *Políticas de Seguridad* - *Gestión de Riesgo*	1, 2, 3	1 - 12
HACER	- *Desarrollo y mantenimiento de aplicaciones y sistemas seguros.*	4	13 - 18
VERIFICAR	- *Desarrollo y mantenimiento de una red segura* - *Seguridad Física*	5 6 7	19 - 26

	- *Protección de los datos de usuario* - *Gestión de Transacciones* - *Supervisión y Pruebas*		
ACTUAR	- *Implementar acciones preventivas y correctivas.*	8	26

2.2 Lineamientos para la Seguridad de la Información

Teniendo en cuenta los aportes de los estándares y las metodologías a los criterios de seguridad seleccionados y esquematizados en las fases del PDCA y principalmente el conocimiento del contexto de las universidades Oficiales, se definen 8 lineamientos y sus correspondientes actividades que se deben implementar en los SPEL para brindar seguridad de la información y del sistema.

Se entiende en este contexto que lineamiento es una directriz, es decir, un conjunto de instrucciones o normas generales para la ejecución de algo; la generación de estos lineamientos no sigue una metodología específica, se crearon a criterio propio pensando en la forma de articular las diferentes estructuras en las que se proponen requerimientos, actividades, procesos tanto de los estándares como de las metodologías enunciadas en el primer capítulo.

1. **Establecer el alcance del SGSI para el SPEL y definir políticas de SI para las siguientes áreas, Desarrollo y Mantenimiento de Aplicaciones, Desarrollo y Mantenimiento de una red segura, Seguridad Física, Protección de datos de Usuario, Supervisión y Pruebas y Gestión de Incidentes de Seguridad**

   En el Desarrollo y mantenimiento de aplicaciones se puede tener en cuenta OWASP punto 3. Entorno de Pruebas. En el Desarrollo y mantenimiento de una red segura, según la RFC en su apartado 3. Arquitectura, define la protección de la red, de la infraestructura y de los servicios. Protección de datos de usuario; es posible tener en cuenta la RFC 2196 apartado 4. Seguridad, Servicios y Procedimientos, y la ISO/IEC 15408 con su clase FDP: Protección de datos de usuario y sus respectivas familias.

   Para la seguridad física es importante tomar como referencia la TIA 942, punto 3. Diseño general de un Centro de Datos. La RFC punto 5. Manejo de Incidentes de Seguridad sirve como guía para el desarrollo de las políticas de seguridad en el área de Gestión de Incidentes de Seguridad.

Todas estas áreas deben ir enmarcadas de acuerdo a la RFC 2196 en su apartado 2.2 teniendo en cuenta las características y componentes de una buena política de seguridad.

a. **Actividad 1. Definir el alcance**
   Definir el alcance del SGSI para el SPEL de su Organización de acuerdo a sus requerimientos internos como pagos, usuarios, tecnologías, interrelación con otros sistemas. Se deben establecer metas de seguridad como lo menciona la RFC 2196 en su punto 2.1, las cuales deben estar basadas en servicios ofrecidos vs seguridad provista, facilidad de uso vs seguridad, costo de seguridad vs riesgo de pérdida.

b. **Actividad 2. Revisión y evaluación de las políticas actuales de seguridad.**
   Se deberán revisar las políticas de la Universidad verificando si existen políticas que enmarquen al SPEL, si las hay se revisan, se aprueban o se modifican, sino se crean.

c. **Actividad 3. Definir una política general del SGSI para el SPEL.**
   Se debe tener en cuenta la ISO/IEC 27001 en su apartado 4.2.1 literal b, la cual debe permitir establecer objetivos, requerimientos comerciales y legales, criterios de evaluación de riesgos y aprobación de la gerencia.

d. **Actividad 4. Creación de Políticas**
   Se deben crear las políticas de seguridad necesarias para el correcto funcionamiento del SPEL y la conservación de la confiabilidad, disponibilidad e integridad de la información.

2. **Determinar los riesgos del SPEL.**

Teniendo en cuenta la ISO/IEC 27001 apartado 4.2.1 literales c, d, e, f incluye:

- Identificar los riesgos (Activos, Amenazas, Vulnerabilidades, Impactos)
- Analizar y evaluar el riesgo (Cálculo del impacto, Calculo de probabilidad de ocurrencia, niveles de riesgo, aceptación de riesgo)
- Identificar las opciones de tratamiento de riesgo (Aceptar, evitar o transferir el riesgo)

Lo anterior se desarrolla basándose en la ISO/IEC 27005.

a. **Actividad 5. Determinar los activos y sus dimensiones de seguridad**
   Determinar los activos relevantes del SPEL y necesarios para su correcto funcionamiento definiendo el valor que tienen para el sistema.

b. Actividad 6. Determinar las amenazas

Definir a que amenazas están expuestos los activos descritos en la actividad anterior y como los afectan.

c. Actividad 7. Estimar el Impacto

Se estima el impacto que se tendría sobre los activos en caso de materializarse una amenaza.

d. Actividad 8. Determinar el Nivel de Riesgo

Definir el impacto ponderado con la frecuencia de ocurrencia.
Nivel de Riesgo = Impacto x Frecuencia

e. Actividad 9. Verificación de Controles de Seguridad existentes

Verificar que controles de seguridad existen para cada uno de los activos evaluados y determinar su efectividad.

f. Actividad 10. Determinar el Riesgo Residual

Definir el riesgo residual de acuerdo al nivel de riesgo y a la efectividad de las medidas de protección.
Riesgo Residual = Nivel de Riesgo / Efectividad

g. Actividad 11. Informe del Análisis de Riesgos

Realizar un informe que consigne los resultados del análisis de riesgos realizado.

3. Crear o seleccionar los controles y procedimientos para la SI del SPEL

La ISO/IEC 27002 menciona diferentes controles que se pueden implementar para reducir los riesgos; los cuales dependen del resultado de la evaluación del riesgo.

a. Actividad 12. Selección de controles para la SI del SPEL

Teniendo en cuenta el resultado del análisis de riesgos, seleccionar y diseñar los controles que garanticen la mitigación del riesgo sobre los activos y las amenazas.

4. Desarrollar la aplicación del SPEL.

Aplica para las Universidades que aún no tienen implementado un SPEL. Se basa en los requerimientos funcionales de ACH y se mejora con OWASP (Proyecto Guía de Pruebas. Punto 3. Entorno de Pruebas), teniendo en cuenta pruebas en las diferentes etapas del desarrollo de la aplicación, lo que permite detectar desde sus primeras fases de desarrollo los riesgos y no esperar a tener un producto final para que los riesgos sean detectados.

a. **Actividad 13. Establecer convenio con ACH para la implementación del SPEL en la Organización.**
   Establecer comunicación con un funcionario de ACH el cual hará la presentación de la propuesta del SPEL, analizará la viabilidad de la implementación del sistema y se establecen los acuerdos para la realización del proyecto para el desarrollo del SPEL.

b. **Actividad 14. Ejecución del plan de actividades propuesto por ACH.**
   Desarrollo de las fases planteadas por ACH teniendo en cuenta el anexo A [78], estas fases se complementan con las actividades que se mencionan a continuación.

c. **Actividad 15. Creación de Modelos UML**
   Se crean los modelos UML para el SPEL, los cuales brindan información que permite entender requerimientos, funcionamiento de la aplicación, relaciones entre actores, entre otros. Esta actividad debe desarrollarse al inicio de la Fase 2 de la actividad anterior.

d. **Actividad 16. Creación de Modelos de Amenazas**
   Se crean los modelos de amenazas para el SPEL que identifican las posibles amenazas que puede sufrir el sistema y se mitigan desde la fase de diseño. Este debe de desarrollarse después del desarrollo de los modelos UML.

e. **Actividad 17. Revisión del Código**
   Finalizando la Fase 2 se debe realizar una revisión exhaustiva del código general con el fin de encontrar fallas o riesgos en la codificación de la aplicación.

f. **Actividad 18. Pruebas de Intrusión**
   Al finalizar la Fase 3 se deben realizar pruebas de intrusión de acuerdo al modelado de la actividad 16 que permitan identificar que tan fácil puede ser accedida o atacada la aplicación, sus componentes y que información se ve comprometida.

5. **Implementar los controles y procedimientos seleccionados.**

Los controles implementados deben abarcar todas las áreas que conforman el SPEL como aplicación, redes, seguridad física, datos de usuario y supervisión y pruebas.

a. **Actividad 19. Cronograma de actividades.**
   Diseñar un cronograma de actividades para la implementación de los controles de seguridad seleccionados.

b. Actividad 20. Implementación de Controles.

Teniendo en cuenta el control seleccionado, se coloca en detalle el contenido del mismo. El desarrollo de esta actividad debe arrojar productos tangibles.

6. Desarrollar planes de pruebas para todas las áreas del SPEL.

En el área de aplicación se puede tener en cuenta a OWASP punto 4. Pruebas de Intrusión de Aplicaciones Web que comprende recopilación de información, comprobación de la lógica del negocio, pruebas de autenticación, pruebas de gestión de sesiones, pruebas de validación de datos, pruebas de denegación de servicio y pruebas de servicios Web. Además también sirve como referencia OSSTMM Sección C: Seguridad en las Tecnologías de Internet, Módulo 8: Testeo de Aplicaciones de Internet e ISSAF en la Sección T: Evaluación de la Seguridad de las Aplicaciones Web

El área de Red se puede basar en ISSAF en sus secciones E (Evaluación de Seguridad del Switch), F (Evaluación de Seguridad del Router), G (Evaluación de Seguridad del Firewall) e I (Evaluación de Seguridad de VPN). También OSSTMM Sección C, Módulo 3 (Identificación de los Servicios de Sistemas), Módulo 7 (Búsqueda y Verificación de Vulnerabilidades) y Módulo 15 (Testeo de Denegación de Servicios) y OSSIM la cual monitoriza la actividad de la red y permite desarrollar características como Correlación, Priorización y Valoración de Riesgos.

En seguridad física se puede tomar como referencia el estándar TIA 942 con su Anexo G, como una lista de comprobación para evaluar los componentes existentes en el Centro de Datos con respecto a los que deberían tener. OSSTMM también se puede tomar como referencia en su Sección F: Seguridad en las Tecnologías de Internet, Módulo 1 (Revisión de Perímetro), Módulo 2 (Revisión de Monitoreo) y Módulo 3 (Evaluación de Controles de Acceso), Módulo 5 (Revisión de Ubicación) y Módulo 6 (Revisión de Entorno)

Para la Protección de los Datos de Usuario se tiene en cuenta la norma ISO/IEC 15408 con su clase FTA: Acceso al Sistema el cual define los requisitos para limitar el alcance de los atributos de seguridad de la sesión de usuario y la clase FIA Identificación y Autenticación. Se complementa con ISSAF Sección Y: Evaluación de Seguridad de la Base de Datos y con OSSTMM Sección B Módulo 1 (Testeo de Solicitud), Módulo 3 (Testeo de las Personas Confiables) y la Sección C Módulo 5 (Revisión de Privacidad).

Para Supervisión y Pruebas se toma en cuenta la ISO/IEC 27001 apartado 4.2.3 Literal d para medir la efectividad de controles y procedimientos

a. Actividad 21. Selección de Plan de Pruebas.

Teniendo en cuenta las áreas donde se implementaron los controles, se deben seleccionar pruebas que permitan evaluar la efectividad del control y descubrir nuevas vulnerabilidades del sistema.

b. Actividad 22. Ejecutar las Pruebas Seleccionadas.

Ejecutar las pruebas anteriormente seleccionadas en cada una de las áreas del SPEL.

c. Actividad 23. Informe del Resultado de Pruebas

Realizar un informe de la ejecución y el resultado de cada prueba.

d. Actividad 24. Evaluación del Resultado de Pruebas.

Evaluar el resultado de las pruebas con el fin de determinar las acciones a realizar.

7. Realizar auditoría interna

Se puede basar en la ISO/IEC 15408 Clase FAU: Auditoría de Seguridad y en la ISO/IEC 27001 punto 4.2.3 literal e (Auditoría Interna). Se debe medir la efectividad de los controles y procedimientos en coherencia con las políticas establecidas de tal forma que se cumplan y por ende minimizar el riesgo asociado a la información.

a. Actividad 25. Planeación del programa de auditoría.

Se debe diseñar un programa que especifique auditores, fechas de auditoría y procesos y áreas a ser auditados.

b. Actividad 26. Resultado de auditoría.

Se deben documentar el resultado de la auditoria donde conste los procedimientos y áreas que cumplen con los controles de seguridad establecidos y las no conformidades encontradas, sus posibles causas y el responsable del área en el cual se presentaron.

8. Implementar acciones preventivas y correctivas

Se basa en la ISO/IEC 27001, apartado 4.2.4 el cual implementa las mejoras identificadas y toma acciones correctivas y preventivas.

El ciclo de gestión del riesgo debe ser una actividad constante en el tiempo para lo cual es necesario programar actividades de mantenimiento que le permitan a la organización mejorar en sus procesos.

a. Actividad 26. Acciones correctivas.

Teniendo en cuenta los resultados de las actividades 24 y 26 se proponen las mejoras al SGSI del SPEL y las propuestas para solucionar las no conformidades asociadas al funcionamiento adecuado del SPEL.

Estas propuestas son los insumos o requerimientos de seguridad para iniciar el siguiente ciclo de SGSI que parte nuevamente en la actividad 1 de estos lineamientos.

Capítulo 3 VALIDACION DEL CONJUNTO DE LINEAMIENTOS

3.1 Desarrollo de los Lineamientos para la Seguridad de la Información

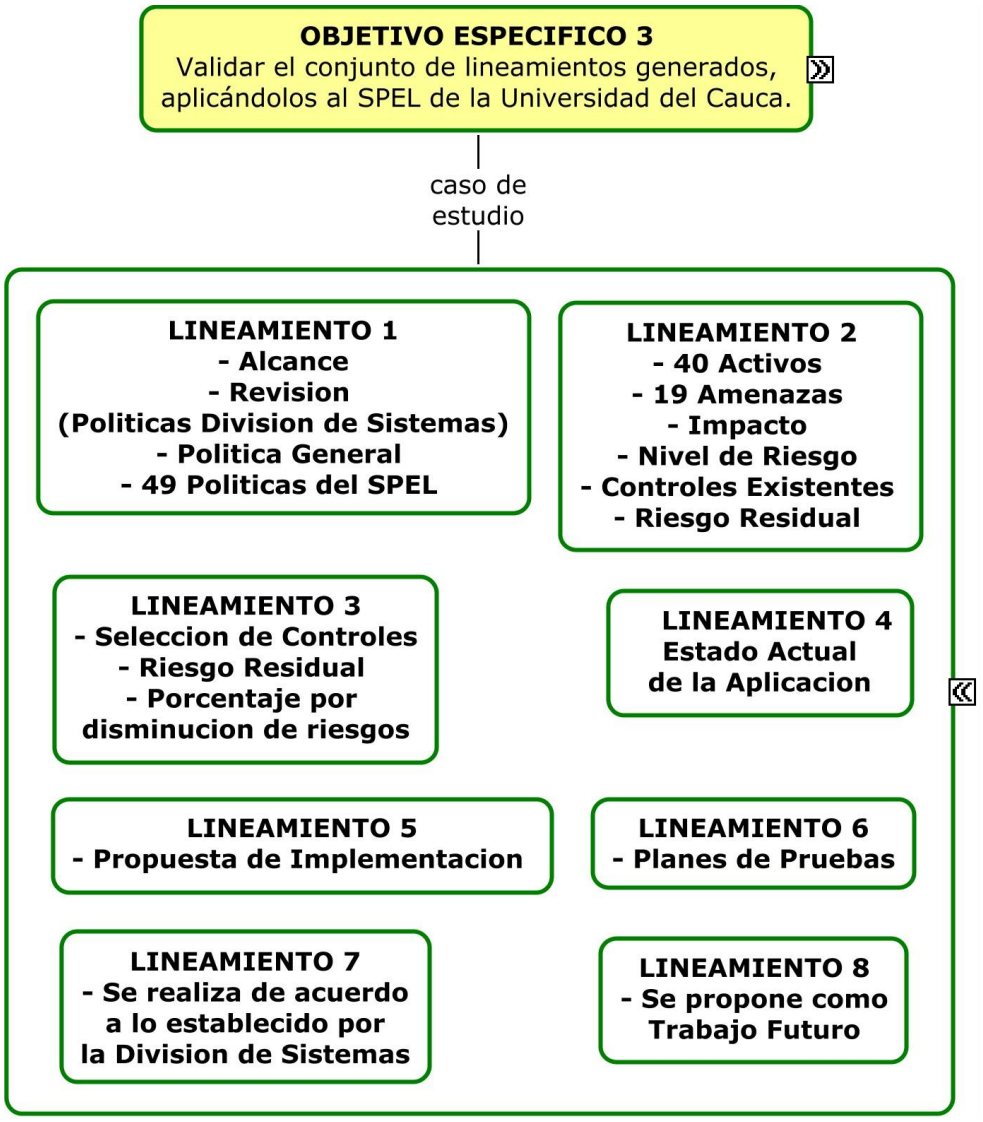


Figura 19. Diagrama Objetivo Específico 3

Teniendo en cuenta los lineamientos propuestos en el capítulo anterior y cada una de las actividades, se desarrollan para el caso de estudio SPEL de la Universidad del Cauca.

3.1.1 Establecer el alcance del SGSI para el SPEL y definir políticas de SI para las siguientes áreas, Desarrollo y Mantenimiento de Aplicaciones, Desarrollo y Mantenimiento de una red segura, Seguridad Física, Protección de datos de Usuario, Supervisión y Pruebas y Gestión de Incidentes de Seguridad

EL SGSI propuesto es para el SPEL (Aplicación de la Universidad del Cauca desarrollada para hacer recaudos por concepto de matrículas de los estudiantes de la Institución a través de su interacción con PSE de ACH Colombia), esta aplicación tiene como insumo la información de la relación de estudiantes con el valor del pago de la matrícula y como resultado el recaudo en las cuentas bancarias de la Universidad a través de la infraestructura de ACH Colombia. El SPEL contiene un conjunto de elementos que permiten su buen funcionamiento como la aplicación software, servidores, enlaces de internet, VPN y certificado de seguridad, para lograr la seguridad del SPEL se han establecido algunas metas como garantizar que el ciclo de desarrollo de las aplicaciones del SPEL sea seguro, confiable y que proteja la integridad de la información; disponer de una arquitectura de red optima que garantice un flujo seguro de información; establecer medidas de seguridad en las instalaciones físicas de tal forma que se proteja el talento humano, los equipos y el sistema en general; conservar la confiabilidad, integridad, disponibilidad y no repudio de la información; realizar supervisión y pruebas periódicamente que aseguren el buen funcionamiento del sistema y todos los incidentes de seguridad deben ser reportados, evaluados y resueltos por la persona encargada.

La División de Sistemas y por ende la Universidad del Cauca se encuentran comprometidos con la SI del SPEL, para lo cual definen procesos y mecanismos que ayudan a la obtención de la misma y garantizan la preservación, confidencialidad, disponibilidad y no repudio de la información de los usuarios y del SPEL.

De acuerdo a las metas de seguridad establecidas se definieron Políticas de Seguridad para el desarrollo, uso y administración del SPEL de la Universidad del Cauca las cuales deben cumplir las personas involucradas con el sistema.

Garantizar que el ciclo de desarrollo de las aplicaciones del SPEL sea seguro y confiable y que proteja la integridad de la información.

DESARROLLADORES

1. Las aplicaciones software del SPEL y desarrolladas por el personal que labora en la División de Sistemas son de propiedad exclusiva de la misma. Se debe dejar explícito el tipo de licencia que cubre la aplicación.
2. Para el desarrollo de la aplicación del SPEL se debe establecer el ciclo de desarrollo del software, que involucre la gestión de la SI en todas sus etapas de desarrollo,

teniendo en cuenta pruebas, licencias y documentación de la aplicación, así como la formación del personal involucrado en el funcionamiento adecuado del SPEL.

3. El ambiente de desarrollo debe tener características similares tanto software como hardware, con relación al ambiente de producción.
4. Debe existir un ambiente de pruebas con iguales características software y hardware, al ambiente de producción.
5. La autenticación a la aplicación del SPEL debe realizarse mediante usuario y contraseña la cual es conocida únicamente por la persona que desea ingresar.
6. Se debe realizar respaldo de los códigos fuente y de los archivos ejecutables en un área de almacenamiento de acceso restringido, externa al ambiente de producción y pruebas, conservando el estado cronológico de las versiones.
7. La aplicación del SPEL debe contar con un manual de procedimientos para su puesta en marcha y su adecuado funcionamiento.
8. La aplicación del SPEL debe ser configurada y validada en un ambiente de pruebas antes de pasar al ambiente de producción.
9. La aplicación debe generar un archivo donde se reporte las operaciones (consultas, transacciones, errores) realizadas.

ADMINISTRADORES

10. Las contraseñas involucradas en el SPEL son de exclusiva responsabilidad del administrador encargado.
11. Las pruebas de funcionamiento y de seguridad deben ser documentadas y aprobadas para que la aplicación o sus actualizaciones pasen al ambiente de producción.
12. Las aplicaciones deben ser actualizadas o modificadas única y exclusivamente por personal autorizado para tal fin.
13. Los administradores deben estar en la capacidad de resolver cualquier situación imprevista presentada en el SPEL.

Disponer de una arquitectura de red óptima que garantice un flujo seguro de información.

ADMINISTRADORES

14. Establecer indicadores para medir el uso y la calidad del servicio.
15. La aplicación del SPEL debe estar disponible las 24 horas del día durante el calendario académico para su operación por parte de los usuarios.
16. Cuando el SPEL se encuentre fuera de servicio se debe restablecer en el menor tiempo posible.
17. Se deben revisar periódicamente los logs (archivos de bitácora) y los registros de la aplicación.

18. El acceso a los equipos relacionados con el SPEL solo se permite al personal encargado de la administración y funcionamiento de los mismos.
19. El SPEL se debe encontrar dentro de la zona desmilitarizada DMZ (demilitarized zone) y debe estar protegido por un firewall que bloquee el acceso de paquetes de información con el fin de reducir el tráfico que sature la red.
20. Se deben cambiar las contraseñas de los equipos relacionados con el SPEL desde el inicio del desarrollo de la aplicación.
21. Se deben realizar copias de seguridad de los archivos de configuración periódicamente y cada vez que se realice una modificación teniendo en cuenta que no pueden ser modificados sin previo aviso. Los archivos de configuración son de acceso restringido a los administradores del sistema.
22. La arquitectura de red del SPEL debe estar documentada así como la evolución de las modificaciones que se le realicen.
23. Todos los equipos y elementos de red involucrados en el SPEL deben estar actualizados a versiones estables conocidas, tendiendo a conservar e incrementar la calidad del servicio que prestan, mediante la mejora de su desempeño. Las actualizaciones se deben realizar de acuerdo a lo establecido por la División de Sistemas y con el aval de esta.
24. Los recursos destinados para el desarrollo del SPEL serán de uso exclusivo de éste y no podrán ser compartidos con otros servicios o destinados para uso personal.
25. Es imprescindible que todos los equipos involucrados en el SPEL utilicen software de seguridad como antivirus actualizados, antispyware, protección *peer to peer* y otros que apliquen, con el propósito de proteger la integridad del sistema.
26. Se debe contar con un certificado de servidor seguro válido, reconocido por una entidad certificadora y correctamente instalado.
27. Todos los equipos pertenecientes al SPEL deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

Establecer medidas de seguridad en las instalaciones físicas de tal forma que se proteja el talento humano, los equipos y el sistema en general

ADMINISTRADORES

28. Todos los equipos y elementos de red involucrados en el SPEL deben encontrarse en lugares apropiados y restringidos, de tal forma que se encuentren protegidos contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.
29. Las instalaciones deben ser adecuadas para los equipos del SPEL para lo cual deben contar con piso falso, cableado estructurado de datos y eléctricos, refrigeración y otras que apliquen.

30. Las instalaciones donde se encuentren los equipos deben contar con elementos de seguridad adecuados como extintores (de diferentes tipos), detectores de humo y fuego, rutas de evacuación y otros que ayuden en situaciones de emergencia.
31. Se debe contar con una fuente de energía alterna.
32. Solo las personas autorizadas pueden acceder a las áreas donde se encuentran los equipos y elementos de red involucrados en el SPEL con el fin de salvaguardar la información que allí se almacena. Estas áreas deben contar con sistemas de control de acceso como chapas de seguridad, cámaras, alarmas, tarjetas inteligentes, dispositivos biométricos entre otros.
33. Debe existir un sistema que registre a todas las personas que entran y salen de las instalaciones donde se encuentran los equipos y el motivo de su ingreso.
34. Se debe reportar a los administradores de las instalaciones las fallas de seguridad física detectadas.
35. Está prohibido el acceso de comidas y bebidas al área de equipos.

Conservar la confiabilidad, integridad, disponibilidad y no repudio de la información

USUARIOS

36. La contraseña para acceder al SPEL es creada por el usuario, es de uso personal e intransferible y está bajo la responsabilidad de cada persona.
37. La contraseña debe tener mínimo 8 caracteres que puede incluir números, letras y símbolos.
38. La contraseña del usuario debe ser modificada cada periodo académico.
39. Tener autorización de su Entidad Financiera y/o conocer el procedimiento para realizar transacciones por Internet con su cuenta bancaria.
40. Descargar el comprobante del resultado de la transacción.

ADMINISTRADORES

41. La información confidencial del SPEL no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de la Institución.
42. Los funcionarios no deben eliminar, copiar o distribuir los archivos relacionados con el SPEL y deben velar por la integridad de la información confiada.
43. Se deben utilizar medios criptográficos para la transmisión interinstitucional de la información confidencial del SPEL.

Realizar supervisión y pruebas periódicamente que aseguren el buen funcionamiento del sistema

ADMINISTRADORES

44. Se debe definir un plan para la realización de las pruebas de funcionamiento y de seguridad.
45. Establecer jornadas de mantenimiento preventivo para software y hardware, a todo equipo perteneciente a la red del SPEL, de tal forma que el riesgo de fallas se mantenga en una probabilidad de ocurrencia baja.
46. Se realizará un monitoreo constante del SPEL.

Todos los incidentes de seguridad deben ser reportados, evaluados y resueltos por la persona encargada

ADMINISTRADORES

47. Establecer un procedimiento de reporte de incidentes relacionados con el SPEL, además de tiempos determinados para dar la solución y tomar las medidas correctivas.
48. Las personas encargadas del SPEL son responsables de registrar y reportar las violaciones a la seguridad, aparición de virus, programas sospechosos e intentos de intrusión y no se debe difundir esta información interna o externamente.
49. Establecer procedimientos de control y validaciones para las transacciones rechazadas o pendientes de procesar.

3.1.2 Determinar los riesgos del SPEL.

Para el desarrollo de este lineamiento se tuvo en cuenta la ISO/IEC 27001, ISO/IEC 27005 y la Metodología Margerit [79], por lo cual se identificaron activos, amenazas, riesgos y medidas para mitigar los riesgos presentados. La información para el desarrollo de este lineamiento como el valor de los activos, amenazas, frecuencia de ocurrencia, efectividad de los controles, se tomaron teniendo en cuenta los datos suministrados por el Ingeniero Héctor Henry Jurado [80] para los campos relacionados con el SEPL y los funcionarios de la división de sistemas para todo lo relacionado con las redes y los ambientes de desarrollo.

Los activos del SPEL se han divido en 8 grupos, Información, Aplicaciones (SW), Equipos (HW), Servicios (S), Redes (R), Equipamiento Auxiliar (AUX), Instalaciones (L), Personas (P), esto permite su fácil identificación y además se han seleccionado de acuerdo al valor que representan para el sistema.

- Información (I):

(1) Base de datos de usuario
(2) Datos ACH
(3) Datos de Configuración
(4) Datos de Conciliación
(5) Datos Certificado Servidor Seguro
(6) Direccionamiento IP
(7) Manuales de Usuario
(8) Copias de respaldo
(9) Políticas de Seguridad
(10) Códigos fuente
(11) Librerías Java

- Aplicaciones (SW):

(12) Aplicación SPEL
(13) Aplicación de Generación de Certificados
(14) WS-Security – extensión de seguridad para mensajes SOAP
(15) Apache Tomcat (Servidor de Aplicaciones Web)
(16) Oracle (Sistema de Gestión de Base de Datos)
(17) Antivirus
(18) Debian (Sistema Operativo)
(19) Firewall (Iptables)

- Equipos (HW):

(20) Servidor de Aplicaciones
(21) Servidor de Base de datos
(22) Servidor Web
(23) Servidor de Pruebas
(24) Elementos de Interconexiones de Red
(25) Firewall
(26) Computadores de usuarios

- Servicios (S):

(27) HTTPs
(28) Consulta de recibo
(29) Pago en línea

- Redes (R):

(30) Red Local LAN

(31) Red Metropolitana MAN
(32) VPN

- Equipamiento Auxiliar (AUX):

(33) Fuentes de alimentación
(34) Sistemas de alimentación ininterrumpida (UPS)
(35) Cableado
(36) Armarios
(37) Equipos de refrigeración.

- Instalaciones (L):

(38) Sala de Servidores.

- Personas (P):

(39) Administradores del SPEL (Área de Servidores, Área de Infraestructura, Área de Desarrollo de Aplicaciones)
(40) Usuarios externos (Estudiantes, Docentes).

Ya identificados los activos se debe realizar su valoración, esto se hizo de una manera cualitativa para lo cual es necesario tener criterios de valoración, por lo tanto se tomó como referencia lo que propone Margerit [81].

Tabla 5. Descripción de valores y criterios

VALOR		CRITERIO
10	Muy alto	Daño muy grave al sistema
7-9	Alto	Daño grave al sistema
4-6	Medio	Daño importante al sistema
1-3	Bajo	Daño menor al sistema
0	Despreciable	Irrelevante a efectos prácticos

La valoración de los activos se va a tener en cuenta de acuerdo a los siguientes atributos o características:

- Disponibilidad (D): El activo debe encontrarse siempre disponible cuando los usuarios autorizados quieran acceder a él. ¿Qué importancia tendría que el activo no estuviera disponible?

- Integridad (I_D): La información debe permanecer exacta y completa. ¿Qué importancia tendría que los datos fueran modificados fuera de control?

- Confidencialidad (C): Solo personas autorizadas deben acceder a la información. ¿Qué importancia tendría que los datos fueran conocidas por personas no autorizadas?

- Autenticidad de los usuarios (A_U): Garantizar la identidad del usuario. ¿Qué importancia tendría que quien accede al activo no es realmente quien se cree?

- Trazabilidad del Servicio (T_S): En todo momento se debe determinar que transacciones realiza cada usuario y en qué tiempo. ¿Qué importancia tendría que no quedara constancia del uso del activo?

De acuerdo a lo anterior se realizó la valoración de los activos la cual se consigna en la siguiente tabla.

Tabla 6. Valoración de Activos

ACTIVO		D	I_D	C	A_U	T_S	VALOR ACTIVO
Información (I)	(1)	10	10	10	10	10	10
	(2)	0	3	6	7	2	4
	(3)	9	9	9	6	2	7
	(4)	0	8	2	2	6	4
	(5)	6	0	0	0	5	2
	(6)	9	9	9	3	9	8
	(7)	6	6	7	0	0	4
	(8)	0	8	8	8	2	6
	(9)	7	7	7	7	7	7
	(10)	9	9	9	9	9	9
	(11)	8	6	0	0	0	3
Aplicaciones (SW)	(12)	10	10	10	10	10	10
	(13)	6	0	0	0	0	6
	(14)	6	4	4	4	2	4
	(15)	10	1	1	1	9	5
	(16)	10	10	10	10	10	10
	(17)	6	0	0	0	0	6
	(18)	10	0	0	0	6	8
	(19)	9	7	7	1	7	6
Equipos (HW)	(20)	10	5	5	5	5	6
	(21)	10	9	9	10	9	10
	(22)	1	4	4	0	0	2
	(23)	5	3	8	7	5	6
	(24)	10	7	6	8	5	7
	(25)	8	8	7	8	7	8

	(26)	10	7	5	6	5	7
Servicios (S)	(27)	10	10	10	10	8	10
	(28)	6	10	6	8	6	7
	(29)	10	10	10	8	10	10
Redes (R)	(30)	5	8	5	5	6	6
	(31)	10	10	8	8	8	9
	(32)	10	10	8	8	8	9
Equipamiento Auxiliar (AUX)	(33)	10	10	8	10	7	9
	(34)	8	10	8	10	7	9
	(35)	10	10	8	10	7	9
	(36)	6	10	8	10	7	8
	(37)	6	10	8	10	7	8
Instalaciones (L)	(38)	10	10	8	10	8	9
Personas (P)	(39)	8	8	9	9	8	8
	(40)	8	8	9	8	7	8

Una vez valorados los activos se deben identificar las posibles amenazas que pueden afectarlos, las cuales se clasificaron en 4 grupos de acuerdo naturaleza y se consignan en las siguientes tablas.

Tabla 7. Amenazas por Desastres Naturales (DN) que pueden afectar el SPEL

DN1. Incendios	
Activos: (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar (L). Instalaciones	Dimensiones: (D). Disponibilidad (T_S). Trazabilidad del Servicio
DN2. Inundaciones	
Activos: (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar (L). Instalaciones	Dimensiones: (D). Disponibilidad (T_S). Trazabilidad del Servicio
DN3. Otros. (Rayos, tormentas eléctricas, terremotos, avalancha, entre otros)	
Activos: (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar (L). Instalaciones	Dimensiones: (D). Disponibilidad (T_S). Trazabilidad del Servicio

Tabla 8. Amenazas por Origen Industrial (OI) que pueden afectar el SPEL

OI1. Avería de Origen Físico o Lógico	
Activos: (HW). Equipos (SW). Aplicaciones (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar	Dimensiones: (D). Disponibilidad (T_S). Trazabilidad del Servicio
OI2. Corte del suministro eléctrico.	
Activos: (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar	Dimensiones: (D). Disponibilidad (T_S). Trazabilidad del Servicio
OI3. Condiciones inadecuadas de temperatura y/o humedad.	
Activos: (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar	Dimensiones: (D). Disponibilidad (T_S). Trazabilidad del Servicio
OI4. Fallos en los servicios de comunicaciones.	
Activos: (R). Redes	Dimensiones: (D). Disponibilidad

Tabla 9. Amenazas por Errores y fallas no intencionadas (E) que pueden afectar el SPEL

E1. Errores de los usuarios.	
Activos: (I). Información (SW). Aplicaciones	Dimensiones: (D). Disponibilidad (I_D). Integridad
E2. Errores de los administradores.	
Activos: (I). Información (S). Servicios (SW). Aplicaciones (HW). Equipos (R). Redes	Dimensiones: (D). Disponibilidad (I_D). Integridad (C). Confidencialidad (A_U). Autenticidad de los usuarios (T_S). Trazabilidad del Servicio
E3. Errores de Configuración.	
Activos: (I). Información (S). Servicios (SW). Aplicaciones (HW). Equipos	Dimensiones: (D). Disponibilidad (I_D). Integridad (C). Confidencialidad (A_U). Autenticidad de los usuarios

(R). Redes	(T_S). Trazabilidad del Servicio
E4. Deficiencias en la Organización	
Activos: (P). Personas	Dimensiones: (D). Disponibilidad
E5. Propagación de virus, gusanos, troyanos, bombas lógicas, espías, etc.	
Activos: (SW). Aplicaciones	Dimensiones: (D). Disponibilidad (I_D). Integridad (C). Confidencialidad (A_U). Autenticidad de los usuarios (T_S). Trazabilidad del Servicio

Tabla 10. Amenazas por Ataques intencionados (AI) que pueden afectar el SPEL

A1. Denegación de Servicio	
Activos: (S). Servicios (HW). Equipos (R). Redes	Dimensiones: (D). Disponibilidad
A2. Ingeniería Social	
Activos: (P). Personas	Dimensiones: (D). Disponibilidad (I_D). Integridad (C). Confidencialidad (A_U). Autenticidad de los usuarios (T_S). Trazabilidad del Servicio
A3. Phishing y Pharming	
Activos: (I). Información (R). Redes	Dimensiones: (I_D). Integridad (C). Confidencialidad
A4. Spoofing	
Activos: (S). Servicios (SW). Aplicaciones (R). Redes	Dimensiones: (I). Integridad (C). Confidencialidad (A_U). Autenticidad de los usuarios
A5.Keylogger	
Activos: (I). Información	Dimensiones: (I_D). Integridad (C). Confidencialidad
A6.Acceso no autorizado	
Activos: (I). Información (S). Servicios	Dimensiones: (I_D). Integridad (C). Confidencialidad de los datos

(SW). Aplicaciones (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar (L). Instalaciones	(A_U). Autenticidad de los usuarios del servicio
A7.Robo	
Activos: (HW). Equipos (R). Redes (S_I). Soportes de información (AUX). Equipamiento Auxiliar	Dimensiones: (D). Disponibilidad (C). Confidencialidad de los datos

Es importante valorar: el nivel de riesgo, el impacto y determinar la frecuencia de ocurrencia de las amenazas, para esto se estableció una escala de valoración de 1 a 5 [76].

Para calcular el impacto se tiene en cuenta esta escala donde 5 es el mayor valor que se le puede dar a los daños causados por dicho impacto al activo y por ende al funcionamiento del sistema.

Tabla 11. Valoración del impacto

VALORACION	DESCRIPCION DEL IMPACTO
5	Alto
4	Moderado
3	Medio
2	Bajo
1	Insignificante

Para calcular la frecuencia en la escala de valoración, el 5 es el mayor valor que se le da a un evento muy frecuente y 1 a un evento de poca probabilidad de ocurrencia.

Tabla 12. Valoración de la Frecuencia

VALORACION	DESCRIPCION DE LA FRECUENCIA
5	Ocurre una vez al día
4	Ocurre una vez a la semana
3	Ocurre una vez al mes
2	Ocurre una vez al año
1	Intervalos superiores a un año

De acuerdo a las escalas de valoración anteriores se calculó el impacto, la frecuencia y el nivel de riesgo (f * I) respecto a cada una de las amenazas encontradas.

f: Frecuencia

I: Impacto

NR: Nivel de Riesgo

V: Valor

Tabla 13. Nivel de Riesgo respecto a las posibles amenazas.

TIPOS DE AMENAZAS		(f)	(I)	(NR)
DESASTRES NATURALES	Incendios	1	5	5
	Inundaciones	1	5	5
	Otros	1	5	5
AMENAZAS POR ORIGEN INDUSTRIAL	Avería de Origen Físico o Lógico	3	3	9
	Corte del Suministro Eléctrico	3	4	12
	Condiciones inadecuadas de temperatura y/o humedad	2	3	6
	Fallos de los servicios de comunicaciones	3	4	12
AMENAZAS POR ERRORES Y FALLAS NO INTENCIONADAS	Errores de los usuarios	4	2	8
	Errores de los Administradores	4	3	12
	Errores de Configuración	2	4	8
	Deficiencias de la Organización	3	3	9
	Propagación de virus, gusanos, troyanos, bombas lógicas, espías, etc.	4	4	16
AMENAZAS POR ATAQUES INTENCIONADOS	Denegación de Servicio	3	5	15
	Ingeniería Social	2	4	8
	Phishing y Pharming	2	5	10
	Spoofing	2	4	8
	Keylogger	3	4	12
	Acceso no autorizado	2	5	10
	Robo	2	5	10

Tabla 14. Nivel de Riesgo respecto a los activos.

ACTIVO		V	f	I	NR
Información (I)	(1)	10	2	5	10
	(2)	4	1	2	2
	(3)	7	2	4	8
	(4)	4	1	4	4
	(5)	2	1	2	2
	(6)	8	3	4	12
	(7)	4	2	3	6
	(8)	6	2	4	8
	(9)	7	4	3	12

	(10)	9	2	3	6
	(11)	3	1	3	3
Aplicaciones (SW)	(12)	10	2	5	10
	(13)	6	2	3	6
	(14)	4	2	4	8
	(15)	5	3	5	15
	(16)	10	2	5	10
	(17)	6	3	4	12
	(18)	8	2	5	10
	(19)	6	2	3	6
Equipos (HW)	(20)	6	2	5	10
	(21)	10	2	5	10
	(22)	2	2	5	10
	(23)	6	2	3	6
	(24)	7	2	4	8
	(25)	8	2	4	8
	(26)	7	3	4	12
Servicios (S)	(27)	10	5	5	25
	(28)	7	2	5	10
	(29)	10	3	5	15
Redes (R)	(30)	6	4	3	12
	(31)	9	2	3	6
	(32)	9	2	5	10
Equipamiento Auxiliar (AUX)	(33)	9	3	2	6
	(34)	9	2	2	4
	(35)	9	2	2	4
	(36)	8	1	2	2
	(37)	8	2	2	4
Instalaciones (L)	(38)	9	2	4	8
Personas (P)	(39)	8	3	4	12
	(40)	8	3	4	12

Dado el nivel de riesgo encontrado, se analizan los controles de seguridad existentes [76], [82], [83] para cada uno de los activos y se valoran estas medidas de protección de acuerdo a la siguiente tabla.

Tabla 15. Valoración de las Medidas de Protección

VALORACION	DESCRIPCION DE LAS MEDIDAS DE PROTECCION
5	Alto
4	Moderado
3	Medio
2	Bajo
1	Ninguno

Teniendo en cuenta el nivel de riesgo encontrado, los controles existentes y la efectividad de los mismos se calcula el riesgo residual (NR / E) así como lo muestra la siguiente tabla.

NR: Nivel de Riesgo

E: Efectividad

RR: Riesgo Residual

Tabla 16. Controles existentes y Riesgo Residual respecto a las posibles amenazas.

TIPOS DE AMENAZAS		NR	Control	E	RR
DESASTRES NATURALES	Incendios	5	Extinguidor	2	2.5
	Inundaciones	5	Ninguno	1	5
	Otros	5	Sistemas de Evacuación	2	2.5
AMENAZAS POR ORIGEN INDUSTRIAL	Avería de Origen Físico o Lógico	9	Reparación y Sustitución	4	2.25
	Corte del Suministro Eléctrico	12	UPS y Planta Eléctrica	3	4
	Condiciones inadecuadas de temperatura y/o humedad	6	Ubicación de las instalaciones	3	2
	Fallos de los servicios de comunicaciones	12	Se cuenta con VPN y canal de Internet de respaldo	3	4
AMENAZAS POR ERRORES Y FALLAS NO INTENCIONADAS	Errores de los usuarios	8	Ninguno	1	8
	Errores de los Administradores	12	Ninguno	1	12
	Errores de Configuración	8	Ninguno	1	8
	Deficiencias de la Organización	9	Perfil del Cargo y sus funciones	3	3
	Propagación de virus, gusanos, troyanos, bombas lógicas, espías, etc.	16	Antivirus	3	5.3
AMENAZAS POR	Denegación de Servicio	15	Firewall	4	3.75

ATAQUES INTENCIONADOS	Ingeniería Social	8	Ninguno	1	8
	Phishing y Pharming	10	Ninguno	1	10
	Spoofing	8	Ninguno	1	8
	Keylogger	12	Ninguno	1	12
	Acceso no autorizado	10	Control de acceso	4	2.5
	Robo	10	Control de acceso	4	2.5

Tabla 17. Controles existentes y Riesgo Residual respecto a los activos

ACTIVO		NR	Control	E	RR
Información (I)	(1)	10	Copias de Seguridad	3	3.3
	(2)	2	Ninguno	1	2
	(3)	8	Ninguno	1	8
	(4)	4	Ninguno	1	4
	(5)	2	Ninguno	1	2
	(6)	12	Ninguno	1	12
	(7)	6	Ninguno	1	6
	(8)	8	Ninguno	1	8
	(9)	12	Ninguno	1	12
	(10)	6	Ninguno	1	6
	(11)	3	Ninguno	1	3
Aplicaciones (SW)	(12)	10	Ninguno	1	10
	(13)	6	Ninguno	1	6
	(14)	8	Ninguno	1	8
	(15)	15	Ninguno	1	15
	(16)	10	Gestión de Usuarios	3	3.3
	(17)	12	Actualizaciones	4	3
	(18)	10	Ninguno	1	10
	(19)	6	Ninguno	1	6
Equipos (HW)	(20)	10	Ninguno	1	10
	(21)	10	Ninguno	1	10
	(22)	10	Ninguno	1	10
	(23)	6	Ninguno	1	6
	(24)	8	Redundancia	3	2.6
	(25)	8	Redundancia	3	2.6
	(26)	12	Redundancia	3	4
Servicios (S)	(27)	25	Ninguno	1	25
	(28)	10	Ninguno	1	10
	(29)	15	Ninguno	1	15
Redes (R)	(30)	12	Ninguno	1	12
	(31)	6	Respaldo	4	1.5
	(32)	10	Respaldo	4	2.5
Equipamiento Auxiliar (AUX)	(33)	6	Respaldo	3	2
	(34)	4	Respaldo	3	1.3
	(35)	4	Cableado	3	1.3

			Estructurado		
	(36)	2	Adecuación de Armarios	3	0.6
	(37)	4	Ninguno	1	4
Instalaciones (L)	(38)	8	Control de Acceso	4	2
Personas (P)	(39)	12	Varios Administradores	3	4
	(40)	12	Ninguno	1	12

3.1.3 Crear o seleccionar los controles y procedimientos para la SI del SPEL

Dado que el análisis anterior evidenció la falta de controles que mitiguen el riesgo es necesario crear unos de acuerdo a la ISO/IEC 27002, las políticas de seguridad planteadas para el SPEL y el análisis de riegos del mismo.

La siguiente tabla enuncia el control y sus respectivos activos y amenazas.

Tabla 18. Controles a implementar

	Control	Activo	Amenaza	Efectividad
1. Documento de la Política de seguridad de la información con copia de respaldo.	Se debe tener un documento que especifique las políticas de seguridad de la información el cual debe ser aprobado, publicado y comunicado a todas las personas involucradas con el sistema, además debe contar con copia de respaldo.	9	E1 E2 E3 E4	4
2. Revisión de la Política de seguridad de la información.	Se debe revisar el documento generado en el control anterior cada determinado intervalo de tiempo, de tal forma que se incluyan cambios o mejoras para con el fin de mantener su eficiencia y efectividad.	9	E1 E2 E3 E4	3
3. Organización Interna del Personal.	Se deben definir claramente los roles que desempeña el personal encargado del sistema, así	7	E4	4

	como la asignación de funciones y responsabilidades.			
4. Acuerdos de confidencialidad.	Se deben establecer acuerdos de confidencialidad o no divulgación con el fin de proteger toda la información concerniente al SPEL teniendo en cuenta términos legales vigentes y ejecutables. Se deben revisar constantemente y cuando ocurran cambios significativos.	1 – 11	A2 A6	4
5. Contacto con las autoridades.	Se debe definir a que autoridades internas a la Universidad se debe acudir y en qué casos específicos como por ejemplo, jefe de área, administrador del sistema, jefe de división de sistemas, rector. En caso necesario se debe recurrir a autoridades externas, las cuales deben definirse como por ejemplo policía, bomberos, proveedor de servicio.	20 - 26 31	DN1 DN2 DN3 OI4 A1 - A6	4
6. Inventario de los Activos.	Todos los activos deben ser inventariados y se les debe asignar una persona responsable de ellos que garantice la seguridad de los mismos.	1-40	E4	4
7. Conocimiento, educación y capacitación en seguridad de la información.	Todas las personas encargadas del SPEL así como sus usuarios deben capacitarse continuamente en seguridad de la información y políticas de seguridad	1- 38	E1 – E5 A1 – A6	4
8. Perímetro de seguridad Física.	Se deben establecer perímetros de seguridad (paredes, puertas, barreras, detección de intrusos, entre otros) para la sala de servidores donde se	38	A6 A7	4

	encuentran activos relacionados con el SPEL			
9. Control de ingreso físico.	Se deben establecer procedimientos que permitan llevar un control de acceso a las instalaciones, teniendo en cuenta el tipo de personas y el motivo del ingreso.	38	A6 A7	4
10. Protección contra amenazas por desastres naturales.	Se deben establecer medidas que protejan a los activos de inundaciones, incendios, terremotos, tormenta eléctrica y otros.	1-38	DN1 DN2 DN3	3
11. Cableado Estructurado.	Se deben tomar todas las medidas de seguridad necesarios que protejan el cableado y tomar en cuenta las especificaciones que se deben tener para cableado estructurado.	35	OI1 E3 A6	4
12. Mantenimiento de Equipos.	Se debe realizar un mantenimiento predictivo, preventivo y correctivo continuo a los equipos para garantizar la continua disponibilidad e integridad de los activos.	20 – 26 30 - 32	OI1 OI4	3
13. Gestión de software.	Se deben planear todos los cambios al sw que se realicen, se debe probar y aceptar el sw antes de ponerse en funcionamiento, de esta forma se minimizan las fallas y se evitan problemas con la disponibilidad del sistema, además se deben realizar proyecciones de capacidad para asegurar el desempeño del sistema en un futuro.	12 – 19	OI1 OI4 A1	3
14. Protección contra códigos maliciosos.	Se deben definir medidas que detecten códigos maliciosos, recuperen el software, controlen el acceso al hw y sw y conciencien a las personas	1 – 29	E5 A1 – A6	4

	involucradas con el SPEL.			
15. Respaldo.	Se deben realizar copias de respaldo tanto a la información como al sw y además a equipos que permitan la continuidad del negocio, teniendo en cuenta la seguridad física de los mismos.	1 – 19	DN1 DN2 DN3 E3 A1 – A7	5
16. Control de redes.	Se debe establecer mecanismos de seguridad para proteger la información que transita por la red así como los sistemas y aplicaciones de la misma.	30 - 32	E4 A1 - A7	4
17. Documentación del Sistema.	Proteger la documentación del sistema de accesos no autorizados.	1-11	A2 A6 A7	5
18. Seguridad de las transacciones.	La información involucrada en las transacciones debe protegerse de acciones fraudulentas, divulgación no autorizada y modificación.	1 - 19	A1 – A7	4
19. Gestión de contraseñas.	Las contraseñas de los administradores y de los usuarios deben gestionarse de tal forma que no generen riesgo para la seguridad del sistema. Se deben exigir buenas prácticas en la generación y gestión de contraseñas.	1 12 15 16 18 19	E1 E2 A2 A6 A7	4
20. Control de acceso al código fuente del programa.	Se debe restringir el acceso al código fuente del programa y crear respaldo del mismo para evitar cambios no autorizados y proteger la integridad de la aplicación.	12	A4 A6	4
21. Filtración de información.	Se debe diseñar políticas y procedimientos para el manejo y transmisión de la información y así evitar las oportunidades para la filtración de la misma.	1-19	E5 A1 A2 A4 A5	4

22. Reporte de debilidades e incidentes de seguridad.	Establecer un procedimiento para el reporte de eventos de seguridad que tenga en cuenta oficina responsable, formato de recepción de eventos y respuesta de eventos, así como también sus debilidades.	Todos	Todas	3
23. Gestión de continuidad del negocio.	Se debe diseñar un plan de continuidad de negocio.	Todos	Todas	4
24. Identificación de la legislación aplicable.	Identificar y documentar toda la legislación colombiana o Internacional que aplique al SPEL, tener en cuenta la ley sobre delitos informáticos del país y el reglamento de la División de Sistemas.	Todos	Todas	3
25. Auditoría.	Realizar una auditoría periódica que permita identificar fallas en el sistema o en el cumplimiento de los controles y políticas de seguridad.	Todos	Todas	4

Si la División de Sistemas implementa estos controles el RR se disminuiría de la siguiente manera:

%: Porcentaje de disminución del riesgo residual

Tabla 19. Controles a implementar, Riesgo Residual respecto a las posibles amenazas y porcentaje de disminución de riesgos.

TIPOS DE AMENAZAS		NR	Control	E	RR	%
DESASTRES NATURALES	Incendios, Inundaciones, Otros	5	5, 10, 15, 22, 23, 24, 25	4	1.25	48%
AMENAZAS POR ORIGEN INDUSTRIAL	Avería de Origen Físico o Lógico	9	11, 12, 22, 23 24, 25	4	2.25	45%
	Corte del Suministro Eléctrico	12	22, 23 24, 25	4	3	75%
	Condiciones inadecuadas de temperatura y/o humedad	6	22, 23 24, 25	4	1.5	75%

	Fallos de los servicios de comunicaciones	12	5, 12 13, 22 23, 24 25	4	3	75%
AMENAZAS POR ERRORES Y FALLAS NO INTENCIONADAS	Errores de los usuarios	8	1, 2 7, 19 22, 23 24, 25	4	2	25%
	Errores de los Administradores	12	1, 2 7, 19 22, 23 24, 25	4	3	25%
	Errores de Configuración	8	1, 2 7, 11 15, 22 23, 24 25	4	2	25%
	Deficiencias de la Organización	9	1, 2 3, 6 7, 16 22, 23 24, 25	4	2.25	75%
	Propagación de virus, gusanos, troyanos, bombas lógicas, espías, etc.	16	7, 14 21, 22 23, 24 25	4	4	75%
AMENAZAS POR ATAQUES INTENCIONADOS	Denegación de Servicio	15	5, 6 13, 14 15, 16 18, 21 22, 23 24, 25	4	3.75	0%
	Ingeniería Social	8	4, 5 7, 14 15, 16 17, 18 19, 21 22, 23 24, 25	4	2	25%
	Phishing y Pharming	10	5, 7 14, 15 16, 18 22, 23 24, 25	4	2.5	25%
	Spoofing	8	5, 7 14, 15 16, 18 20, 21	4	2	25%

			22, 23 24, 25			
	Keylogger	12	5, 7 14, 15 16, 18 21, 22 23, 24 25	4	3	25%
	Acceso no autorizado	10	5, 7 8, 9 11, 14 15, 16 17, 18 20, 22 23, 24 25	4	2.5	0%
	Robo	10	8, 9 15, 16 17, 18 19, 22 23, 24 25	4	2.5	0%

Tabla 20. Controles a implementar, Riesgo Residual respecto a los activos y porcentaje de disminución de riesgos.

ACTIVO		NR	Control	E	RR	%
Información (I)	(1)	10	4, 6 7, 10 14, 15 17, 18 19, 21 22, 23 24, 25	4	2.5	75%
	(2)	2	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	0.5	25%
	(3)	8	4 ,6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	2	25%
	(4)	4	4, 6	4	1	25%

			7,10 14,15 17, 18 21, 22 23, 24 25			
	(5)	2	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	0.5	25%
	(6)	12	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	3	25%
	(7)	6	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	1.5	25%
	(8)	8	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	2	25%
	(9)	12	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	3	25%
	(10)	6	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	1.5	25%

	(11)	3	4, 6 7, 10 14, 15 17, 18 21, 22 23, 24 25	4	0.75	25%
Aplicaciones (SW)	(12)	10	6, 7 10, 13 14, 15 18, 19 20, 21 22, 23 24, 25	4	2.5	25%
	(13)	6	6, 7 10, 13 14, 15 18, 21 22, 23 24, 25	4	1.5	25%
	(14)	8	6, 7 10, 13 14, 15 18, 21 22, 23 24, 25	4	2	25%
	(15)	15	6, 7 10, 13 14, 15 18, 19 21, 22 23, 24 25	4	3.75	25%
	(16)	10	6, 7 10, 13 14, 15 18, 19 21, 22 23, 24 25	4	2.5	75%
	(17)	12	6, 7 10, 13 14, 15 18, 21 22, 23 24, 25	4	3	0%
	(18)	10	6, 7 10, 13	4	2.5	25%

			14, 15 18, 19 21, 22 23, 24 25			
	(19)	6	6, 7 10, 13 14, 15 18, 19 21, 22 23, 24 25	4	1.5	25%
Equipos (HW)	(20)	10	5, 6 7, 10 12, 22 23, 24 25	3	3.3	33%
	(21)	10	5, 6 7, 10 12, 22 23, 24 25	3	3.3	33%
	(22)	10	5, 6 7, 10 12, 22 23, 24 25	3	3.3	33%
	(23)	6	5, 6 7, 10 12, 22 23, 24 25	3	2	33%
	(24)	8	5, 6 7, 10 12, 22 23, 24 25	4	2	77%
	(25)	8	5, 6 7, 10 12, 22 23, 24 25	4	2	7%
	(26)	12	5, 6 7, 10 12, 22 23, 24 25	3	4	0%
Servicios (S)	(27)	25	6, 7	4	6.2	25%

			10, 14 22, 23 24, 25			
	(28)	10	6, 7 10, 14 22, 23 24, 25	4	2.5	25%
	(29)	15	6, 7 10, 14 22, 23 24, 25	4	3.75	25%
Redes (R)	(30)	12	6, 7 10, 12 16, 22 23, 24 25	3	4	33%
	(31)	6	5, 6 7, 10 12, 16 22, 23 24, 25	4	1.5	0%
	(32)	10	6, 7 10, 12 16, 22 23, 24 25	4	2.5	0%
Equipamiento Auxiliar (AUX)	(33)	6	6, 7 10, 22 23, 24 25	4	1.5	75%
	(34)	4	6, 7 10, 22 23, 24 25	4	1	77%
	(35)	4	6, 7 10, 11 22, 23 24, 25	4	1	77%
	(36)	2	6, 7 10, 22 23, 24 25	4	0.5	83%
	(37)	4	6, 7 10, 22 23, 24 25	4	1	25%
Instalaciones (L)	(38)	8	6, 7 8, 9	4	2	0%

			10, 22 23, 24 25			
Personas (P)	(39)	12	6, 22 23, 24 25	4	3	75%
	(40)	12	6, 22 23, 24 25	4	3	25%

Dado el nivel de riesgo respecto a los activos y a las amenazas se evidencia la necesidad que la División de Sistemas implemente estos nuevos controles de seguridad, las tablas anteriores muestran que el porcentaje de disminución del riesgo residual es significativo en la mayoría de las amenazas y activos, además se encontró que algunos de ellos arrojan un porcentaje cero lo cual demuestra que los controles existentes son suficientes aunque no está demás complementarlos con los controles propuestos.

3.1.4 Desarrollar la aplicación del SPEL

En el año 2006 la Universidad del Cauca estableció contacto con ACH, dado su interés de implementar el SPEL con el fin de beneficiar a los estudiantes proporcionando otro medio de pago y beneficiándose la misma institución en la gestión de los pagos y el fácil control de las transacciones.

La División de Sistemas bajo la responsabilidad de un grupo de ingenieros asumió el desarrollo de este proyecto y compró el primer Certificado de Servidor Seguro para la Universidad el cual en el momento se está utilizando para otras aplicaciones; la aplicación se desarrolló en un corto tiempo y no se tuvieron en cuenta las medidas de seguridad necesarias, por ejemplo: no cuenta con controles ni políticas de seguridad, la aplicación no se encontraba en ningún servidor sino que se manejaba directamente desde el entorno de trabajo del ingeniero encargado el cual fue el directamente responsable del sistema, esta persona dejó de trabajar con la Universidad y nadie quedó bajo la responsabilidad del sistema por lo cual dejó de funcionar. La aplicación del SPEL se desarrolló y se encuentra en un equipo fuera de servicio.

La Universidad cuenta con un repositorio de información que hace constar el desarrollo de las fases, tiene los acuerdos con ACH, bosquejo de diagramas UML, manuales de instalación de aplicaciones, código impreso de la aplicación, pantallazos del proceso, certificación de ACH, etc., pero corresponde al primer prototipo que se desarrolló y no permite ver los cambios realizados a la aplicación y su estado actual.

La División de Sistemas está realizando una reestructuración en la cual está previsto integrar sus diferentes sistemas de información, entre ellos el SPEL, pero en el momento no es prioritario este servicio por lo cual aún no se ha dedicado el tiempo suficiente para su puesta en funcionamiento.

No es del alcance de este proyecto la realización de la aplicación del SPEL ni su puesta en marcha.

3.1.5 Implementar los controles y procedimientos seleccionados.

El SPEL de la Universidad del Cauca no se encuentra en funcionamiento actualmente, para su puesta en marcha es necesario establecer nuevamente su interacción con el PSE de ACH ya que ésta terminó cuando el SPEL dejó de funcionar, para ello es necesario tener de nuevo un acercamiento con ACH y diligenciar nuevamente unos registros, la actualización de esta información ya se inició pero se encuentra sometida a procesos administrativos de la Universidad que se salen del tiempo estipulado para este proyecto, es por esto que la implementación de los controles se deja como propuesta para la División de Sistemas ya que este es un servicio importante para la Institución.

a. Documento de la Políticas de seguridad de la información con copia de respaldo.

- Generar un documento que especifique las políticas de seguridad necesarias para proteger el SPEL y su información, el cual debe ser aprobado por la División de Sistemas y la Rectoría de la Universidad.
  Este criterio fue implementado y se puso en conocimiento de la División de Sistemas.
- Realizar una copia de seguridad del documento de las políticas de seguridad y se debe guardar en un lugar diferente y alejado de donde se encuentra el original.
- Comunicar a los administradores y usuarios del SPEL las políticas generadas y firmar acuerdos de confidencialidad para la no divulgación de las mismas a personas externas a la División de Sistemas.
- Capacitar, educar y concienciar a las personas sobre la importancia del cumplimiento de las políticas de seguridad.

b. Revisión de la Política de seguridad de la información.

- Las políticas de seguridad se deben revisar cada año con el fin de analizar cuales se deben modificar, eliminar o cambiar para mantener su eficiencia y efectividad, esto siempre y cuando sean autorizadas por el Jefe de Área y el Jefe de la División de Sistemas.
- Cada tres meses se debe evaluar al personal y sus respectivas actividades para identificar si se están cumpliendo de manera adecuada las políticas de seguridad.

- Establecer procesos disciplinarios para el manejo de las no conformidades presentadas en el cumplimiento de las políticas de seguridad.

c. Organización Interna del Personal.
- Los roles, funciones y responsabilidades se encuentran definidos en la División de Sistemas.

d. Acuerdos de Confidencialidad.
- Firmar acuerdos de confidencial con todos los empleados de la División de Sistemas encargados del SPEL y con las persona externas que por motivo laboral o investigativo tengan acceso al sistema. Ver Anexo B
- En caso de incumplimiento del acuerdo de confidencialidad se deben tomar las medidas legales respectivas.

e. Contacto con las autoridades.

Autoridades Internas:
- En caso de cualquier incidente se debe informar inmediatamente y conservando el conducto regular a:
- Administrador del SPEL
- Jefe de Área
- Jefe de la División de Sistemas
- Vicerrector Administrativo
- Rector

Autoridades Externas
- Vigilancia Privada de la Universidad del Cauca
- En caso de robo a la Policía y DAS
- En caso de incendio a los Bomberos
- Fallas en la Red al Proveedor de Servicio de Internet

f. Inventario de los activos.

- Inventario de todos los activos relacionados con el SPEL. De acuerdo al lineamiento 2 tenemos.

Tabla 21. Inventario de Activos con sus responsables

ACTIVO	RESPONSABLE
(1) Base de datos de usuario	Jefe del Área de Desarrollo
(2) Datos ACH	Jefe del Área de Desarrollo
(3) Datos de Configuración	Jefe del Área de Desarrollo Jefe del Área de Servidores
(4) Datos de Conciliación	Jefe de la División Financiera

(5) Datos Certificado Servidor Seguro	Jefe del Área de Desarrollo
(6) Direccionamiento IP	Jefe del Área de Desarrollo Jefe del Área de Servidores
(7) Manuales de Usuario	Jefe del Área de Desarrollo
(8) Copias de respaldo	Jefe del Área de Desarrollo Jefe de División de Sistemas
(9) Políticas de Seguridad	Jefe de División de Sistemas Jefes de Áreas Monitores
(10) Códigos fuente	Jefe del Área de Desarrollo
(11) Librerías Java	Jefe del Área de Desarrollo
(12) Aplicación SPEL	Jefe del Área de Desarrollo Jefe del Área de Servidores
(13) Aplicación de Generación de Certificados	Jefe del Área de Servidores
(14) WS-Security – extensión de seguridad para mensajes SOAP	Jefe del Área de Desarrollo
(15) Apache Tomcat (Servidor de Aplicaciones Web)	Jefe del Área de Desarrollo Jefe del Área de Servidores
(16) Oracle (Sistema de Gestión de Base de Datos)	Jefe del Área de Desarrollo Jefe del Área de Servidores
(17) Antivirus	Jefe del Área de Servidores
(18) Sistema Operativo (Debian)	Jefe del Área de Servidores Jefe del Área de Desarrollo
(19) Firewall (Iptables)	Jefe del Área de Servidores
(20) Servidor de Aplicaciones	Jefe del Área de Servidores
(21) Servidor de Base de datos	Jefe del Área de Servidores
(22) Servidor Web	Jefe del Área de Servidores
(23) Servidor de Pruebas	Jefe del Área de Servidores Jefe del Área de Desarrollo
(24) Elementos de Interconexiones de Red	Jefe del Área de Infraestructura
(25) Firewall	Jefe del Área de Servidores
(26) Computadores de usuarios	Usuarios Monitores de Salas
(27) HTTPs	Jefe del Área de Servidores
(28) Consulta de Recibo	Jefe del Área de Desarrollo
(29) Pago en línea	Jefe del Área de Desarrollo
(30) Red Local LAN	Jefe del Área de Infraestructura Jefe del Área de Servidores
(31) Red Metropolitana MAN	Jefe del Área de Infraestructura Jefe del Área de Servidores Proveedor de Internet
(32) VPN	Jefe del Área de Servidores

(33) Fuentes de alimentación	Jefe del Área de Infraestructura Jefe del Área de Servidores
(34) Sistemas de alimentación ininterrumpida (UPS)	Jefe del Área de Infraestructura Jefe del Área de Servidores
(35) Cableado	Jefe del Área de Infraestructura
(36) Armarios	Jefe del Área de Infraestructura
(37) Equipos de refrigeración.	Jefe del Área de Infraestructura
(38) Sala de Servidores	Jefe del Área de Servidores
(39) Administradores del SPEL	Jefe de la División de Sistemas
(40) Usuarios Externos	Usuarios Externos

g. Conocimiento, educación y capacitación en seguridad de la información

- Las personas involucradas en el SPEL deben asistir a una conferencia, seminario o taller de seguridad de la información cada seis meses ya sea programada directamente por la Universidad o con una Institución externa.

h. Perímetro de seguridad física.

- Trazar mapa del perímetro físico
- Trazar mapa de las medidas de protección físicas (puertas, ventanas, luces, etc.)
- Trazar mapa de las rutas de acceso.
- Las instalaciones deben encontrarse siempre con la puerta cerrada.
- Cuando no haya personal dentro de las instalaciones se deben dejar la puerta cerrada con llave y las ventanas cerradas y con seguro.
- El ingreso a las instalaciones debe hacerse mediante tarjetas inteligentes
- En las instalaciones debe instalarse una alarma que en el momento de accionarse informe a la Empresa de Seguridad y a la División de Sistemas.

i. Control de ingreso físico

- Debe existir un libro que lleve el registro diario del ingreso de las personas a la sala de servidores, debe contener los siguientes campos: Fecha, hora de entrada, nombre, cargo, motivo de ingreso, hora de salida y firma. Este registro debe ser supervisado por el Jefe de Área. Ver anexo C

j. Protección contra amenazas por desastres naturales

- La sala de servidores debe contar con alarmas contra incendios e inundaciones.
- Los equipos hardware deben ser colocados en gabinetes altos que los proteja en caso de inundación.
- Instalar en la sala de servidores un extintor de solkaflan vigente que proteja los equipos electrónicos.
- Los elementos de combustión o inflamables son prohibidos en la sala de servidores y deben permanecer a una distancia prudente de esta.
- La red eléctrica debe contar con protección de polo a tierra.

k. Cableado estructurado

- El cableado debe debajo de un piso falso y dentro de tubo o canaleta.
- Los cables de energía y los de comunicaciones deben estar separados y marcados para una fácil identificación.
- Se debe tener planos de cableado.
- Tener en cuenta las recomendaciones de la TIA 942.

l. Mantenimiento de Equipos

- Establecer un cronograma de mantenimiento preventivo para cada uno de los equipos según lo estipulado por la División de Sistemas. El mantenimiento debe incluir limpieza de los equipos, arreglo de partes que se encuentre fallando o sustitución de las mismas.

m. Gestión de Software

- La actualización del software solo puede ser realizada por el administrador encargado.
- El software debe instalarse solo después de varias pruebas de utilidad, seguridad, efectos sobre otros sistemas, facilidad de usuario, etc. y solo se puede instalar versiones estables conocidas.
- Mantener copia de respaldo de toda la configuración del sistema.
- Tener una estrategia de “regreso a la situación original” antes de implementar los cambios.
- Tener copia de las versiones anteriores instaladas
- No permitir actualizaciones automáticas.

n. Protección contra códigos maliciosos

- Prohibir el uso e instalación de software no autorizado.
- Instalación y actualización regular de software para la detección de códigos maliciosos.
- Revisión contínua del software instalado.

o. Respaldo

- Realizar copias de seguridad para la información cada semana.
- Realizar copias de seguridad para el software cada que se realice un cambio.
- Las copias de respaldo deben guardarse en lugares diferentes a donde se encuentra la información o software original.
- Deben contar con toda la seguridad física con que cuenta la información original.
- Deben encontrarse protegidos con medios de codificación.
- Solo personas autorizadas pueden acceder a las copias de respaldo.
- Las copias de respaldo solo se pueden utilizar cuando la información original haya sido afectado por una amenaza.

p. Control de Redes
- Establecer controles de acceso a la red.
- Establecer métodos de autenticación para accesos de red remotos.
- Llevar registros de acceso, monitoreo de la red e intentos de acceso fallidos.
- Tener controles de autenticación, codificación y conexión de red.
- Establecer control de acceso público.
- Contar con sistemas de detección de intrusos.
- Establecer control de routing.

q. Documentación del Sistema
- La documentación del sistema debe almacenarse de una manera segura.
- Definir listas de acceso.
- La información que transita por la red debe ir encriptada y codificada.

r. Seguridad de las transacciones
- Tener una conexión válida con el PSE.
- Cualquier transacción, información de pago o datos de usuario deben ser totalmente confidenciales.
- Evitar la pérdida o duplicación de la información de la transacción.
- Hacer uso de firmas digitales.

s. Gestión de contraseñas
- La contraseña debe mantenerse confidencial y no debe divulgarse.
- La contraseña debe ser fácil de recordar, no utilizar información personal, no debe ser una palabra que esté incluida en un diccionario, debe contener números, letras y caracteres especiales.
- La contraseña debe cambiarse cada seis meses.
- Evitar el re-uso de contraseñas antiguas.
- No usar la misma contraseña para otros sistemas.
- Almacenar y transmitir las contraseñas en un formato protegido.

t. Control de acceso al código fuente de los programas
- Establecer listas de acceso.
- El código fuente debe encontrarse protegido con medios de codificación.

u. Filtración de información
- Escanear el flujo de entrada de la red en busca de información escondida.
- Monitoreo constante del personal y sus actividades.
- Monitoreo de la utilización de los recursos del sistema.
- Mantener políticas de acceso.

v. Reporte de debilidades e incidentes de seguridad

- Definir una persona encargada de recibir los reportes de los eventos quien debe estar siempre disponible para ello.
- Informar al personal de los resultados después de haber resuelto el incidente.
- Diligenciar un formato que ayude al personal a recordar cada detalle del evento.
- Todo el personal debe reportar cualquier debilidad que encuentren en el sistema y que afecte la seguridad del mismo.
- El personal no debe tratar de probar las debilidades encontradas, solo debe reportarlas y esperar que el administrador encargado de una solución.
- Definir cambios estratégicos en el sistema para eliminar las debilidades encontradas.

w. Gestión de continuidad del negocio

- Desarrollar e implementar un plan de contingencia. [Ref. Tesis de Fabián]

x. Identificación de la legislación aplicable

- Asegurar el cumplimiento de los Derechos de propiedad intelectual de la aplicación del SPEL y de todo el software utilizado en el mismo. Esto mediante Publicación del uso legal de los productos software e información. Adquisición del software con proveedores conocidos y con sus licencias, marcas registradas y patentes respectivas. Instalación únicamente de software legal. Prohibido copiar, duplicar o convertir a otro formato, audio, video, libros, artículos, documentos, software aparte de aquellos permitidos por la ley.
- Tener en cuenta las leyes sobre delitos informáticos del país que buscan la Protección y Privacidad de la información.
- Divulgar el reglamento interno del Centro de Datos de la Universidad con el fin de que el personal lo conozca y lo aplique.
- Concientizar al personal de la importancia de la seguridad de la información para que velen por ella.
- Los controles criptográficos se deben realizar de acuerdo a la legislación colombiana.
- Dar a conocer al personal los controles y políticas de seguridad y asegurar su cumplimiento.

y. Auditoría

- Se realizará de acuerdo lo que tenga establecido la División de Sistemas.

3.1.6 Desarrollar planes de pruebas para todas las áreas del SPEL.

Se desarrolló un plan de pruebas para cada una de las áreas fundamentales del SPEL.

Para la aplicación del SPEL se tuvo en cuenta a OWASP y a OSSTMM, dentro de las pruebas principales que se le deben realizar se encuentran las siguientes:

Tabla 22. Pruebas para la aplicación del SPEL y el Servidor Web

PRUEBA	ESTANDAR	DESCRIPCION
Pruebas de firma digital de Aplicaciones Web	OWASP OWASP-IG-004	Es importante conocer el tipo exacto de las versiones de los programas del servidor sobre el cual corre la aplicación, ayuda al proceso de análisis, a determinar vulnerabilidades y así fácilmente analizar su respuesta.
Descubrimiento de Aplicaciones	OWASP OWASP-IG-005	Es necesario conocer que aplicaciones se encuentran instaladas en el servidor web junto al SPEL para determinar vulnerabilidades que lo pueden afectar y realizar un análisis completo así no se omiten aplicaciones ocultas.
Pruebas SSL/TLS	OWASP OWASP-CM-001	El SPEL emplea el SSL como un estándar seguro para las comunicaciones cliente servidor ya que además de proporcionar cifrado de la información que transita, también permite la identificación de los servidores mediante certificados digitales, requisito fundamental del SPEL. Es de vital importancia comprobar la configuración del SSL que está en uso para evitar cifrados débiles y para realizar una validación del certificado de seguridad.
Prueba de métodos HTTP y XST	OWASP OWASP-CM-008	Se debe identificar si el certificador web en su configuración permite ataques Cross Site Tracing (XST) y métodos HTTP peligrosos que puedan afectar la aplicación, insertar, cambiar o eliminar archivos, acceder a la información, etc.
Transporte de Credenciales sobre canal cifrado	OWASP OWASP-AT-001	Es importante verificar que la información de acceso al SPEL que ingresan los usuarios, es transmitida utilizando canales cifrados que evite intercepciones.
Buscar credenciales de cuentas válidas por fuerza bruta	OSSTMM	Complementa la prueba anterior con el fin de identificar la facilidad del acceso a las credenciales.
Prueba del Esquema de Gestión de Sesión	OWASP OWASP-SM-001	Se debe verificar la gestión de sesiones con el fin de validar la seguridad de las mismas y sobre todo de las cookies que son vitales para la aplicación web del SPEL, de esta manera evitar el acceso de un atacante a las cookies para robar sesiones de usuarios válidos.
Determinar la Información de Administración de	OSSTMM	Complementa la prueba anterior con el fin de brindar seguridad a la sesión

Sesiones: Número de sesiones concurrentes, Autenticaciones basadas en IP, Autenticación basada en roles, Autenticación basada en Identidad, uso de Cookies, ID de sesión dentro de las secuencias de codificación de la URL, ID de sesión en campos HTML ocultos, etc.		establecida por el usuario para evitar robo de sesiones y accesos privilegiados.
Manipular el estado de las cookies (session/persistent) para tirar o modificar la lógica dentro de las aplicaciones web "server-side".	OSSTMM	Complementa la prueba de seguridad en la gestión de sesiones
Inyección SQL	OWASP OWASP-DV-005	Verificar si la aplicación realiza una validación adecuada de los datos cuando se ingresan consultas SQL directamente en la base datos, si se encuentra una vulnerabilidad es probable que exista un fácil acceso a la base de datos del SPEL
Inyectar comandos SQL en las entradas de cadenas de caracteres de aplicaciones web basadas en bases de datos.	OSSTMM	Esto con el fin de validar si es fácil el acceso a la base de datos del SPEL mediante consultas SQL.
Entrada de usuario como un contador de bucle.	OWASP OWASP-DS-005	Comprobar si es posible que la aplicación realice un bucle de repetición sobre un segmento del código que afecte el rendimiento del servidor y se presente una DoS
Probando WSDL	OWASP OWASP-WS-002	Asegurar que el servidor web no brinde información confidencial. Se verifica el WSDL asociado al servidor y se envían operaciones ocultas tomando como base los mensajes SOAP

Para el área de Red tenemos:

Tabla 23. Pruebas para la red

PRUEBA	ESTANDAR	DESCRIPCION
Usar escaneos SYN TCP (Half-Open) para enumerar puertos abiertos, cerrados o	OSSTMM Sección C	Se debe escanear todos los puertos TCP del sistema para identificar cuales se encuentra abiertos, cerrados o filtrados, una vez identificados los puertos abiertos

filtrados para aquellos puertos TCP utilizados por defecto en el test, en todos los servidores de la red.		se debe identificar que aplicación escucha detrás de ese servicio
Usar escaneos UDP para enumerar puertos abiertos o cerrados para los puertos UDP por defecto si UDP no está siendo filtrado.	OSSTMM Sección C	Se debe escanear todos los puertos UDP del sistema para identificar cuales se encuentra abiertos, cerrados o filtrados.
Relacionar cada puerto abierto con un servicio y protocolo.	OSSTMM Sección C	Se debe identificar qué servicio y qué protocolo se encuentra en cada puerto abierto, esto con el fin de identificar quien escucha detrás de cada puerto y en qué manera puede afectar al SPEL.
Evaluación General de la Seguridad del Switch	ISSAF Sección E.5.1	Con esas pruebas se busca verificar el estado de seguridad de los switch
Evaluación de ataques sobre las VLAN	ISSAF Sección E.5.3	Identificar las configuraciones de las redes virtuales que tiene el sistema.
Evaluación de la seguridad del Router	ISSAF Sección F	Evaluar la seguridad del router con el fin de identificar configuraciones, escaneo de puertos, verificar si se puede realizar ipspoofing, acceso por consola, re direccionamiento ICM, ataque de DoS, entre otros.
Evaluación de la seguridad del Firewall	ISSAF Sección G	Identificación de la configuración por defecto y filtros de usuarios y sitios remotos. Verificar el estado de seguridad del firewall y realizar pruebas de ataques como re direccionamiento de puertos y puertas traseras del firewall.
Evaluación de la seguridad de VPN	ISSAF Sección I	Evaluar la seguridad con el fin de realizar descubrimiento de VPN y su huella digital.

Para seguridad física:

Tabla 24. Pruebas para seguridad física

PRUEBA	ESTANDAR	DESCRIPCION
Checklist de Seguridad	TIA 942 Anexo G	Lista de comprobaciones que nos permite evaluar la infraestructura para identificar qué tipo de respaldo se puede tener en cuanto a la disponibilidad del Centro de Datos.
Revisión de Perímetro	OSSTMM Sección F	Estas pruebas permiten evaluar y actualizar los mapas y documentos relacionados al perímetro físico. Verificar los puntos de acceso a las instalaciones, áreas

		monitoreadas y no monitoreadas, así como revisar el estado y funcionamiento de las alarmas y dispositivos de control de acceso.

En cuanto a Protección de Datos de Usuario tenemos:

Tabla 25. Pruebas para protección de datos de usuario

PRUEBA	ESTANDAR	DESCRIPCION
Evaluación de la seguridad de las bases de datos Oracle	ISSAF Sección Y.2	Esta nos permite identificar hasta qué punto la base de datos está protegida contra ataques por fuerza bruta a la base de datos y ataques de manipulación de los procesos.
Pruebas de Ingeniería Social	OSSTMM Sección B	Se pueden probar los comportamientos de los funcionarios en cuanto a dar acceso de la información confidencial del sistema, esto bajo las normativas de la Institución y del país.

Las actividades 22, 23 y 24 de este lineamiento no se llevaron a cabo dado que el SPEL no se encuentra funcionando por lo tanto este plan de pruebas queda como propuesta para la División de Sistemas.

3.1.7 Realizar auditoría interna.

La auditoría interna debe realizarse una vez el SPEL se encuentre en funcionamiento y se implementen los lineamientos de seguridad planteados. Ésta se realizará de acuerdo a lo establecido por la División de Sistemas.

3.1.8 Implementar acciones preventivas y correctivas.

Cuando el SPEL se encuentre en funcionamiento y una vez realizado el lineamiento 6 y 7 se deben implementar las acciones pertinentes que mejoren la seguridad del sistema y teniendo en cuenta que la gestión de la seguridad debe ser una actividad constante en el tiempo.

CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

Conclusiones

- ✓ Los lineamientos propuestos en este trabajo de grado, son una herramienta que las Universidades pueden tomar en cuenta para implantar un SGSI para el SPEL y de esta manera disminuir los riesgos a los cuales se encuentra expuesto.

- ✓ Los lineamientos propuestos se encuentran enmarcados en la ISO/IEC 27001, único estándar certificable en seguridad de la información, por lo tanto se ha avanzado en el cumplimiento de algunos de los requisitos necesarios para alcanzar la certificación de seguridad de la información.

- ✓ Es necesario conocer y aplicar las metodologías existentes relacionadas con la seguridad de la información ya que estas son aprobadas por un consenso mundial, además de que proporcionan las mejores prácticas o formas con las que se puede garantizar la seguridad, es por ello que se tomaron como base para la propuesta de los lineamientos aplicándolas al contexto del SPEL.

- ✓ Los lineamientos propuestos en este documento son una articulación coherente de estándares y metodologías de gestión de la seguridad de la información, tomando cada uno de los aspectos que contribuyen a la seguridad del SPEL.

- ✓ Con el análisis de riesgos se obtuvo un informe general de la seguridad actual del SPEL y de la División de Sistemas de la Universidad del Cauca frente a las amenazas a las cuales se encuentran expuestos y evidenció la necesidad de la implementación de controles de seguridad que mitigue el riesgo los cuales fueron propuestos en este documento.

- ✓ Los lineamientos generados en este trabajo son aplicables a la gestión de seguridad de cualquier sistema de información, ya que se encuentran basados en estándares y metodologías generales de la SI.

Recomendaciones y trabajos futuros

- ✓ Implementar los lineamientos propuestos una vez el SPEL se encuentre en funcionamiento con el fin de garantizarle al usuario un medio de pago seguro.

- ✓ Crear una cultura de seguridad de la información que involucre principalmente a los usuarios, puesto que esta depende en gran medida de ellos, formar conciencia en el manejo de contraseñas, información confidencial y transacciones con el fin de disminuir fraudes por desconocimiento de las medidas de seguridad que se pueden tener.

- ✓ Mantener un canal disponible con ACH COLOMBIA ya que el SPEL se encuentra regulado directamente por sus disposiciones y además la aplicación ejecuta servicios WEB tanto desde el sitio web de la Universidad como del PSE, se debe recordar que el desarrollo y gestión del sistema es responsabilidad exclusiva de la Universidad.

- ✓ Implementación de la Infraestructura de Llave Pública (pki Public Key Infraestructure) dentro de la Universidad del Cauca para posibilitar la comunicación segura entre servicios, dependencias y facultades.

- ✓ Implementación de la funcionalidad al SPEL que permita hacer registro de las transacciones realizadas durante el día y el estado de las mismas. Esto como soporte del funcionamiento del servicio dentro de los servidores de la Universidad y como medio de comprobación con los reportes emitidos por el PSE en los archivos de conciliación.

- ✓ Es necesario que la Institución Universitaria siga estos lineamientos de seguridad con el fin de proteger la información del SPEL, ya que es un servicio por el cual se transmite información relacionada con dinero, lo cual lo convierte en un sistema llamativo para la realización de fraudes y robos.

- ✓ Implementar en la aplicación del SPEL la funcionalidad de autenticación de usuario y contraseña, esto con el fin de que toda la información relacionada con el pago sea vista exclusivamente por el usuario y así evitar que cualquier persona puede conocer esta información simplemente digitando el código del estudiante.

- ✓ Dar continuidad al sistema de gestión de seguridad propuesto, primero fortaleciendo el SPEL y luego expandiendo su control con otros servicios de una manera incremental hasta cubrir toda la División de Sistemas con un SGSI.

- ✓ Desarrollo de la aplicación del sistema de pago para ambientes móviles.

REFERENCIAS BIBLIOGRÁFICAS

[1] C. E. Serrano, “Modelo Integral para el Profesional en Ingeniería”. Colombia: Editorial Universidad del Cauca, 2005, pp. (12-20), Consultada el 09 de Abril de 2008.

[2] ISO/IEC, “Estándar Internacional ISO/IEC 27001 Tecnología de la Información – Técnicas de Seguridad –Sistemas de Gestión de Seguridad de la Información - Requerimientos”, 1ra. ed., (2005, Octubre 15).

[3] ISO/IEC, “Estándar Internacional ISO/IEC 27002 Tecnología de la Información – Técnicas de Seguridad – Código para la práctica de la gestión de la seguridad de la información”, 2da. ed., (2005, Junio 15).

[4] ITU. “Globlal strategic report – Technical & Procedural Measures”. [En línea]. Consultada el 20 de Octubre del 2009. Disponible en: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_2.html

[5] RAE. Consultada el 22 de Marzo de 2008. [En línea]. Información disponible en: www.rae.es

[6] ISO/IEC, “7498-1:1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model”. 2da. Ed., (1994, Noviembre 15).

[7] C. Borghello. *El arma infalible: la Ingeniería Social.* (2009, Abril). Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.eset-la.com/centro-amenazas/1515-arma-infalible-ingenieria-social

[8] Congreso de Colombia. “Ley 527 de 1999”. (1999, Agosto). [En línea]. Consultada el 20 de Junio del 2009. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

[9] Congreso de Colombia. “Ley 1273 de 2009”. (2009, Enero). Consultada el 20 de Junio del 2009. [En línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[10] Naciones Unidas. “Ley Modelo de la CNUDMI sobre Comercio Electrónico”. (1999, Diciembre). Consultada el 20 de Junio del 2009. [En línea]. Disponible en: http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

[11] Microsoft. I.Lopez. *Pharming, otro nuevo fraude cibernético.* Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.microsoft.com/business/smb/es-es/legal/pharming.mspx

[12] ICONTEC, “Estándar Internacional ISO/IEC 15408”, Segunda Edición 2005.

[13] ISO. “ISO/IEC 13335 – 1:2004. Information technology – Security techniques – Management of information and communications technology security”. Consultada el 24 de Junio de 2008. [En Línea]. Disponible en: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066

[14] Network Work Group. B. Fraser. “RFC 2196. Site Security Handbook”, (1997, Septiembre). Consultada el 20 de Noviembre de 2008. [En Línea]. Disponible en: http://www.ietf.org/rfc/rfc2196.txt

[15] BSI. “BS 7799-1:2005 Information technology. Security techniques. Code of practice for information security management”. (2005, Junio). Consultada el 26 de Junio de 2009. [En línea].Disponible en: http://www.bsigroup.com/en/Shop/Publication-Detail/?pid=000000000030166440

[16] BSI. “BS 7799-2:2005 Information technology. Security techniques. Information security management systems. Requirements”. (2005, Octubre). [En línea]. Consultada el 26 de Junio de 2009. Disponible en: http://www.bsigroup.com/en/Shop/Publication-Detail/?pid=000000000030126472

[17] BSI. “BS 7799-3:2006 Information security management systems. Guidelines for information security risk management”. (2006, Marzo).Consultada el 26 de Junio de 2009. [En línea]. Disponible en: http://www.bsigroup.com/en/Shop/Publication-Detail/?pid=000000000030125022

[18] ISO, “Norma Internacional ISO 9000 Sistemas de gestión de la calidad – Conceptos y vocabulario”, Ginebra: 2000.

[19] TIA, “TIA-942 Standard Telecommunications Infrastructure Standard for Data Centers”, 2005.

[20] ITU, “Annual Report 2008”, Ginebra, Suiza: 2009.

[21] ITU. (2009). “New GCA Brochure”. Consultada el 20 de Junio de 2009. [En línea]. Disponible en: http://www.itu.int/osg/csd/cybersecurity/gca/index.html

[22] Security Standars Council. PCI. DSS. (2009, Julio). Consultada el 26 de Junio de 2009. [En línea].Disponible en: hhttps://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

[23] ISECOM. P.Herzog. “OSSTMM 2.2”, Diciembre 2006. Consultada el 20 de Junio de 2008. [En línea]. Disponible en: http://www.isecom.org/osstmm/

[24] J. Casal, OSSIM Fast Guide. (2004, Febrero). Consultada el 20 de Junio de 2008. [En línea]. Disponible en: www.ossim.net

[25] OWASP Foundation. (2009). “Welcome to OWASP”. Consultada el 26 de Junio de 2009. [En línea]. Disponible en: http://www.owasp.org/index.php/Main_Page

[26] OWASP Foundation. (2007). “OWASP Top Ten”. Consultada el 26 de Junio de 2009. [En línea]. Disponible en: http://www.owasp.org/images/e/e8/OWASP_Top_10_2007.pdf

[27] OWASP Foundation. (2008). “OWASP Testing Guide”. (V3.0). Consultada el 26 de Junio de 2009. [En línea]. Disponible en: https://www.owasp.org/images/8/89/OWASP_Testing_Guide_V3.pdf

[28] OWASP Foundation. “A Guide to Building Secure Web Applications and Web Services”. (2.0 ed.) (2005, Julio 27). [En línea]. Consultada el 26 de Junio de 2009. Disponible en: http://ufpr.dl.sourceforge.net/sourceforge/owasp/OWASPGuide2.0.1.pdf

[29] OISSG. (2006 May. 01). “Inforamtion Systems Security Assessmente Framework (ISSAF)”. (V0.2.1ª-B). Consultada el 26 de Junio de 2009. [En línea]. Disponible en: http://www.oissg.org/downloads/issaf/information-systems-security-assessment-framework-issaf-draft-0.2.1a/download.html

[30] Decreto 1400 (2005). Consultada el 29 de Julio de 2009. [En línea]. Información disponible en: http://www.sic.gov.co/Normatividad/Decretos/Decreto%201400-2005.php

[31] OECD. "The OECD Definitions of the Internet and e-commerce transactions". Consultada el 30 de Julio de 2009. [En línea]. Información disponible en: www.oecd.org/dataoecd/34/16/2771174.pdf

[32] J. Bernal y C. Merlano. (2007, Noviembre). "Infraestructura Para Los Pagos Minoristas Y Automatización De Los Pagos De Gobierno". Consultada el 18 de Marzo de 2008. [En línea]. Disponible en: www.forodepagos.org/pdf/week2007/pw2007-24.pdf

[33] ACH COLOMBIA S.A. Consultada el 15 de Marzo de 2008. [En línea]. Información disponible en: http://www.achcolombia.com.co/portal/page/portal/PortalACHColombia/index.html.

[34] "Decreto 1465" (2005, Mayo). Consultada el 10 de Septiembre de 2009. [En línea]. Información disponible en: www.minproteccionsocial.gov.co

[35] COM (97). "Iniciativa Europea sobre comercio electrónico" (2006, Diciembre). Consultada el 10 de Septiembre de 2009. [En línea]. Información disponible en: http://europa.eu/legislation_summaries/information_society/l32101_es.htm

[36] Gómez Fernández E. "Seguridad y Comercio Electrónico" (2008, Septiembre), Consultada el 10 de Septiembre de 2009. [En línea]. Información disponible en: http://www.scribd.com/doc/15902988/Seguridad-y-Comercio-Electronico

[37] "Internet World Stats". Consultada el 09 de Octubre de 2009. [En línea]. Información disponible en: http://www.internetworldstats.com/

[38] DANE, "Indicadores Básicos de Tecnologías de la Información y la Comunicación TIC" (2009, Marzo). Consultada el 09 de Octubre de 2009. [En línea]. Información disponible en: www.dane.gov.co

[39] Asobancaria. "Semana Económica" (2009, Marzo). Consultada el 10 de Septiembre de 2009. [En línea]. Información disponible en: http://www.asobancaria.com/subCategorias.jsp?id=544&sup=

[40] PSE. Consultada el 15 de Marzo de 2008. [En línea]. Información disponible en: www.pse.com.co.

[41] ACH COLOMBIA S.A. "Manual de Operaciones Instructivo Modulo Administrativo PSE-EMP". Colombia. (2003, Enero). Consultada el 25 de Junio de 2009.

[42] ASP.NET. Consultada el 28 de Junio de 2009. [En línea]. Información disponible en: www.es-asp.net.

[43] NACHA. Consultada el 22 de Marzo de 2008. [En línea]. Información disponible en: www.nacha.org.

[44] OASIS OPEN. "Web Services Security: SOAP Message Security 1.1". (2006, Febrero). Consultada el 10 de Julio de 2009. [En línea]. Disponible en: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[45] OASIS OPEN. Consultada el 10 de Julio de 2009. [En línea]. Información disponible en: www.oasis-open.org.

[46] W3C. “Simple Object Access Protocol (SOAP) 1.1”. (2000, Mayo). Consultada el 10 de Julio de 2009. [En línea]. Disponible en: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[47] J.M. Morales Vásquez, “SSL, Secure Sockets Layer y otros protocolos seguros para el comercio electrónico” (2002). Consultada el 10 de Julio de 2009. [En línea]. Disponible en: http://www.moratalaz.jazztel.es/pdfs/ssl.pdf

[48] Congreso de Colombia. “Ley 115 de 1994; artículos 35 y 213”. (1994, Febrero). Consultada el 20 de Junio del 2009. [En línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=292

[49] Congreso de Colombia. “Ley 30 de 1992; artículos 16, 17, 18, 19, 23, 57 y 85”. (1992, Diciembre). Consultada el 20 de Junio del 2009. [En línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=253

[50] Congreso de Colombia. “Ley 749 de 2002; artículos 1 y 2”. (2002, Julio). Consultada el 20 de Junio del 2009. [En línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6833

[51] MEN-SNIES. “Estadísticas”. Consultada el 10 de Enero de 2010. [En línea]. Disponible en: http://200.41.9.227:7777/men/

[52] Sistema Universitario Estatal (SUE). “Revisión De La Financiación Con Recursos De La Nación Para Las Universidades Públicas”. (2009, Junio). Consultada el 10 de Enero de 2010. [En línea]. Disponible en: www.semana.com/douments/Doc-1967_20091021.doc

[53] Universidad del Valle, OPDI-Área de Análisis. “Estudio Comparativo De Cuatro Universidades Públicas Colombianas”. (2009, Junio). Consultada el 10 de Enero de 2010. [En línea]. Disponible en: www.univalle.edu.co

[54] A. Hervalejo. Universidad Politécnica de Valencia. *Auditorias de Seguridad Informática y la OSSTMM.* (2009, Julio). Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.scribd.com/doc/17740680/Auditorias-de-Seguridad-Informatica-y-la-OSSTMM

[55] ESET. *Robo de Información Personal Online*. (2008, Junio). Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.eset.com.pa/threat-center/articles/robo_informacion_online.pdf

[56] Internet Ya, Soluciones Web. *Segunda Oleada de Phishing en Colombia.* (2007, Octubre). Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.internetyasw.net/newsdt.php?id=64

[57] *Global Phishing Survey: Trends an domain name use in 1H2009.* (2009, Octubre). Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://anti-phishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf

[58] Microsoft. I.Lopez. *Pharming, otro nuevo fraude cibernético.* Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.microsoft.com/business/smb/es-es/legal/pharming.mspx

[59] ClubSymantec. *Glosario*. Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.symantec.com/es/es/norton/clubsymantec/glossary/index.jsp

[60] Recovery Labs. *Fraude en Internet: Del phishing al pharming*. Consultada el 24 de Noviembre de 2009. En línea. Disponible en: http://www.recoverylabs.com/informes/Recovery_Labs_pharming.pdf

[61] Kioskea. *Ataque por denegación de servicio.* (2008, Octubre). Consultada el 29 de Noviembre de 2009. En línea. Disponible en: http://es.kioskea.net/contents/attaques/dos.php3

[62] SeguInfo. *Amenazas Lógicas – Tipos de Ataques – Denial of Service (DoS).* Consultada el 01 de Diciembre de 2009. En línea. Disponible en: http://www.segu-info.com.ar/ataques/ataques_dos.htm

[63] "*Ping de la Muerte".* Consultada el 01 de Diciembre de 2009. [En línea]. Información disponible en: http://www.taringa.net/posts/info/2257717/Conoces-el-ping-de-la-muerte.html

[64] *"TCP SYN".* Consultada el 01 de Diciembre de 2009. [En línea]. Información disponible en: http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a00800f67d5.shtml

[65] E. Abril. *ARP FLOOD – Denegación de Servicio en la Internet.* (2009, Marzo). Consultada el 29 de Noviembre de 2009. En línea. Disponible en: http://hacking-avanzado.blogspot.com/search?q=ARP+Flood

[66] *"ICMP Flood Attack".* Consultada el 01 de Diciembre de 2009. [En línea]. Información disponible en: http://anml.iu.edu/ddos/types.html

[67] F. Limón. Universidad Politécnica de Madrid. *Sistemas Distribuidos de Denegación de Servicio.* Consultada el 01 de Diciembre de 2009. En línea. Disponible en: http://panoramix.fi.upm.es/~flimon/ddos.pdf

[68] V. Velasco. SANS Institute. *Introduction to IP Spoofing.* (2000, Noviembre). Consultada el 01 de Diciembre de 2009. En línea. Disponible en: http://www.sans.org/reading_room/whitepapers/threats/introduction_to_ip_spoofing_959

[69] F. Ali. Cisco. IP Spoofing. Consultada el 01 de Diciembre de 2009. En línea. Disponible en: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html

[70] Cisco. DNS Spoofing. (2006). Consultada el 06 de Diciembre de 2009. En línea. Disponible en: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtdnsspf.pdf

[71] F. Carli. SANS Institute. Security Issues with DNS. (2003). Consultada el 01 de Diciembre de 2009. En línea. Disponible en: http://www.sans.org/reading_room/whitepapers/dns/security_issues_with_dns_1069

[72] E. Felten, D. Balfanz, D Dean, D Wallach. Universidad de Princeton. Web Spoofing una estafa en Internet. Consultada el 01 de Diciembre de 2009. En línea. Disponible en: http://www.govannom.org/seguridad/web_cgi/web_spoofing.html

[73] C. Borghello. Keylogger. Consultada el 015 de Diciembre de 2009. (2006, Julio). En línea. Disponible en: http://www.segu-info.com.ar/articulos/46-keylogger.htm

[74] RAE. Consultada el 28 de Mayo de 2010. [En línea]. Información disponible en: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=componente

[75] RAE. Consultada el 28 de Mayo de 2010. [En línea]. Información disponible en: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=criterio

[76] F. Mera y C. Guevara, "Criterios para establecer políticas de seguridad de la información y plan de contingencia caso de estudio el Centro de Datos de la Universidad del Cauca". Colombia: Editorial Universidad del Cauca, 2008.

[77] Ciclo PDCA. Consultada el 15 de Noviembre de 2009. [En línea]. Información disponible en: www.pdca.es

[78] ACH COLOMBIA S.A. "Cronograma PSE". Colombia. Consultada el 25 de Junio de 2009.

[79] Consejo Superior de Administración Electrónica. Gobierno de España. *"Margerit – v2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información"*. Consultada el 23 de Febrero de 2010. [En línea]. Información disponible en: http://www.csae.map.es/csi/pg5m20.htm

[80] H. Jurado, Universidad del Cauca. Popayán. [Entrevista]. (2008, Marzo 27)

[81] Consejo Superior de Administración Electrónica. Gobierno de España. *"Margerit – v2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II-Catálogo de Elementos"*. Consultada el 23 de Febrero de 2010. [En línea]. Información disponible en: http://www.csae.map.es/csi/pdf/magerit_v2/catalogo_v11_final.pdf

[82] L.C. Pito, Universidad del Cauca. Popayán. [Entrevista]. (2009, Noviembre)

[83] F.A. Mera, Universidad del Cauca. Popayán. [Entrevista]. (2009, Noviembre)