AMBIENTE DE APRENDIZAJE PARA EL ÁREA DE AUDITORÍA, SEGURIDAD Y CONTROL EN INFORMÁTICA BASADO EN COMPETENCIAS

UNIDAD DE APRENDIZAJE: TÉCNICAS DE SEGURIDAD INFORMÁTICA

ALEXANDER SILVA CARDOZO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO – MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2008

AMBIENTE DE APRENDIZAJE PARA EL ÁREA DE AUDITORÍA, SEGURIDAD Y CONTROL EN INFORMÁTICA BASADO EN COMPETENCIAS

UNIDAD DE APRENDIZAJE: TÉCNICAS DE SEGURIDAD INFORMÁTICA

ALEXANDER SILVA CARDOZO

Trabajo de grado para optar por el título de
Ingeniero de Sistemas

Director
LUIS CARLOS GÓMEZ FLOREZ
Ingeniero de Sistemas y Magíster en Informática

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍA FÍSICO – MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2008

AGRADECIMIENTOS

No sólo son agradecimientos sino sentimientos de participación para con todas y cada una de las personas que intervinieron en el desarrollo del producto final que conllevó mucho esfuerzo y sacrificios tangibles e intangibles.

Se destacan, mi tutor espiritual que le debo las energías físicas y mentales que cada día tuve para la realización del mismo, mi esposa que desde nuestros inicios no me ha abandonado en ninguna circunstancia.

Mis padres que plasmaron con sus manos un hombre honesto, realista y capaz de desarrollar su propia vida, mi hermano que con su paciencia y sosiego logra entender lo que yo no.

Al escueto y sincero conocimiento que inyectó mi director de proyecto Luis Carlos Gómez Florez en mis músculos sensoriales y cognitivos abriendo un camino claro y prudente para el logro de los objetivos propuestos.

Por último al campus universitario que durante mis años de estadía en él soporto mis pisadas y me enseñó parte de lo que hoy aplico.

EN HOMENAJE:

A Dios por iluminarme y entenderme,

A mi esposa por enseñarme a ser mejor persona,

A mi familia por su calor.

CONTENIDO

CAPÍTULO III

CAPÍTULO IV

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

TÍTULO:

AMBIENTE DE APRENDIZAJE PARA EL ÁREA DE AUDITORÍA, SEGURIDAD Y CONTROL EN INFORMÁTICA BASADO EN COMPETENCIAS*

AUTOR: Alexander Silva Cardozo**

PALABRAS CLAVES:

Objetos de Aprendizaje, Unidad de Aprendizaje, Competencias Cognitivas, Sistema de Gestión de Aprendizaje, Tecnologías de la Información y la Comunicación, SCORM, Ficha Temática, Aprendizaje Activo.

DESCRIPCIÓN:

El proceso que actualmente está transformando la educación en la UIS ha permitido al grupo de Investigación STI generar el espacio y uso de las TICs de la universidad, además, aplicar las metodologías de aprendizaje en línea que ha manejado desde sus inicios.

El Sistema de Gestión de Aprendizaje Moodle es ampliamente dominado por el profesor de área y a partir de ahí es que se genera una oportunidad para dar más profundidad a los contenidos presentados y administrados, permitiendo así, dar al estudiante una concepción que lo haga responsable frente al papel que juega con su aprendizaje en línea.

Dado lo anterior y con la nueva modalidad de Práctica en Docencia, se logra hacer un seguimiento detallado de las actividades de los estudiantes de la asignatura, para analizar, diseñar, implementar y poner en marcha objetos de aprendizaje que cautiven su atención, éstos cimentados en el aprendizaje activo y las competencias cognitivas.

El conocimiento del área por parte del profesor y el acompañamiento del autor de proyecto durante el desarrollo de sus actividades pedagógicas durante un período académico, dan como resultado un fortalecimiento de la estructura curricular para alcanzar un conocimiento más duradero en los estudiantes que permita reconocer realmente el alcance del proyecto dentro del aula de clase.

_____

* Trabajo de grado en la Modalidad de Práctica en Docencia.

** Facultad de Ingenierías Físico – Mecánicas. Escuela de Ingeniería de Sistemas e Informática. Director: MI. Luis Carlos Gomez Florez.

SUMMARY

TITLE:

SET OF LEARNING FOR THE AUDIT AREA, SECURITY AND CONTROL IN COMPUTER SCIENCE BASED IN COMPETENCES*

AUTHOR: Alexander Silva Cardozo**

KEY WORDS:

Learning Objects, Learning Unit, Cognitive Competences, Learning Management System, Technologies of the Information and the Communication, SCORM, Thematic card, Active Learning.

DESCRIPTION:

The process that at the moment is transforming the education in the UIS it has allowed to the group of Investigation STI to generate the space and use of the TICs of the university, also, to apply the methodologies of on-line learning that it has managed from their beginnings.

The Learning Management System Moodle is broadly dominated by the area professor and starting from there it is that an opportunity is generated to give more depth to the presented contents and administered, allowing this way, to give the student a conception that makes it responsible in front of the paper that plays with its learning in it lines.

Given the above-mentioned and with the new modality of Practice in Teaching, it is possible to make a detailed pursuit of the activities of the students of the subject, to analyze, to design, to implement and to start learning objects that capture their attention, these laid the foundation in the active learning and the cognitive competences.

The knowledge of the area for part of the professor and the project author's accompaniment during the development of their pedagogic activities during an academic period, they give an invigoration of the curricular structure as a result to reach a more durable knowledge in the students that it really allows to recognize the reach of the project inside the class classroom.

---

* Degree Project in the Education Practice Modality

** Faculty of Physical – Mechanicals Engineering. School of Systems Engineering and Computer Science. Director: M.CS. Luis Carlos Gómez Florez.

GLOSARIO

ADL (del inglés *Advanced Distributed Learning,* aprendizaje distribuido avanzado). Conjunto de normas diseñadas para facilitar la labor de compartir Objetos de Aprendizaje a través de diversos Sistemas de Gestión de Aprendizaje.

AMBIENTE DE APRENDIZAJE: Escenario donde existen y se desarrollan condiciones favorables de aprendizaje. Un espacio y un tiempo en donde los participantes desarrollan capacidades, competencias, habilidades y valores

APRENDIZAJE ACTIVO: Aprendizaje enmarcado dentro del constructivismo que parte del hecho de que cada persona aprende de forma distinta. Los estudiantes son el eje y los protagonistas del proceso y son quienes deciden cuándo y cómo aprender, mientras el profesor es un orientador.

ASINCRÓNICA: Se refiere a una interacción desfasada, que no es en tiempo real, para muchos casos podría ser es mas efectivo que las herramientas sincrónica. Un ejemplo es el e-mail.

AUDITORIA INFORMÁTICA: Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de las TI de una empresa con vistas a mejorar su rentabilidad y seguridad.

AUTORIDAD CERTIFICANTE: (del inglés Certification Authority) Entidad de confianza encargada de emitir, registrar y publicar certificados. Además verifica la identidad del solicitante del certificado y publica las listas de revocación de certificados.

CASO DE ESTUDIO: Método particular de investigación cualitativa. Se usa para examinar un número limitado de variables. Envuelven una profundización y examen longitudinal de una sencilla instancia o evento.

CERTIFICADO DIGITAL: Registros electrónicos que atestiguan fehacientemente que determinada clave pública pertenece a una persona o entidad.

COMPETENCIA: Conjunto de características propias del ser humano que se ponen en juego en un contexto específico y particular, evidenciada a través de acciones concretas que se consideran indicadores de la misma.

COMPETENCIA COGNITIVA: Clasificación de las competencias Interpretativas, Argumentativas y Propositivas sobre las cuales se fundamenta el modelo de evaluación del ICFES.

CONSTRUCTIVISMO: El estudiante construye conocimiento; el aprendizaje es una interpretación personal de la experiencia; el aprendizaje es activo, cooperativo, y situado en un contexto real; y la evaluación del aprendizaje está integrada dentro del contexto del aprendizaje mismo.

CONTROL EN INFORMÁTICA: Es la función del control dual en los diferentes departamentos, que puede ser normativo, marco jurídico, o funciones del control interno..

FIRMA DIGITAL: (del inglés Digital Signature) Valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido con la clave del iniciador y que el mensaje l no ha sido modificado después de efectuada la transformación.

HACKING: El hacking o jaqueo se basa en el arte informático de construir y solucionar problemas que atenten contra la vulnerabilidad de un sistema o aplicación, compartiendo este mismo método con otros hackers.

HIPERMEDIA: Método de almacenaje y recuperación de información que proporciona múltiples enlaces entre sus elementos. Permite al estudiante navegar con facilidad de un documento a otro, almacenar y recuperar textos.

INFRAESTRUCTURA DE CLAVE PÚBLICA: (del inglés Public Key Infraestructure): es una arquitectura de seguridad que ha sido desarrollada para proveer de un nivel mayor de confidencialidad al intercambiar información en Internet.

MOODLE: Moodle es un Sistema de Gestión de Aprendizaje de libre distribución (*Learning Management System* LMS) que ayuda a los educadores a crear comunidades de aprendizaje en línea.

OBJETO DE APRENDIZAJE: Representación electrónica de archivos multimedia, textos, imágenes, u otros datos, o la combinación de esos fragmentos de datos en una unidad de formación.

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

SCORM: (del inglés *Sharable Content Object Reference Model,* Modelo de Referencia de Objetos de Contenido Compartibles): Conjunto de estándares

que definen el modelo de combinación de contenidos de aprendizaje basado en Web y el entorno de tiempo de ejecución de los objetos de aprendizaje.

SEGURIDAD INFORMÁTICA: Reglas, planes y acciones aplicadas para asegurar las Tecnologías de Información de una organización y la información que se considera importante no sea fácil de acceder por cualquier persona que no se encuentre acreditada.

S.D.I: (del inglés Intrusión Detection System), Herramienta de seguridad que intenta *detectar o monitorear los eventos* ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema

SINCRÓNICA: Se refiere al tipo de comunicación en que la interacción entre emisor y receptor es simultánea (por ejemplo, la conversación telefónica o videoconferencia).

SISTEMAS DE GESTIÓN DE APRENDIZAJE: (del inglés Learning Management System), herramienta informática y telemática organizada en función de unos objetivos formativos de forma integral [es decir que se puedan conseguir exclusivamente dentro de ella] y de unos principios de intervención psicopedagógica y organizativos.

TICs: Se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de hardware y software como medio de sistema informático.

UNIDAD DE APRENDIZAJE: Referente técnico pedagógico que permite la organización del trabajo del profesor para la orientación del proceso de aprendizaje.

INTRODUCCIÓN

Las grandes transformaciones de la educación en los últimos años, suponen el establecimiento de nuevas modalidades y estrategias de formación que le confieren a la pedagogía un claro sentido de formación que rebasa los escenarios universitarios, dirigiendo su atención a problemas asociados con los conflictos socio-educativos y el desarrollo humano de los estudiantes y las comunidades, en escenarios que no son necesariamente formativos.

Como lo indica (DUARTE, 2003: 1) "La emergencia histórica de "nuevos" escenarios para la pedagogía... (Giroux, 1997)[1]" se viene dando de tiempo atrás, y es necesario hacer una análisis formal de la formación unidireccional dado sus aportes y resultados a largo plazo.

Las tecnologías digitales e Internet hacen posible pensar en alternativas de formación que fortalezcan los criterios educativos generales que orientan las decisiones y concepciones en los campos social, político, económico, cultural etcétera, que sobre el programa académico el profesor identifica.

Además el aprendizaje requiere que el estudiante sea un participante activo como acota (Castrillón, 2006:36) "…el aprendizaje es un proceso activo y de construcción que lleva a cabo, en su interior, el sujeto que aprende (Barbosa, 2004)[2]".

En un área que disponga de Objetos de Aprendizaje[3] se generan interrogantes sobre los roles que juega el profesor y el estudiante, sobre su relación con el contenido, sobre cómo se entiende ese contenido y cómo debe quedar representado en esta.

El presente proyecto pretende enriquecer la Unidad de Aprendizaje ***"Técnicas de Seguridad"***[4] de la asignatura Seguridad Informática mediante una implementación de OA basados en SCORM[5] (del inglés: *Sharable Content Object Reference Model*), complementados sobre los lineamientos de competencias cognitivas (ACOFI, 2005) y el aprendizaje activo (Ruiz, 2006).

[1] Documento original de la cita.
[2] Documento original de la cita.
[3] De ahora en adelante OA.
[4] De ahora en adelante UA.
[5] Es el Modelo de Referencia de Objetos de Contenido Compartibles.

CAPÍTULO I

1. DESCRIPCIÓN DEL PROYECTO

El grupo de Investigación en Sistemas y Tecnología de la Información[6] de forma descentralizada ha fijado su desarrollo y eventual evolución, en las Tecnologías de la Información y la Comunicación[7] que la Universidad ofrece y es en estos momentos en los cuales se encuentra a disposición el CENTIC[8] (Peña, 2006), se hace necesario dar pie a proyectos que promuevan la cultura del aprendizaje activo en el estudiante y el desarrollo pedagógico en los docentes que utilizan el aprendizaje en línea para desarrollar sus asignaturas.

Actualmente el Sistema de Gestión de Aprendizaje Moodle[9] permite administrar cursos a cargo del profesor Luis Carlos Gómez Florez[10] dentro de los cuales se encuentra el de Auditoria, Seguridad y Control en Informática[11].

Siendo tutor en el primer semestre de 2007 de esta área, se plantearon ideas, para diseñar estrategias de aprendizaje que permitieran dar mayor aceptación a un área recién explorada en la universidad.

Según se pudo analizar en diferentes instituciones universitarias[12], éstas poseen grupos de investigación y/o programas de Posgrado al respecto. En buena hora este proyecto de Práctica en Docencia permitirá incentivar a los estudiantes a promover la cultura de la Seguridad Informática que tantos perjuicios acarrea a la universidad, el país y el mundo.

El Ambiente de Aprendizaje para Auditoria, Seguridad y Control en Informática[13], mediará su aprendizaje diseñando OA, con la orientación pedagógica del profesor, utilizando las metodologías de Resolución de casos de estudio, Juegos de roles, Simulación y Cuestionarios tipo ECAES, bajo los lineamientos del aprendizaje activo y las competencias cognitivas.

1.1. ANTECEDENTES

[6] Grupo STI.
[7] De ahora en delante TICs.
[8] Centro de Tecnologías de la Información y la Comunicación de la UIS.
[9] De ahora en adelante SGA.
[10] De ahora en adelante LCGF.
[11] De ahora en adelante AS y CI.
[12] EAFIT con Virtual PC, UPB con Especialización en Seguridad Informática, ICESI con un diplomado en Seguridad Informática, Javeriana con SIDRe-Sistemas Distribuidos y Redes.
[13] De ahora en adelante A^2 – AS y CI.

1.1.1. Tecnologías de la Información[14] como soporte al aprendizaje en la UIS

De un tiempo para acá y actualmente se están planteando una serie de propuestas por parte de los estudiantes de las diferentes carreras de la universidad a través de los proyectos de grado, para sacar provecho de las TICs que ofrece, desarrollando OA para ambientes de aprendizaje en línea.

1.1.1.1. El CENTIC

Como ente participativo del Proyecto Institucional para el Soporte al Proceso Educativo mediante Tecnologías de Información y Comunicación[15] que declara: "...se definió una ***política*** y se diseñaron ***estrategias*** tendientes a asegurar condiciones que permitan, mediante sistemas de aprendizaje en línea, ofrecer experiencias de aprendizaje con elevados estándares de calidad" (PEÑA, 2006), el A^2 – AS y CI tiende a aprovechar estas TICs para desarrollar el proyecto y la metodología de aprendizaje.

1.1.1.2. Escuela de Ingeniería de Sistemas e Informática[16]

La EISI se ha articulado al ProSPETIC gracias a una serie de proyectos de pregrado en los cuales se proponen el diseño instruccional de las asignaturas correspondientes a Ingeniería de Sistemas y la creación de OA que finalmente se relacionarán en un repositorio para su posterior utilización, las demás carreras también hacen parte del proceso, pues éste plantea metodologías estandarizadas en el aprendizaje en línea y en el desarrollo de los programas académicos de la universidad.

1.1.1.3. El Grupo STI

El grupo sigue la línea del aprendizaje en línea a través de la plataforma Moodle[17], pues ésta ha soportado y adaptado a las necesidades que el profesor ha considerado para el correcto desarrollo de sus asignaturas. Ahora, viendo la transformación de las metodologías pedagógicas que está planteando la UIS, también se está haciendo un análisis que permita desarrollar el aprendizaje en línea y sus metodologías.

No obstante, viendo que el proceso es largo y requiere de una serie de fases que permitan que el proceso sea acogido por los estudiantes de forma sustancial, se hace necesario no solamente hacer parte del mismo desde

[14] De ahora en adelante TI.
[15] De ahora en adelante ProSPETIC.
[16] De ahora en adelante EISI.
[17] Para mayor referencia diríjase a [0] en bibliografía.

adentro sino desde afuera. Y, ¿Cómo se logra? Pues desarrollando lo que actualmente se está planteando en el ProSPETIC y con OA mediados bajo las TICs, basado en competencias y con una metodología de aprendizaje fundamentada en el estudiante, todo sustentado en el SGA Moodle.

1.1.2. Reseña del Grupo STI[18]

Como estudiante de pregrado e integrante del grupo STI, cabe destacar cómo el grupo STI ha logrado a través de su trayectoria, formar y conformar un grupo interdisciplinario conocedor del tema de Tecnologías y Sistemas de Información gracias a sus diferentes investigaciones, publicaciones y otros. A continuación se presenta a grosso modo, su grupo humano:

GRUPO STI	
EQUIPO HUMANO	VÍNCULOS
PROFESORES UIS	
Luis Carlos Gómez Florez, Dir. / Hugo Hernando Andrade Sosa Luis Eduardo Becerra Ardila / Fernando Antonio Rojas Morales	
EGRESADOS MAESTRÍA	
Carlos Alberto Cobos Lozada, Unicauca….	
ESTUDIANTES MAESTRÍA	
María Fernanda Reyes Sarmiento, UIS…	
EGRESADOS PREGRADO	
Cristina Isabel Acuña Taborda, UIS	
ESTUDIANTES PREGRADO	
Rafael Torres, UIS, ***Alexander Silva, UIS,*** Yadir Molina, UIS…	

- Association for Information Systems AIS – Mundial
- Association for Computing Machinery ACM – Mundial
- Information Systems Audit and Control Association ISACA - Mundial
- RIBIE

Tabla 1. Equipo humano del grupo STI

1.1.2.1. Investigaciones

- Ponencias en Anales/Memorias de Eventos Internacionales, Nacionales
- Software
- Computadores Para Educar – CPE

1.1.2.2. Publicaciones

- Revista UIS Ingenierías, Nacionales
- Libros, Conferencias de clase

1.1.2.3. Plataforma Web del Grupo STI

Desde un principio el profesor LCGF se ha dedicado a dar a conocer el manejo de las TICs en el aprendizaje en línea y es de ahí que surge la necesidad de adoptarlo, el profesor reconoce las falencias presentes y

[18] Para mayor referencia diríjase a [1] en bibliografía.

suscita al grupo a sacar provecho de sus conocimientos para promover su uso y construir su base de conocimientos.

A partir de ahí el grupo STI se dio a la tarea de entender su funcionamiento y si la viabilidad de este tipo de proyectos radicaba en la realización de un entorno de aprendizaje en línea o la aplicabilidad de un SGA ya hecho y soportado por los estándares internacionales. Los resultados arrojaron como mejor alternativa el empalmar el desarrollo de los cursos ofrecidos por el profesor en el SGA Moodle, el cual se adaptaba a sus necesidades.

1.1.3. Auditoria, Seguridad y Control en Informática

En el pensum de Ingeniería de Sistemas de la UIS el área esta catalogada como electiva técnica profesional con nomenclatura "*Seguridad Informática"* y pretende dar al estudiante un enfoque en relación a riesgos y controles que se pueden implementar al encontrar falencias en las T.I. de una organización.

Actualmente el profesor LCGF la cataloga como Auditoria, Seguridad y Control en Informática por las áreas que comprende. Se presenta a continuación un cuadro con una referencia según la importancia dada al tema de AS y CI en el panorama global.

ENTIDAD	DESCRIPCIÓN	APLICACIONES EN TI
ISACA[19]-MODELO COBIT[20]	Las TI cada vez tienen mayor importancia dentro de las organizaciones, debido al impacto competitivo que generan. Es por esto que la seguridad, auditoria y control de estas tecnologías se convierten en un paso importante a la hora de implementarlas.	Los procesos de TI son el medio que pone en funcionamiento los recursos de TI, son los que deben ser adecuadamente definidos, implementados y monitoreados.

Tabla 2. Descripción AS y CI según ISACA

1.1.3.1. Marco Internacional

AUDITORIA[21]

"… abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes".

SEGURIDAD Y CONTROL EN INFORMÁTICA

[19] Information Systems Audit and Control Association –Asociación de Auditoria y Control de Sistemas de Información.
[20] Para mayor referencia diríjase a [2] en bibliografía.
[21] Según ISACA: Refiérase a [3] en bibliografía.

El control en informática[22] registra que todas las actividades se realicen según los estándares, procedimientos, normas fijadas por la directiva organizacional, así como el marco legal. Tiene como objetivos *los controles preventivos, detectivos y correctivos.*

Áreas que cubre la seguridad informática:

* Políticas de Seguridad
* Seguridad Física
* Autentificación
* Integridad
* Confidencialidad
* Control de Acceso
* Auditoria

CURSOS DE AS y CI PROPUESTOS EN EL MARCO INTERNACIONAL			
ENTIDAD	**OBJETIVOS**	**ÁREAS TEMÁTICAS**	**RELACIÓN**
ASI[23] AUDITORES (MÉXICO)	• Identificar los mecanismos de seguridad, integridad en el manejo de la información • Riesgos de la información • Comunicación humana	• Riesgos de la información • Control y seguridad en la informática • Resistencia al cambio • Formación de equipos de trabajo	***CONTROL Y SEGURIDAD EN INFORMÁTICA***
	• Automatización de la auditoria • Elementos auditoria y informática • Auditoria asistida por computador	• Auditoria e informática • Auditoria asistida por computador • Paquete de auditoria	***LA INFORMÁTICA APLICADA A LA AUDITORIA***
	• Era digital y comunicaciones • Transformaciones digitales • Servicios electrónicos • Seguridad, integridad, información.	• Evolución TI y telecomunicaciones • Impacto y resistencia al cambio • Riesgos de la información • Oportunidades de Internet	***CONTROL Y SEGURIDAD EN INTERNET***
CUBA[24]	• Control interno de la entidad • Políticas, normas y procedimientos • Seguridad razonable de los recursos	+ Dirección y administración TI + Políticas y planes informáticos. + Controles de acceso + Controles seguridad y continuidad	***AUDITORIA INFORMÁTICA***
CHILE[25]	• Concepto Auditoria Informática • Metodologías para auditar	• Conceptos y terminología • Planeación y auditoria • Evaluación sistemas y proceso • Evaluación seguridad e información	***AUDITORIA Y SEGURIDAD DE SISTEMAS***

Tabla 3. Cursos de AS y CI internacionales

[22] [3], op. cit. p. 5.
[23] Para mayor referencia diríjase a [4] en bibliografía.
[24] Para mayor referencia diríjase a [5] en bibliografía.
[25] Para mayor referencia diríjase a [6] en bibliografía.

1.1.3.2. Marco Nacional

CURSOS DE AS y CI PROPUESTOS EN EL MARCO NACIONAL			
ENTIDAD	**OBJETIVOS**	**ÁREAS TEMÁTICAS**	**RELACIÓN**
ICESI	• Metodologías y estándares de administración riesgo informático, mejores prácticas internacionales, casos prácticos, auditoria, seguridad y control.	I. GOBIERNO DE TI Y BSC. II. CONTROL INFORMÁTICO - 1 y 3 dominio del Modelo COBIT. III. MEJORES PRÁCTICAS.	***DIPLOMADO EN ADMÓN. DE RIESGO TECNOLÓGICO***[26]
EAFIT	• Herramientas auditoria informática. • Identificar y evaluar riesgos • Planeación estratégica de informática.	• Control, Dirección, Comunicación • Auditoria de Gestión Informática • Seguridad en Bases de datos • Seguridad de la información	***ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS***[27]
UNIANDES	• Perfiles profesionales Seguridad. • Tendencias internacionales en Seguridad de la Información.	• Host, Network security • Modelos y estándares • Ingeniería criptográfica • Administración gerencial	***ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN***[28]
UNIPILOTO	• Conceptos de auditoria de sistemas y riesgos asociados a los negocios	I. AUDITORIA DE SISTEMAS II. SEGURIDAD INFORMÁTICA III. CONTINGENCIA Y CONTINUIDAD IV. AUDITORIA DE E -BUSINESS	***DIPLOMADO EN AUDITORIA DE SISTEMAS***[29]
PONTIFICIA BOLIVARIANA	• Cultura de Seguridad Informática. • Políticas de seguridad	Módulo I. Redes y conectividad Módulo II. Principios de seguridad Módulo IV. Criptografía Módulo V. S.D.I, BMC Módulo VI. Computación Forense	***DIPLOMADO EN SEGURIDAD INFORMÁTICA***[30]

Tabla 4. Cursos de AS y CI nacionales

[26] Para mayor referencia diríjase a [7] en bibliografía.
[27] Para mayor referencia diríjase a [8] en bibliografía.
[28] Para mayor referencia diríjase a [9] en bibliografía.
[29] Para mayor referencia diríjase a [9] en bibliografía.
[30] Para mayor referencia diríjase a [10] en bibliografía.

1.1.3.3. Marco Institucional

CURSO DE AS y CI PROPUESTO EN LA UIS			
ENTIDAD	**OBJETIVOS**	**ÁREAS TEMÁTICAS**	**RELACIÓN**
GRUPO STI	• Explorar contenidos actuales en el área de AS y CI • Introducir al estudiante en el campo de riesgos y controles de las TI • Permitir al estudiante reconocer el marco legal del derecho informático aplicable dentro de una organización • Entender los antecedentes, conceptos e importancia de la Continuidad del Negocio. • Analizar las Normas Técnicas Colombianas de Seguridad Informática. • Estar a la vanguardia en las Técnicas de Seguridad Informática utilizadas.	• Riesgos y controles en TI • Marco legal derecho informático • Continuidad de negocios (BCM) • Normas Técnicas Colombianas en Seguridad Informática -NTC- • Técnicas de Seguridad Informática	**Auditoria de Sistemas**

Tabla 5. Curso de AS y CI propuesto en la UIS

1.1.4. UA

La Unidad de Aprendizaje sobre la cual se diseñan y aplican los OA es la de Técnicas de Seguridad Informática, perteneciente al área de AS y CI dictada por el profesor LCGF desde el año 2006 con una intensidad horaria de cuatro horas semanales en el CENTIC con amplio espacio físico, 32 equipos de cómputo, 1 equipo para el profesor, tablero de acrílico y aire acondicionado. *Ver Figuras a continuación*. Durante el II semestre de 2007 esta electiva no fue adoptada por la EISI debido a que no es evaluable en el ECAES.

Figura 1. Topología del salón del CENTIC

1.1.4.1. Áreas Temáticas

Comprende las áreas de Esteganografía en imágenes, Informática Forense, Biometría, ***Hacking***, Criptografía, ***Sistemas de Detección de Intrusos***, Seguridad en Redes, ***Firma y certificación Digital***, Seguridad en Servicios Web, ***Phishing.*** Estos temas son tratados desde el punto de vista de prevención, riesgos y controles para enfocar al estudiante en las soluciones pro activas que se llevan a cabo dentro de una organización.

1.1.5. Formulación Del Problema

1.1.5.1. Caracterización

En su actual proceso de transformación, la materia no cuenta con una infraestructura curricular que permita al profesor disponer de los temas de forma ordenada y clara. Es necesario analizar la UA para conocer que temas son los que realmente deben pertenecer a esta.

Es preciso complementar el proceso actual con el que se está impartiendo la asignatura de Seguridad Informática para proporcionar los elementos necesarios en el proceso de enseñanza – aprendizaje que sean acordes al enfoque teórico – práctico que esta exige.

Es aquí donde el presente proyecto aboca una oportunidad para enriquecerla mediante la implementación de la UA Técnicas de Seguridad para posibilitar la generación de aprendizaje activo que lleve al estudiante a participar más y aprender de una manera auto estructurante partiendo de sus competencias cognitivas.

1.1.5.2. Visión de la UIS

La UIS programa incorporar sus TICs a través del proyecto ProSPETIC, y es necesario que los profesores y estudiantes aprovechen éstas desarrollando sus áreas de conocimiento a través del aprendizaje en línea, es por esto que es importante como describe ProSPETIC: "…implica la transformación permanente de la estructura organizacional y académica de las mismas…" (Peña, 2005), ya que así se logra conocer las características inherentes de las áreas y lineamientos a seguir, para lograr su aprovechamiento.

1.1.5.3. Visión del Grupo STI

Descentralizar las metodologías de educación en línea pero centralizadas en el CENTIC, es el propósito fundamental del grupo STI puesto que así se logran abrir caminos de investigación hacia nuevas metodologías, TI, pedagogías e instrucciones que propendan a un eficiente desarrollo del aprendizaje en línea.

Este proyecto aboca a lo anterior haciendo uso de los lineamientos del aprendizaje activo, las competencias cognitivas y la modalidad de Práctica en Docencia para aplicarlos en el desarrollo de los OA para entender sus capacidades y posibles repercusiones en el aprendizaje del estudiante.

La omisión de la asignatura para el II semestre de 2007 no es impedimento para el desarrollo del presente proyecto pues los OA quedarán en un repositorio para su eventual aplicación y el análisis funcional - pedagógico se realizó durante le I semestre de 2007.

1.1.6. Propuesta de solución

El aporte que el autor pretende dar con el desarrollo de OA basados en competencias cognitivas y aprendizaje activo, es entender a través del acompañamiento a los estudiantes durante el desarrollo de contenidos, las necesidades básicas, intereses, y aptitudes individuales y grupales que muestran durante el desarrollo de una actividad y de la UA como tal.

A partir de ahí se hace necesario enfocar al estudiante dentro de un contexto que le de la oportunidad de generar conocimiento, entender un tema y participar de forma activa en su desarrollo, porque se evidencia la falta de interés en el estudiante en actividades en las cuales su interacción con la misma no le permita apropiarse del tema ni hacerse partícipe de él.

El área maneja temas que se van transformando y actualizando. De ahí surgió la necesidad de elegir unos temas principales que según los resultados vistos durante el desarrollo del contenido de la UA fueron los que mayor aceptación tuvieron por parte de los estudiantes y mayor dinamismo crearon al interior del grupo llamados **TEMAS A DESARROLLAR**[31]. A continuación se presentan imágenes enriquecidas de cada uno en su orden, Firma y Certificado Digital, Hacking, Phishing, S.D.I.

[31] **Firma y Certificado digital**: Firma de documentos electrónicos**. Hacking:** Intrusión. **Phishing**: Robo de identidad o datos. **Sistemas de detección de intrusos**: Software de control de intrusos. Para mayor referencia diríjase al numeral 2.1.9.

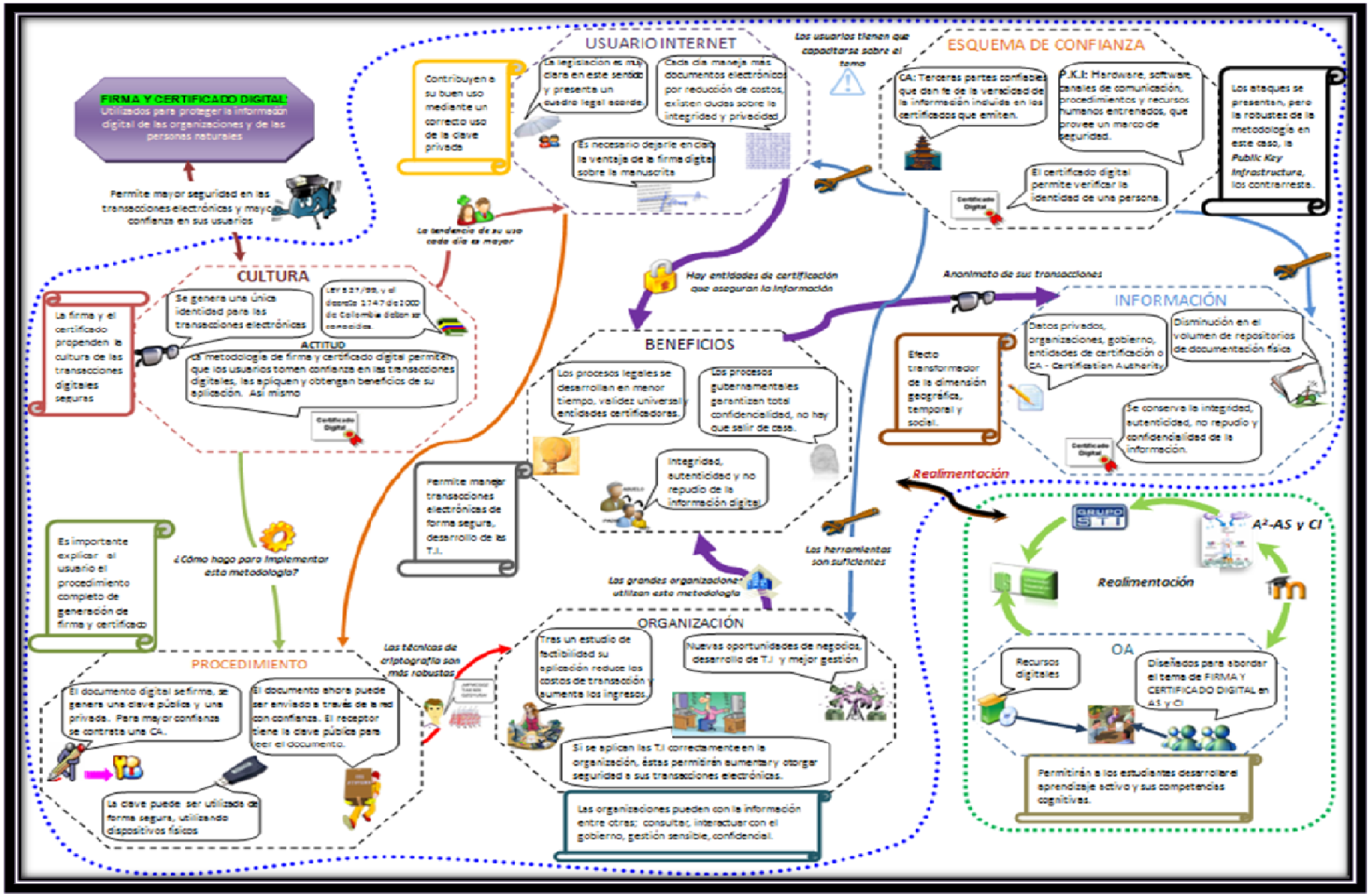


Figura 2. Imagen enriquecida Firma y Certificado Digital

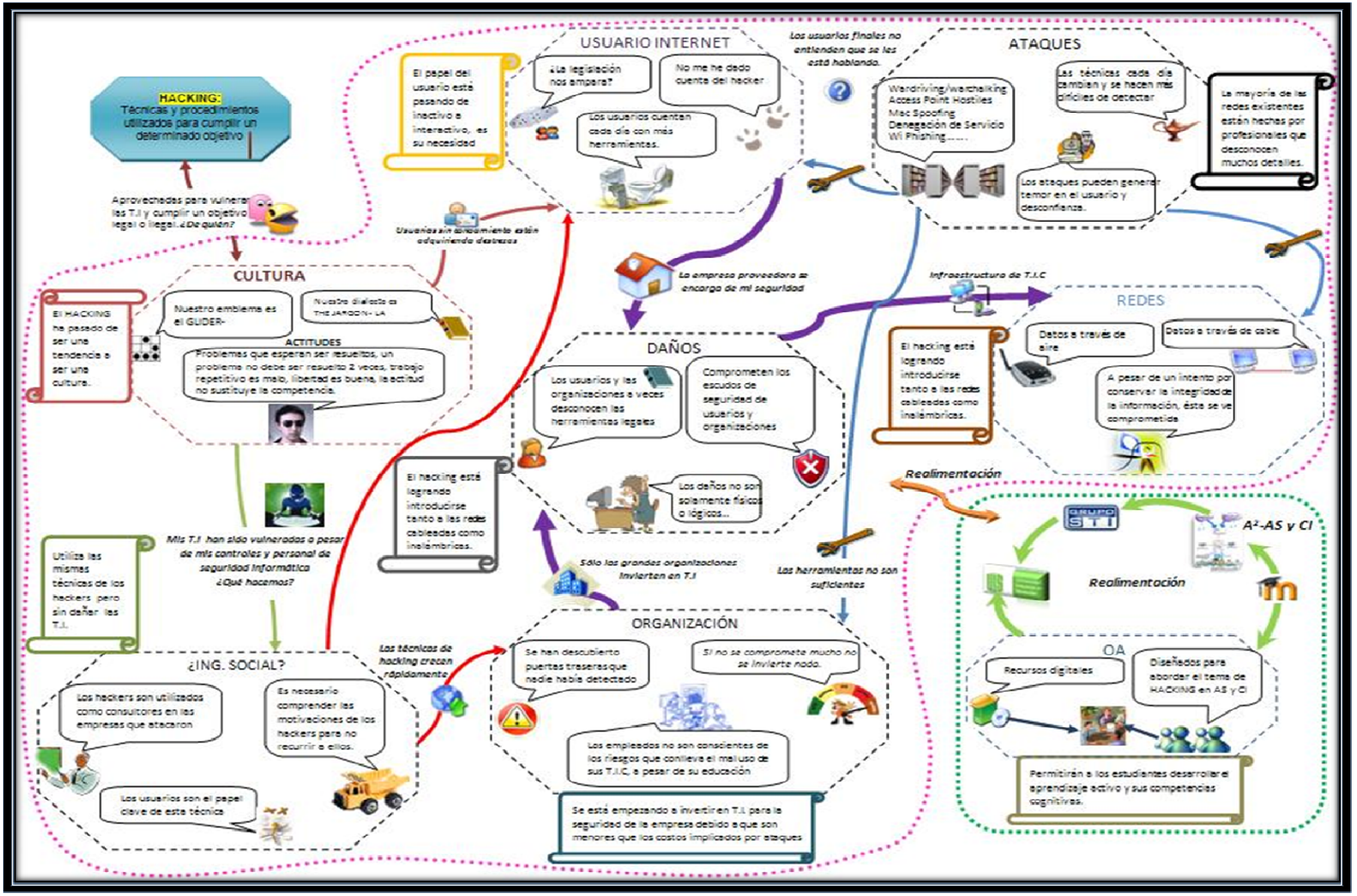


Figura 3. Imagen enriquecida Hacking

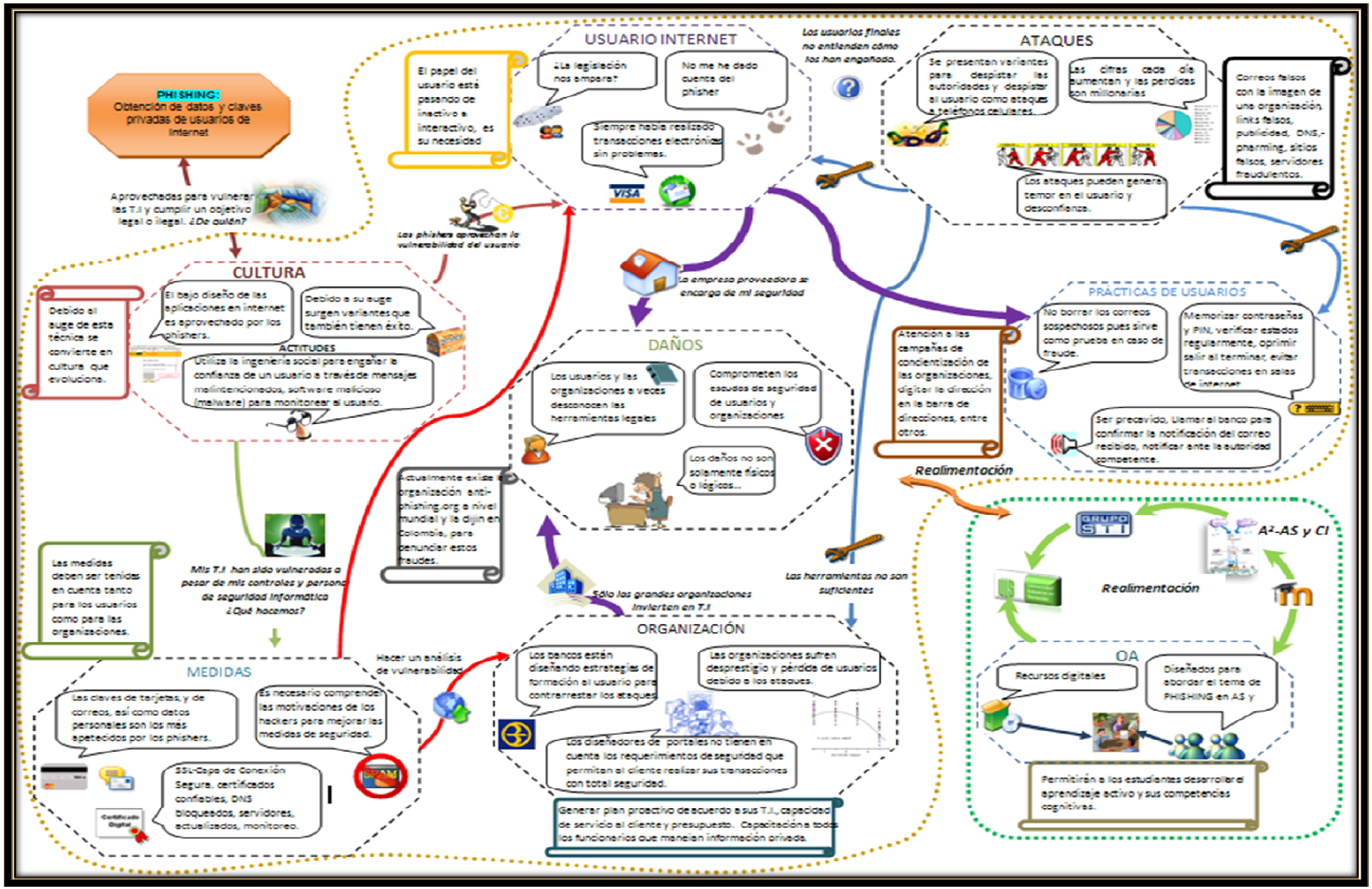


Figura 4. Imagen enriquecida Phishing

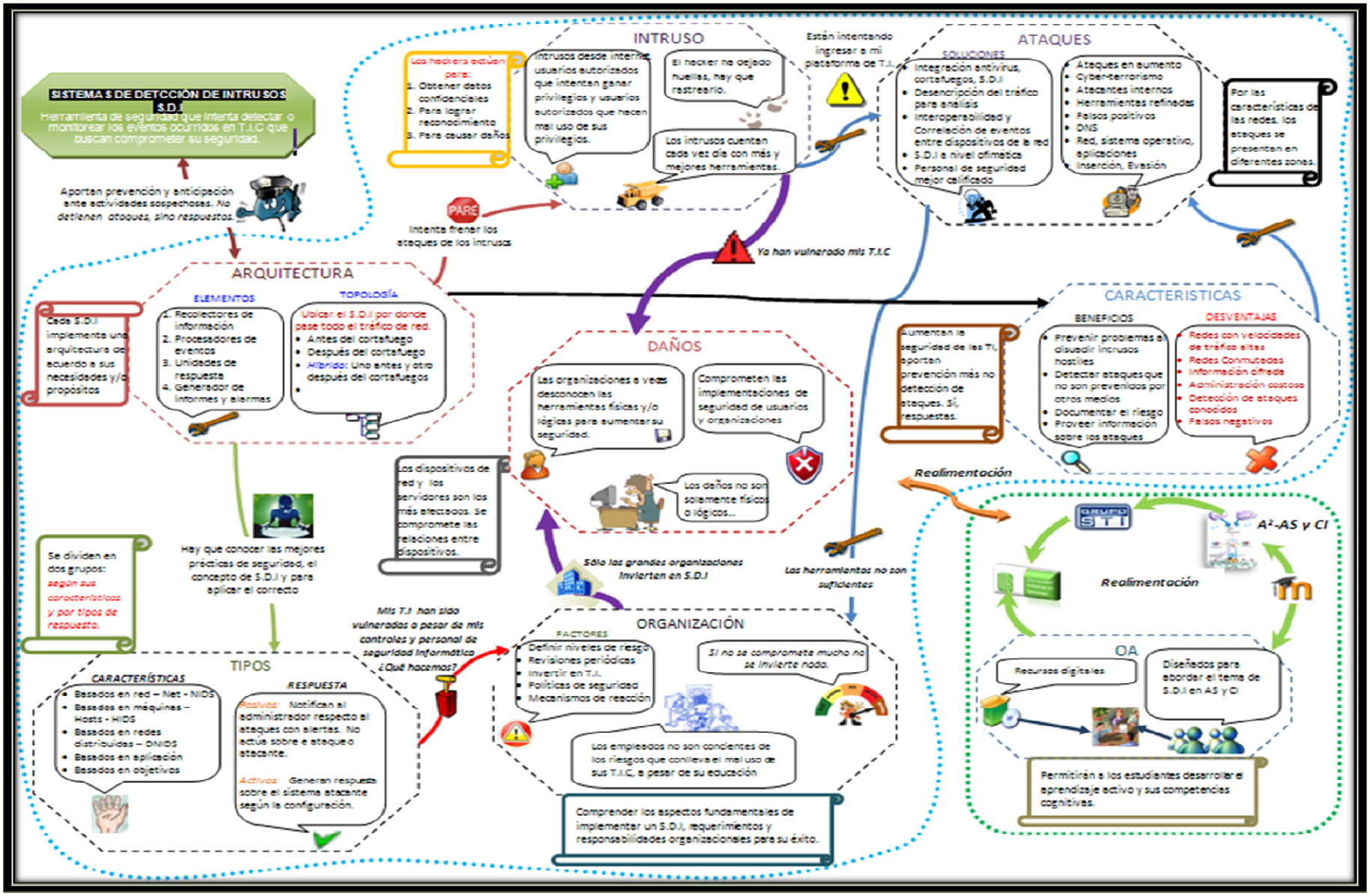


Figura 5. Imagen enriquecida Sistemas de Detección de Intrusos

1.2. OBJETIVOS

1.2.1. Objetivo general

Contribuir como eje integrador en el aprendizaje del estudiante perteneciente al área de Auditoria, Seguridad y Control en informática, mediante el desarrollo de un ambiente educativo soportado en el sistema de gestión de aprendizaje Moodle basado en los lineamientos de competencias cognitivas y aprendizaje activo bajo la disposición de OA.

1.2.2. Objetivos específicos

- Implementar un ambiente educativo para la unidad de aprendizaje Técnicas de Seguridad orientado a la Web y desarrollado en php y Mysql e implantado en la página del grupo STI, se presentará como una actividad SCORM y se desarrollará sobre cuatro temas. La unidad de aprendizaje estará formada por tres componentes que soportaran:

  - ✓ La gestión de datos que permitirá capturar las acciones que el estudiante realice en las actividades propuestas.

  - ✓ La gestión del ambiente que permitirá presentar los contenidos y las actividades a desarrollar por el estudiante.

  - ✓ El control de la interacción que permitirá al profesor dar la valoración a las actividades realizadas por el estudiante de forma cuantitativa o cualitativa.

- Recopilar y estructurar las fuentes bibliográficas digitales de cada tema a desarrollar para que el estudiante pueda consultarlas y aclarar dudas de las actividades teniendo como opciones de búsqueda:

  Vínculos

  - ✓ Estarán ubicados los tipos de fuentes a un lado de la página en un listado de selección organizados así; revistas, documentos, videos[32], presentaciones y portales Web, que al elegirlos presentarán los temas y sub temas organizados y al frente de ellos una síntesis de su

[32] Dado la cantidad de información que transita en línea y al ancho de banda que ocupan, algunos videos serán anexados a la investigación en formato DVD para ofrecerlos como soporte físico a la UA.

temática. Estos últimos serán vínculos a páginas externas para su eventual visualización.

Palabras claves:

- ✓ Las palabras claves serán abstraídas de la información contenida en cada uno de los temas a desarrollar, organizadas y estructuradas para que el estudiante tenga la oportunidad de realizar una búsqueda personalizada, ágil y óptima en línea.

- Diseñar y desarrollar cuatro objetos temáticos de aprendizaje[33] utilizando hipermedia, vinculados a los temas a desarrollar y disponibles durante una semana cada uno para que el estudiante los ejecute. Estarán integrados a elementos como: un glosario, un espacio para recomendaciones, una síntesis de cada tema y un espacio que documentará la experiencia del presente proyecto. A continuación se enumeran:

1. Resolución de casos de estudio
2. Juegos de roles
3. Simulación
4. Cuestionarios tipo ECAES

- Se elaborará una ficha temática en base a cada uno de los objetos para presentar sus objetivos, contenidos, actividad sincrónica y/o asincrónica a desarrollar como metodología Philips 6.6, imágenes enriquecidas, mapas conceptuales y foros que permitirán al estudiante entender la definición de competencias cognitivas y aprendizaje activo, utilizando como medios de apoyo el repositorio de fuentes bibliográficas expuestos anteriormente. Cada OA tendrá una duración de 4 horas presenciales por semana, dividida en dos sesiones de dos horas cada una. Se elaboró un ejemplo ilustrativo de la ficha temática. Ver numeral 3.1.2.

- Aplicar al desarrollo de los objetos propuestos la definición del aprendizaje activo y los lineamientos de la formación basada en competencias cognitivas, “sobre las cuales se fundamenta el modelo de evaluación del ICFES” (ACOFI, 2005) y actualmente articuladas a las pruebas ECAES para contextualizarlos al área de AS y CI.

[33] De ahora en adelante OA.

El Objetivo General y los Objetivos Específicos en conjunto permiten reconocer los puntos básicos para desarrollar un proyecto en la Modalidad de Práctica en Docencia según el Acuerdo Nº 004 del Consejo superior en el año 2.007. *Ver Tabla 6* a continuación.

PRÁCTICA EN DOCENCIA				
	DESCRIPCIÓN	**ACTIVIDADES**	**PROYECTO DE AULA**	**APOYOS**
NORMATIVIDAD UIS[34]	Comprende la experiencia y los aportes del estudiante en la cátedra universitaria mediante el desarrollo de Proyectos de Aula que contribuyan al mejoramiento del proceso de aprendizaje o enriquecimiento de ***Unidades de Aprendizaje*** en las que se desarrollen ***Objetos de Aprendizaje*** mediante el uso de TICs.	Seleccionar la asignatura en la cual desarrollará su Proyecto de Aula. Proponer y/o Evaluar: • Nuevas metodologías • Estrategias didácticas • Procesos de evaluación de asignaturas.	Enriquecimiento de una unidad de aprendizaje utilizando como mediaciones objetos virtuales de aprendizaje; estos desarrollos deberán estar articulados con el proyecto de apoyo al aprendizaje a través de TICs de la Universidad.	El estudiante podrá contar durante el período de desarrollo del Proyecto de Aula con el apoyo de CEDEDUIS para la orientación de su trabajo desde el punto de vista pedagógico y metodológico.
A^2 – AS y CI	Tutoría a los estudiantes de AS y CI del I semestre de 2007 y valoración del desarrollo de las exposiciones propuestas sobre temas de la UA: ***HACKING, PHISHING, S.D.I Y CERTIFICADO Y FIRMA DIGITAL.*** Reconocimiento de los aportes de los estudiantes y sus expectativas que permitieron encaminar el diseño de los OA bajo la orientación de LCGF.	Bajo la tutela del profesor de área se decidió generar los OA para la asignatura de Seguridad en Informática y bajo los lineamientos de competencias cognitivas y aprendizaje activo, utilizando actividades sincrónicas y/o asincrónicas a desarrollar como metodología Philips 6.6, exposiciones, mapas conceptuales, debates y foros.	Basados en las TICs del CENTIC se aplicarán cuatro OA: • ***CASOS DE ESTUDIO*** • ***JUEGO DE ROLES*** • ***SIMULACIONES*** • ***PREGUNTAS TIPO ECAES.***	El apoyo utilizado fue el conocimiento pedagógico del profesor LCGF, las TICs de la UIS, los estudiantes de AS y CI y el CEDEDUIS que bajo sus proyectos permitieron dar forma al proyecto como tal.

Tabla 6. Tabla resumen modalidad Práctica en Docencia para trabajo de grado

[34] Adaptado del ACUERDO Nº 004 de 2007 por parte del Consejo Superior con relación al desarrollo de los trabajos de grado.

1.3. JUSTIFICACIÓN

En la actualidad, la Escuela de Ingeniería de Sistemas e Informática se está viendo abocada a un cambio curricular que conlleva toda una reestructuración en el plan de estudios.

Viendo esto el grupo STI incursionó en el SGA Moodle para redimensionar su funcionamiento y posicionamiento global y así utilizar su estándar como apoyo en el área de Auditoria, Seguridad y Control en Informática, la cual es dictada actualmente por el profesor Luis Carlos Gómez Florez.

El SGA debe permitir la realización de procesos dinámicos e innovadores encaminados hacia la mejora de la calidad de la enseñanza y el aprendizaje, y soportados en el uso de las Tecnologías de Información y Comunicación. El proyecto actual reconoce la necesidad de desarrollar un medio facilitador en la tarea docente y estudiantil.

Es aquí donde entra a jugar un papel muy importante la consecución de la unidad de aprendizaje de Técnicas de Seguridad para contribuir al desarrollo de la misma. La evolución de la unidad de aprendizaje irá ligada junto con la del plan de materia puesto que este último es muy joven y requiere la construcción y constante evolución de conceptos para enfocar su contenido estructural a la educación por competencias cognitivas la cual busca potencializar los conceptos adquiridos por el estudiante en busca de un conocimiento empírico y activo.

1.4. IMPACTO Y VIABILIDAD

1.4.1. Impacto

Según las nuevas directrices de las modalidades en los proyectos de grado y en este caso la de práctica en docencia, es relevante empezar a aplicarla para promover e incentivar su desarrollo y evolución, además para ir a la par con la implementación de metodologías que contribuyan al mejoramiento del aprendizaje.

El estudiante como participante activo y constructor de su conocimiento será el encargado de romper con los paradigmas actuales del aprendizaje. Construir conocimiento es un reto por parte del autor del proyecto y de los estudiantes, pues su vínculo durante el desarrollo del presente proyecto será

el que permitirá saber cuáles son sus necesidades para lograr plasmarlas en el producto software que se desarrollará.

La implementación de la unidad de aprendizaje servirá como modelo en la construcción de actividades que propendan un mejor desempeño, un mayor y mejor aprovechamiento de las herramientas TICS que provee la universidad y la disposición por parte del estudiante. El profesor proveerá su conocimiento en la creación y consecución de esta.

1.4.2. Viabilidad

El SGA Moodle es una herramienta organizacional y estructural que permite al profesor actualmente manejar la unidad de aprendizaje en línea para la asignatura de Seguridad Informática y al estudiante acceder a la información administrativa (cualitativa y cuantitativa) relacionada con las actividades propuestas en la misma.

El proyecto cuenta actualmente con el SGA Moodle con alojamiento y espacio en la web costeado por el grupo STI, siendo un paso importante en la disponibilidad necesaria para poner en marcha el presente proyecto. Moodle es libre de licencia y documentación por lo tanto permite conocer sus fundamentos y características de una forma completa y clara, se fundamenta en el lenguaje de programación PHP y MYSQL, ambos también libres de licencia y de amplia documentación.

Según Castrillón “El aprendizaje se entiende como un proceso permanente donde el protagonista central es el estudiante…” (Castrillón, 2006: 28), y estamos de acuerdo con esto ya que aptitud que el estudiante adopte frente a esta metodología de enseñanza permitirá el aprovechamiento de la misma y es su disposición en el cumplimiento de trabajos y actividades dentro de los límites de tiempo establecidos, la prueba fehaciente de su buen desempeño.

Además como aporte de los autores Spinel y Ortiz que enuncian que “Las condiciones sociales, políticas y económicas del nuevo siglo muestran que el perfil del ingeniero actual es muy distinto al del ingeniero de hace varias décadas...” (Caro, 2001: 1). Es por esto que la educación universitaria actual y futura postula a utilizar aprendizaje activo en el desarrollo de su plan de estudios. El usufructo de las competencias como ente facilitador en el desempeño del estudiante es un método renovador.

Otro punto a tener en cuenta es el posible acceso fuera de las instancias universitarias que el estudiante realizara para concluir las actividades correspondientes con la materia. Es ahí donde la infraestructura en TICs de la universidad solventará esto permitiendo que desarrolle todas las actividades propuestas en la unidad de aprendizaje, en horarios y espacios adecuados de forma gratuita. Este último permitirá que el estudiante adopte una modalidad de aprendizaje activo y se apropie del rol que juega dentro de la unidad para lograr un buen desempeño.

Es fundamental dejar en claro el papel que representarán los estudiantes de la asignatura de Seguridad Informática en el transcurso de este proyecto, ya que realizarán exposiciones de los temas a desarrollar. Estas permitirán llevar un registro de sus aportes que se aprovecharán en la ejecución de los OA y Contenidos de Aprendizaje[35].

[35] De ahora en adelante CA.

CAPÍTULO II

2. MARCO TEÓRICO Y METODOLÓGICO

2.1. MARCO TEÓRICO

2.1.1. TICs en la Educación Superior

Para lograr hacer una correcta aplicabilidad de las TICs en instituciones de educación superior es indispensable hacer una "transformación permanente de la estructura organizacional y académica de las mismas…" como lo enuncia (Peña, 2006: 1).

Según la experiencia de UNIANDES (Tibaná, 2003: pp. 2-3), se deben presentar circunstancias propicias para que la implementación de TICs desde la perspectiva docente, permita al estudiante descubrir sus competencias individuales para luego aplicar las grupales.

En este proceso se hace necesaria la presencia de la universidad en las áreas económica, administrativa, logística y formativa a través de sus diferentes áreas de investigación para ponerlas en marcha. A partir de estos preceptos es importante dejar en claro que el papel docente es primordial y se hacen necesarios unos cuestionamientos en torno a su rol:

- La evaluación docente que genera la universidad ¿es suficiente?
- ¿Las TICs presentes son las que el docente necesita?
- ¿Qué expectativas tiene el docente del aprendizaje en línea?

La aplicabilidad de TICs en un ambiente de aprendizaje no está sujeto solamente a éstas sino a que"…posibilite la interacción del estudiante con fuentes diversas de información" (Peña, 2005: 37), para lograr aplicar las definiciones teóricas de aprendizaje en línea dentro de sus procesos de formación académica.

2.1.2. TICs en el Proyecto Educativo de la UIS

> *En la Universidad Industrial de Santander, mediante el proyecto ProSPETIC, se definió una **política** y se diseñaron **estrategias** tendientes a asegurar condiciones que permitan, mediante sistemas de aprendizaje en línea ofrecer experiencias de aprendizaje con elevados estándares de calidad.*

A partir del párrafo anterior que presenta un aparte del Resumen Ejecutivo del ProSPETIC *(Peña, 2005: 1)* nos damos cuenta que la línea de

investigación del Grupo STI sigue los lineamientos del proceso y permite generar conocimiento a través de sus investigaciones.

Con este proceso en desarrollo se están diseñando las fases de profundización que permitirán incursionar gradualmente en sus TICs y servirán como medios de apoyo para las áreas que la UIS ofrece (Cruz, 2006). Como resultado de esto se pueden ver algunos proyectos de pregrado que muestran el diseño instruccional.

2.1.3. Proyectos interdisciplinarios

2.1.3.1. En la UIS

PROYECTOS EN POSGRADO	
PROYECTO	**RESUMEN**
AVA DE SOPORTE A LA EDUCACIÓN SUP…, (Lizcano, 2006)	Investigación proyectada a dar a conocer la implementación de los SGA en procesos de aprendizaje, la utilización de SGA, establecimientos de pautas y lineamientos pedagógicos.
MULTIMEDIA Y CONSTRUCCIÓN COMPETENCIAS… (Vásquez, 2006)	Análisis de los diferentes factores que impiden un correcto desarrollo en el área de anestesiología y por ende propuesta de métodos alternativos de enseñanza que suplan estos inconvenientes.
PROTOTIPO PARA EL DESARROLLO DE… BASADOS EN AVA. (Castrillón, 2005).	El trabajo presenta un diagnóstico y caracterización de perfiles de usuario, para el desarrollo de un programa de especialización en línea que permita romper con los paradigmas que presentan los AVA dentro del campus universitario.

Tabla 7. Proyectos en Posgrado en relación a A2- AS y CI

2.1.3.2. En la EISI

PROYECTOS EN PREGRADO	
PROYECTO	**RESUMEN**
DISEÑO INSTRUCCIONAL EN COMPETENCIAS …(Cruz, 2006).	Presenta la construcción del diseño instruccional de análisis Numérico I bajo la visión de competencias y OA .
MÓDULO APOYO A LA ENSEÑANZA BORROSA… (Valdivieso, 2007)	Proyecto aplicativo en el SGA Moodle que diseña OA para presentar los contenidos de la Lógica Borrosa y estructurar sus contenidos.
MÓDULO DE APOYO AL APRENDIZAJE DERIVA (Angulo, 2006)	se crearon OA basados en el estándar SCORM para integrarlos a Moodle…”.

Tabla 8. Proyectos en pregrado en relación A2 – AS y CI

2.1.3.3. En el Grupo STI

PROYECTOS	
PROYECTO	**RESUMEN**
AVA PARA APOYAR LAS ACTIVIDADES ACADÉMICAS … (Maestre, 2006)	Ambiente de aprendizaje diseñado para mejorar la gestión de aprendizaje de los estudiantes y del profesor.
AMBIENTE COMPUTACIONAL PARA EL APRENDIZAJE… (Mendoza, 2003)	Desarrollo de una ambiente basado en la metodología JIGSAW utilizando TICs, como propuesta para el mejoramiento del aprendizaje bajo dirección profesor LCGF.

Tabla 9. Proyectos en el grupo STI

2.1.4. Área de AS y CI

2.1.4.1. Estructura del curso

Universidad Industrial de Santander **Escuela de Ingeniería de Sistemas e Informática – AS y CI**									
INFORMACION BÁSICA DE LA ASIGNATURA									
PROGRAMA		**ASIGNATURA**							
Nombre	**Cód.**	**Nombre**	**Cód**	**Créd**	**Nivel**	**H. Presenciales.**	**H. Individual.**	**Naturaleza**	Elaborado
Ingeniería de Sistemas e informática	**11**	Seguridad Informática	**22490**	**4**	**7-10**	**4**	**16**	**Electiva Prof.**	**LCGF**
PRESENTACIÓN DE LA ASIGNATURA									
JUSTIFICACIÓN									
Desde las exigencias del negocio, la asignatura contribuye en gran parte en el desarrollo profesional y laboral ya que permite conocer los últimos avances de la seguridad informática como aporte al desarrollo local, regional, nacional y global dados los daños culturales y económicos que genera.									
COMPETENCIAS DESARROLLADAS									
a. Introducción y Generalidades ▪ Asociar los diferentes programas académicos en AS y CI en Colombia ▪ Practicar las normas de comunicación en los SGA **b. Riesgos y controles en sistemas de TI** ▪ Identificar los niveles de riesgo en los Sistemas Informáticos ▪ Asociar cada nivel con los medios de control necesarios ▪ Distinguir las principales diferencias entre cada nivel de riesgo ▪ Proponer solución a los niveles de riesgo vulnerados e identificados en casos de estudio **c. Marco legal del derecho Informático** ▪ Interpretar los objetos de las áreas del derecho informático ▪ Diferenciar delito de delito informático ▪ Definir los principios de protección de datos ▪ Ejemplificar las figuras delictivas y tipos de fraudes ▪ Reconocer la legislación colombiana concerniente al derecho informático						**d. Continuidad de negocios (BCM)** ▪ Examinar los antecedentes de BCM ▪ Relacionar TI con BCM ▪ Identificar el rol del Ingeniero de sistemas en la BCM ▪ Elaborar un plan de contingencias **e. Normas Técnicas Colombianas en Seguridad Informática – NTC – ISO 27001-17799** ▪ Identificar y comprender las técnicas de Seguridad ▪ Proponer técnicas de representación gráfica y/o escrita para las normas ▪ Sustentar las propuestas de representación de las normas f. **Técnicas de Seguridad** ▪ Clasificar las referencias bibliográficas que apliquen a la UA ▪ Fundamentar en contexto los temas de la UA ▪ Describir casos de uso ▪ Relacionar los recursos ofrecidos por el SGA con la función que cumplen			
UA									

<table>
<tr><td>a. Introducción y Generalidades
b. Riesgos y controles en sistemas de TI
c. Marco legal del derecho Informático</td><td>d. Continuidad de negocios (BCM)
e. Normas Técnicas Colombianas en Seguridad Informática – NTC
f. Técnicas de Seguridad</td></tr>
<tr><td colspan="2">METODOLOGÍA</td></tr>
<tr><td colspan="2">Coherente con la nueva propuesta institucional que se ubica dentro de la metodología activa - competente que permite al estudiante ser partícipe en la construcción de su conocimiento, cada sesión permite evidenciar la secuencia y relación entre los componentes tanto de los contenidos como de las competencias que se pretender alcanzar mediado a través del SGA Moodle.</td></tr>
<tr><td colspan="2">EVALUACIÓN</td></tr>
<tr><td colspan="2">Dado el orden expuesto a las UA se generan actividades sincrónicas y asincrónicas en el SGA como tareas, talleres, foros, wikis, etcétera, fundamentados en recursos que permiten al estudiante fomentar conocimiento individual y grupal basado en un puntaje de 0-100 que el profesor propone en común acuerdo con los estudiantes.</td></tr>
<tr><td colspan="2">OBJETIVO GENERAL</td></tr>
<tr><td colspan="2">Dar a conocer la importancia del aprendizaje en línea mediante el uso del SGA Moodle en el desarrollo de la asignatura de Seguridad Informática con el fin de crear conocimiento activo y competente.</td></tr>
<tr><td colspan="2">OBJETIVOS ESPECÍFICOS</td></tr>
<tr><td>▪ Explorar contenidos actuales en el área de AS y CI
▪ Introducir al estudiante en el campo de riesgos y controles de las TI
▪ Permitir al estudiante reconocer el marco legal del derecho informático aplicable dentro de una organización</td><td>▪ Entender los antecedentes, conceptos e importancia de la Continuidad del Negocio.
▪ Analizar las Normas Técnicas Colombianas de Seguridad Informática.
▪ Estar a la vanguardia en las Técnicas de Seguridad Informática.</td></tr>
<tr><td colspan="2">BIBLIOGRAFÍA</td></tr>
<tr><td>▪ Álvarez, Marañón. Seguridad Informática para empresas y particulares. Editorial Mc Graw Hill, 1a. Ed. España, 2.004
▪ Icontec. Norma técnica Colombiana NTC-ISO/IEC 17799-2004/12/0. Código de buenas practicas para la gestión de la seguridad de la Información.</td><td>▪ Calder, Alan. Nueve claves para el éxito -Una visión general de la implementación de la norma NTC-ISO/IEC 27001.
▪ Grupo de estudios en Internet, comercio electrónico y telecomunicaciones e informática. Internet, Comercio Electrónico y Telecomunicaciones.</td></tr>
</table>

Tabla 10. Información de AS y CI

2.1.4.2. Unidades de Aprendizaje

a. Introducción y Generalidades

Permite entender la metodología utilizada por el profesor LCGF, TI, envío de archivos a través del SGA Moodle, formas de evaluación y novedades.

b. Riesgos y controles en sistemas de TI

Concepto de riesgo, Concepto de control. Niveles de Riesgo y sus mecanismos de control: Acceso general, Acceso a funciones de procesamiento, Ingreso de datos, Ítems rechazados o en suspenso, procesamiento, estructura organizativa y cambios a los programas.

c. Marco legal del derecho Informático

Derecho informático, Áreas del derecho informático, Principios de protección de datos, Derechos de explotación de obras intelectuales, Delito Informático, Figuras delictivas y tipos de fraudes informáticos.

d. Continuidad de negocios (BCM)

Antecedentes, concepto e importancia. TI y continuidad del negocio. El rol del Ingeniero de sistemas en la BCM. Plan de contingencias.

e. Normas Técnicas Colombianas en Seguridad Informática – NTC

Icontec - ISO. Código de buenas prácticas para la gestión de la seguridad de la Información -NTC-ISO/IEC 17799-. Técnicas de seguridad, Sistema de gestión de la seguridad de la Información -NTC-ISO/IEC 27001.

f. Técnicas de Seguridad

Esteganografía en imágenes, Informática Forense, Biometría, Hacking, Criptografía, Detección de intrusos, Seguridad en Redes, Firma y certificación Digital.

2.1.5. Competencias Cognitivas

De acuerdo con (Ferrández, 1997)[36] que enuncia que "arrancando de la capacidad se llega a la competencia", influenciada por factores extrínsecos sociales, económicos, culturales o políticos que permiten llegar a la definición estandarizada y la cual el proyecto adopta: ***saber hacer en contexto*** bajo un conocimiento teórico práctico que permite sustentar los conocimientos

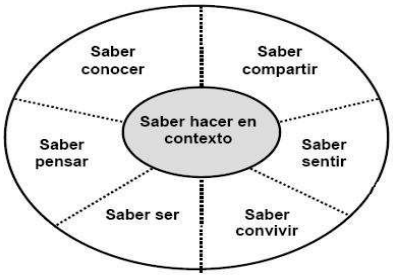


Figura 6. Sentido de las competencias

adquiridos por el estudiante. Por ejemplo cuando alguien lee un texto y lo *interpreta* (saber hacer).

"Desde el punto de vista universitario debería preocupar el liderazgo que genera un conocimiento responsable" como lo expone (Suárez, 2005) ya que así se llegaría a un estudiante competente, con menos dificultades en su desarrollo como se ve en las universidades del país.

- ***Competencias Interpretativas***

[36] Ver [FERNÁNDEZ1999] en bibliografía para mayor referencia.

"Observable en acciones encaminadas a encontrar el sentido de un texto, un problema, una gráfica, un diagrama de flujo…" (ACOFI, 2005: 23). Tal y como lo expone ACOFI son las competencias que le dan instrumentos a un estudiante para desenvolverse en un contexto.

- ***Competencias Argumentativas***

Es la expuesta por el estudiante en el desarrollo de áreas de su disciplina como por ejemplo resolución de casos, exposición de temas, discusiones que revelan en él la capacidad de raciocinio y comprensión para sustentar algo que puede ser o no cierto, en muchos casos son ocultadas por temor a expresar lo que se sabe.

- ***Competencias Propositivas***

Como futuros Ingenieros de Sistemas, diseñadores de soluciones a la medida y consecuentes de los problemas sociales, políticos, etcétera, del país, se denota esta capacidad en el estudiante cuando es capaz de disipar sus propias dudas ante un tema o una situación utilizando las herramientas que tenga a la mano.

2.1.5.1. El ECAES

- **Contenidos temáticos referenciales para Ingeniería de Sistemas**

De acuerdo a un consenso de las facultades de ingeniería del país hay cuatro áreas primordiales aplicables en las preguntas del ECAES[37], éstas hacen parte del plan de carrera en la UIS[38].

2.1.5.2. Competencias aplicables a Ingeniería de Sistemas

Según ACOFI, existen unas competencias con características comunes a todas las ingenierías (ACOFI, 2005: ibídem), las cuales deben dar las capacidades suficientes a un estudiante para desenvolverse en su área de conocimiento. Las concernientes a Ingeniería de Sistemas, son:

d1. *Utilizar teoría, prácticas y herramientas apropiadas para la solución de problemas de programación.*

[37] Para mayor referencia véase [12] en bibliografía.
[38] Para mayor referencia véase [13] en bibliografía.

d2. *Modelar sistemas, componentes o procesos informáticos que cumplan con especificaciones deseadas.*

d3. *Dimensionar y evaluar alternativas de soluciones informáticas.*

"Los grupos de competencias señalados se denominan ***COMPONENTES DE LA PRUEBA ECAES"*** *– incluyen además las competencias inherentes para las ingenierías en general, (op. cit.: 26)*. Permitiendo así clasificar las competencias cognitivas.

2.1.5.3. Competencias Cognitivas de la UA

Se subdividieron en dos categorías; GENERALES y ESPECÍFICAS, la primera es inherente a los cuatro temas y la segunda es la manifiesta en cada tema a desarrollar. *Ver numeral 2.2.6.*

INSTRUMENTOS DE CONOCIMIENTO[39]

Figura 7. Instrumentos de conocimiento

2.1.6. Ambiente de Aprendizaje

2.1.6.1. Conceptos

Siguiendo la definición de (Castrillón, 2006: 27), el ambiente de aprendizaje son las "…condiciones de una institución educativa, orientadas a favorecer el logro de los fines de ésta". El ambiente es el que provee las capacidades, competencias, habilidades y valores que le permitan desarrollar sus actividades.

[39] Citado en PEI Colegio Bilingüe Divino Niño – Bucaramanga. p. 86.

2.1.6.2. Componentes[40]

Están a cargo del docente para lograr aplicar su área de conocimiento. Según (Barbosa, 2006), está comprendido por:

Contenido, interacción, evaluación, seguimiento y orientación, los cuales pueden estar articulados al currículo[41]

Figura 8. Deber ser de un currículo.

2.1.6.3. Funciones Pedagógicas

A partir de los planteamientos de (Zapata, 2003: 8), se clasifican:

- Utilizar los recursos disponibles para llevar un control del estudiante
- Relacionar a los estudiantes para el desarrollo de actividades
- Uso de medios de evaluación y autoevaluación didácticos
- Manejo de información adecuada en el contexto desarrollado
- Organización de los componentes del ambiente

2.1.6.4. Integración Espacio – Tiempo

Según las evidencias tomadas en el CENTIC, ver numeral 2.2.1.2.2 y la opinión de (Duarte, 2003), la cual presenta los principios espaciales dentro de un ambiente de aprendizaje, se destacan:

"***El ambiente de la clase ha de posibilitar el conocimiento de todas las personas del grupo y el acercamiento de unos hacia otros…***"

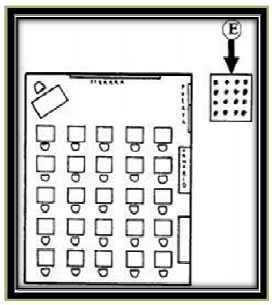


Figura 9. Disposición espacial salón tradicional

[40] PEI, op. cit., p. 87.
[41] Conjunto de propuestas que permiten caracterizar un ambiente de aprendizaje.

DISPOSICIÓN ESPACIAL DE UN SALÓN "TRADICIONAL"

- Provee una comunicación unidireccional y las actividades del grupo son iguales e individuales, además generan competencia en el grupo más no cooperación.

2.1.6.5. Costo

"En herramientas de código abierto hay que preocuparse del capital humano…". (Tibaná, 2003).

Esto permite disminuir los costos ostensiblemente y permite aprovechar los recursos económicos en otras TICs que a veces no son tenidas en cuenta pero que en el desarrollo del aprendizaje son importantes.

2.1.6.6. Estado en la UIS

En el caso que hemos tratado a lo largo de la investigación, es muy claro el papel que juegan los profesores dentro del desarrollo del ProSPETIC y es por esto que de acuerdo a los lineamientos del mismo, es necesaria su participación a través de las capacitaciones que la universidad ofrece con el CEDEDUIS. También es importante destacar que los grupos de investigación, como en este caso el STI, que no ha seguido las directrices directas del mismo, participan a través del uso y desarrollo de proyectos de investigación *–como este Proyecto de Aula* - en TICs en pregrado y posgrado.

2.1.7. Aprendizaje activo

"...el aprendizaje es un proceso activo y de construcción que lleva a cabo, en su interior, el sujeto que aprende" (Castrillón, 2005. p 36). Esto quiere decir que el estudiante según sus capacidades puede ser competente o no dentro de un grupo dada la disposición y las herramientas que tenga.

Existen tres tipos de modelos pedagógicos: heteroestructurantes, interestructurantes y autoestructurantes. Para el presente trabajo aplica el autoestructurante según el cual "…la responsabilidad en la búsqueda del conocimiento recae en el estudiante y el docente es un acompañante de la acción educativa" (Ruiz, 2006: 6). Además el estudiante es el que dirige y da forma a su aprendizaje.

2.1.7.1. Constructivismo

El aprendizaje activo se enmarca dentro de la teoría constructivista que define: “los estudiantes son el eje y los protagonistas del proceso y son ellos quienes deciden cuándo y cómo quieren aprender” (RUIZ, 2006: 1) y a partir de ahí se desarrollan los OA para aplicar esta metodología en las clases de AS y CI. Aportes al aprendizaje activo: (Castrillón, 2005: 32):

- El estudiante es un agente activo frente al saber, su relación sujeto-aprendizaje debe ser dinámica.
- Reestructuración conceptual permanente del conocimiento.
- El desarrollo cognitivo es individual.

2.1.7.2. Preceptos

El entorno de aprendizaje centrado en el estudiante, le permite interactuar con otros estudiantes, el docente, las TICs, etcétera... y además “…provee al estudiante con un andamiaje de apoyo para desarrollar sus conocimientos y habilidades…” A partir del estudio de (Trías, 2004: 27).

De acuerdo con esto y luego del análisis al ProSPETIC la universidad vira hacia el logro de la aplicabilidad de sus TICS en el proceso de enseñanza aprendizaje. Es por esto que es importante hacer partícipes y apropiar los roles que cada uno desempeña.

2.1.7.3. Actividades (Ruiz, 2006)

Figura 10. Niveles de retención según actividades propias del aprendizaje activo

Métodos y mecanismos de enseñanza que promueven el Aprendizaje Activo (Caro, 2003):

- El trabajo en grupo, desarrollo de aprendizaje a través de actividades experimentales y relación con el mundo exterior.

- Objetivos claros, métodos de enseñanza acorde con los objetivos, mecanismos de apoyo (TICs), sistemas de evaluación concretos.

2.1.8. SGA Moodle

AS y CI está relacionada directamente con el concepto de aprendizaje en línea debido a que en la actualidad su formación académica está sustentada en el SGA "*herramienta informática y telemática organizada en función de unos objetivos formativos de forma integral*" (Zapata, 2003:1) Moodle, el cual ofrece recursos que propenden a la comprensión de sus contenidos. En (Lizcano, 2006: 74) se muestran las estadísticas de uso y la expansión del mismo.

2.1.8.1. Estándar SCORM(**S**harable **C**ontent **O**bject **R**eference **M**odel)[42]

Resultado de la iniciativa de ADL[43] y la colaboración de IMS e IEEE. Es el desarrollo de OA reusables y portables, que permite independizar los contenidos de las implementaciones para que los OA sean fácilmente compartidos entre múltiples SGA. Establece una jerarquía de tres niveles de los contenidos educativos:

- Recursos (Assets)
- SCOs **(Sharable Content Objects – OA Compartibles**)
- Agregación de contenidos

2.1.8.2. Objetos de Aprendizaje[44]

"*...composición digital basada en un objetivo de enseñanza que necesariamente debe poseer un contenido, una aplicación, una evaluación, algunos vínculos de profundización del contenido y un metadato".*

2.1.8.2.1. Funciones[45]

•**Estimular** el aprendizaje activo.

---

[42] Para mayor referencia diríjase a [14] en bibliografía.
[43] Para mayor referencia diríjase a [15] en bibliografía.
[44] Para mayor referencia diríjase a [16] en bibliografía.
[45] Para mayor referencia diríjase a [17] en bibliografía.

•**Promover** el trabajo colaborativo.
•**Posibilitar** el acceso remoto a los contenidos de aprendizaje.
•**Posibilitar** la integración de diferentes elementos multimedia.
•**Contribuir** a la actualización permanente de profesores y estudiantes.
•**Estructuración** de la información en formato hipertexto.

2.1.8.2.2. Características

Figura 11. Características de un OA

2.1.8.2.3. Nivel de Globalidad

Un Objeto de aprendizaje **temático** (OAt), presenta un objetivo orientado a un tema específico, permite el desarrollo de objetos aún más específicos. En este proyecto se desarrollan OAt.

2.1.8.2.4. Evaluación

Debe asegurar al profesor una correcta valoración del contenido aprendido por el estudiante. Se debe mostrar al estudiante la respuesta correcta una vez resuelto el OA con su respectivo puntaje. En esta investigación se diseñarán OA basados en las siguientes técnicas para propender una evaluación acorde:

Resolución de casos de estudio
Juegos de roles
Simulación
Cuestionarios tipo ECAES

2.1.8.2.5. Profundización

Los OA se profundizarán a través de actividades sincrónicas y/o asincrónicas como metodología Philips 6.6, imágenes enriquecidas, exposiciones, wiki, cuestionarios, mapas conceptuales, foros, etcétera.

2.1.9. Áreas temáticas del Ambiente

"El tema de seguridad informática no es ajeno a la dinámica del mundo…"[46], pues su gama de actividades es mayor a la capacidad de análisis, por ende hay que saber hoy las tendencias futuras. Temas a desarrollar en el ambiente:

2.1.9.1. Hacking

En la actualidad y mucho antes de lo que podamos imaginar podríamos estar siendo manipulados sin darnos cuenta, esto debido a la suspicacia de personas que utilizan las TI para realizar actividades ilícitas a través de redes de computadores e infiltrarse en lugares remotos accediendo a todo tipo información.

Todo esto apoyado en la gran red de la Internet que ha catapultado a muchas personas que con o sin experiencia logran acciones encaminadas a transgredir la seguridad de un sistema informático. No sin menospreciar las TI de las empresas. Siendo la información un recurso tan valioso, se hace necesario conocer diferentes estrategias para la protección de la misma y así prepararse frente a las vulnerabilidades que los atacantes aprovechan.

La práctica de este tipo de actividades se conoce con el nombre de Hacking, que ha nacido de la curiosidad, habilidad y capacidad que los hackers aprovechan de las herramientas informáticas; esto no es sinónimo de debilidad para las organizaciones sino de habilidad para reconocer que han visto algo que su infraestructura de seguridad informática no ha descubierto y de ahí la importancia de conocer la forma como estos atacante actúan.

2.1.9.2. Phishing

Las vulnerabilidades en Internet continúan planteando amenazas serias porque permiten a los atacantes evadir las medidas tradicionales de seguridad, permitiendo a los atacantes el acceso a información confidencial sin necesidad de comprometer los servidores.

[46] Para mayor referencia diríjase a [18] en bibliografía.

La actividad de phishing consiste en la obtención de claves y datos privados de los usuarios de Internet mediante la intermediación no visible entre el envío de datos y el servidor. Todo esto con la intención de realizar compras fraudulentas o el retirar cantidades exageradas de dinero de las cuentas de los clientes sin que el banco tenga soporte alguno para la negación a estas transacciones. Solamente los bancos pueden utilizar herramientas que permitan sospechar de operaciones inusuales de sus clientes.

Dentro de este abanico de modalidades se encuentra una muy común utilizada por los delincuentes mediante la obtención de datos de cuentas bancarias a través del envío de e-mails con formularios de recogida de datos adjunto o bien a través de la simulación de la Web oficial de la entidad bancaria, la cual reproduce, con total fidelidad, la original. La mejor arma para combatir el phishing es estar informado de que existe y de cómo se lleva a cabo.

2.1.9.3. Sistemas de Detección de Intrusos (S.D.I)

Hoy en día cuando las empresas están perdiendo dinero sin vislumbrar el alcance que puede llegar a tener la intromisión de alguien sin acceso autorizado en sus TI es necesario el apoyo de una herramienta que las monitoree.

Esto quizás es solo el comienzo puesto que los accesos no autorizados se realizan en cualquier momento sin respetar fecha ni horario; un SDI es un software dedicado a evitar la intromisión de estos personajes las 24 horas del día y los siete días de la semana. Tiene la capacidad de prevenir y dar aviso de posibles ataques, además de facilitarnos el análisis posterior en caso de una intrusión en el sistema.

Un SDI no debe ser nunca un sustituto de una buena política de seguridad en la red que vayamos a instalar. No serviría de nada tener un SDI instalado si se dejan puertos abiertos en el servidor, contraseñas a la vista de alguien o empleados desleales. Por tanto, un SDI siempre deberá ser un complemento al sistema de seguridad ya instalado, es decir, corresponde a una capa adicional de protección.

2.1.9.4. Firma y Certificado Digital

El comercio electrónico cada día abarca más áreas y ante una positiva respuesta de las herramientas que ofrece, se está garantizando su adecuado

uso y correspondiente viabilidad. Los documentos electrónicos han empezado a circular entre empresas y personas que ven en este medio respaldo en sus operaciones y además su certificación electrónica permite aumentar la seguridad en el transporte de los mismos.

La firma digital es en esencia un conjunto de datos electrónicos que identifican a una persona en concreto. Esta firma digital suele unirse a documentos que se envían por medio telemático, como si de la firma manuscrita se tratara y permite que el receptor del mensaje esté seguro quién ha sido el emisor, así como que el mensaje no haya sido alterado. Algo que es esencial en las transacciones electrónicas y que el ámbito educativo reconoce para ser analizada y aplicada.

2.1.10. Temas a Evolucionar en el Ambiente

Seleccionados debido a su uso en el área de AS y CI y a las implicaciones que tienen en las TI actualmente, además se catalogaron en este ítem debido a lo extenso de su temática y para permitir dar participación a otros estudiantes que deseen aplicarlos en el SGA.

2.1.10.1. Seguridad en Redes[47]

Alámbrica: En muchas empresas, existen controles significativos en los perímetros de las redes pero no se cuenta con nivel de seguridad interno:

- Las estadísticas indican que la mayor parte de los incidentes de seguridad se originan en los propios funcionarios.
- Adicionalmente, existen cada vez más puntos de acceso a las redes internas que deben ser tenidos en cuenta.
- Usualmente no se cuenta con procedimientos de monitoreo constantes, no se detecta un incidente en forma oportuna.

Inalámbrica: Consta de cifrado y de autenticación. El cifrado se utiliza para cifrar o codificar los datos antes de que se envíen a la red inalámbrica. Con la autenticación se requiere que los clientes inalámbricos se autentiquen antes de que se les permita unirse a la red.

2.1.10.2. Delitos Informáticos[48]

[47] Para mayor referencia diríjase a [19] en bibliografía.
[48] Para mayor referencia diríjase a [20] en bibliografía.

Actividades que han permitido que el delito informático tenga éxito:

- Los empleados dejan a su familia usar sus portátiles corporativos.
- Conectan algún periférico a su computador corporativo.
- Almacenan contenido personal en su computador corporativo.
- Descargan contenido mientras están en el trabajo.
- Tienen poco conocimiento en materia de seguridad.
- Se tiene acceso a áreas que no debería.

2.1.10.3. Biometría[49]

Proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital, palmas, ojos, orejas, etcétera…

2.1.10.4. Virus[50]

Son programas-rutinas capaces de infectar archivos de computadoras, reproduciéndose una y otra vez cuando se accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento. Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero su fin es **PROPAGARSE**.

Es importante destacar que ***el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa***. La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características: *Es Dañino, es Auto reproductor, es Subrepticio*

2.1.10.5. Informática Forense[51]

[49] Trabajo de seguridad II semestre 2006. Adjunto como soporte digital al proyecto.
[50] Para mayor referencia diríjase a [21] en bibliografía.
[51] Para mayor información diríjase a [22] en bibliografía.

Las vulnerabilidades en sistemas de información, las fallas humanas, procedimentales o tecnológicas sobre infraestructuras de computación, ofrecen un escenario para los intrusos informáticos.

La criminalística ofrece un espacio de análisis y estudio sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. Es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

2.1.10.6. Peritaje informático[52]

En un mundo interconectado y digital, las conductas criminales establecen paradigmas y retos que exigen de la justicia, de la academia, del gobierno, de la industria y de la sociedad una respuesta coherente y formal que permita enfrentar la inseguridad informática.

Se deben desarrollar elementos técnicos, jurídicos y administrativos que permitan confrontar, validar y asegurar un proceso ante situaciones donde la evidencia digital, electrónica e informática es primordial. De ahí surge la necesidad de formar personal especializado que permitirá resolver casos en menor tiempo y eficacia.

2.1.10.7. Esteganografía[53]

Método ampliamente utilizado para ocultar mensajes en otros aparentemente inofensivos, para evitar ser detectado por terceros. A diferencia de la criptografía, que busca que un mensaje se torne incomprensivo, la Esteganografía esconde el mensaje dificultando la posibilidad de un ataque. Su campo de análisis es extenso y en la universidad se está abriendo paso a su estudio, sea esta la oportunidad para aprovechar sus posibles aplicaciones en el campo de las TI.

2.2. MARCO METODOLÓGICO

2.2.1. Área de AS y CI

[52] Para mayor información diríjase a [23] en bibliografía.
[53] Para mayor información diríjase a [24] en bibliografía.

2.2.1.1. Observación de la estructura del curso

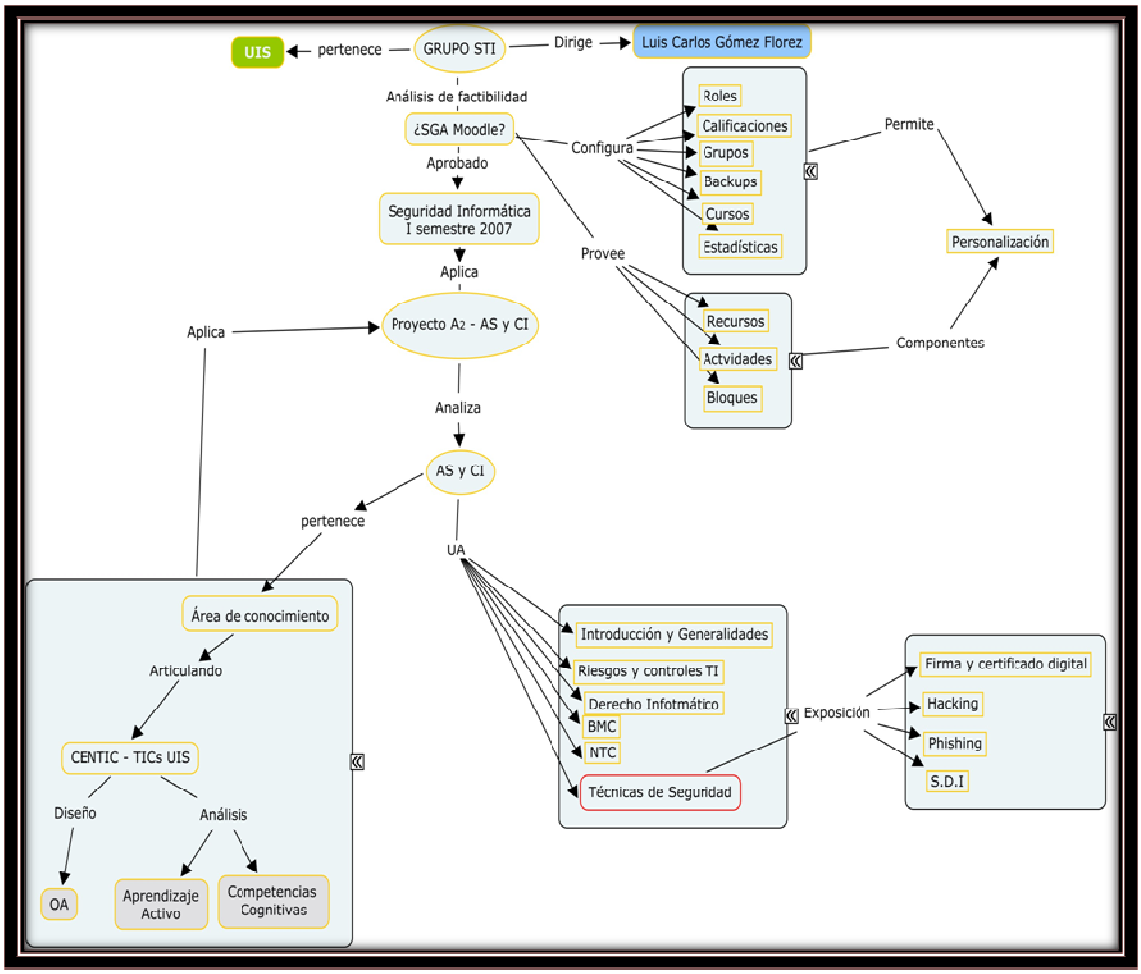


Figura 12. Estructura del curso de AS y CI

2.2.1.2. Seguimiento a estudiantes: I semestre 2007

Se elaboró un cronograma de actividades en conjunto con los estudiantes, profesor y tutor para desarrollar una exposición como objetivo final de la UA. Para efectos del Proyecto de Aula se llevaron a cabo estas actividades con la intención de acercar al estudiante a los temas de competencias y aprendizaje activo, además de conocer sus expectativas hacia la materia. Se utilizaron algunas técnicas de sustentación y actividades apoyadas en el SGA para las discusiones orales así como la posibilidad de seleccionar temas para la UA.

2.2.1.2.1. Cronograma de Actividades

CRONOGRAMA DE ACTIVIDADES PARA EL DESARROLLO DE LA EXPOSICION "UA: TECNICAS DE SEGURIDAD" DURANTE EL II SEMESTRE 2007 - AS Y CI

1.	Selección de temas y conformación de grupos	27 febrero – 01 marzo
2.	Búsqueda de fuentes con respecto al tema propuesto por cada grupo.	06 -27 marzo
	2.1 Cada fuente debe ir con su respectiva fuente bibliográfica y glosario	
3.	Entrega por parte del tutor del disco compacto con la información correspondiente a los temas manejados el semestre pasado.	27 marzo
4.	Comparación de la información de ambos semestres por parte de los estudiantes y filtrar la información de cada grupo.	27 mar- 17 abril
5.	Guardar la información primordial en el disco compacto entregado y devolverlo al tutor	19 abril
6.	Entrega de la información por parte del tutor al grupo con visto y recomendaciones.	17 mayo
7.	Responder primer encuesta basada en información general y en la situación actual de la materia	17 mayo
8.	Dudas y exposición de avances por parte de los estudiantes del desarrollo del tema de exposición.	22 mayo
9.	Preparación de las exposiciones	22 mayo – 19 junio
10.	Responder segunda entrevista basada en el aprendizaje activo	19 junio
11.	Exposición por parte de los estudiantes de AS y CI, repartidos así:	
	19 de junio ***Seguridad en Web Services***. Duración 1 hora	
	19 de junio ***Hacking.*** Duración 1 hora	
	21 de junio ***Informática Forense***. Duración 1 hora	
	21 de junio ***Phishing***. Duración 1 hora	
	26 de junio ***Seguridad en redes***. Duración 1 hora	
	26 de junio ***SDI*** (Sistemas de Detección de Intrusos). Duración 1 hora	
	28 de junio ***Esteganografía en Imágenes.*** Duración 1 hora	
13.	Evaluación de las exposiciones y recomendaciones	02 julio

Figura 13. Cronograma I semestre de 2007 con los estudiantes de AS y

2.2.1.2.2. Evidencias

Se desarrollaron durante el I semestre 2007 las actividades del cronograma para realizar un informe final sustentado bajo una exposición oral. En la siguiente gráfica se observa la entrega de los de las fuentes bibliográficas para la respectiva revisión por parte del autor del proyecto. Se formaron siete grupos relacionados como lo muestra el cronograma. Se generó una realimentación a través de un foro con los estudiantes, dado el interés de los temas.

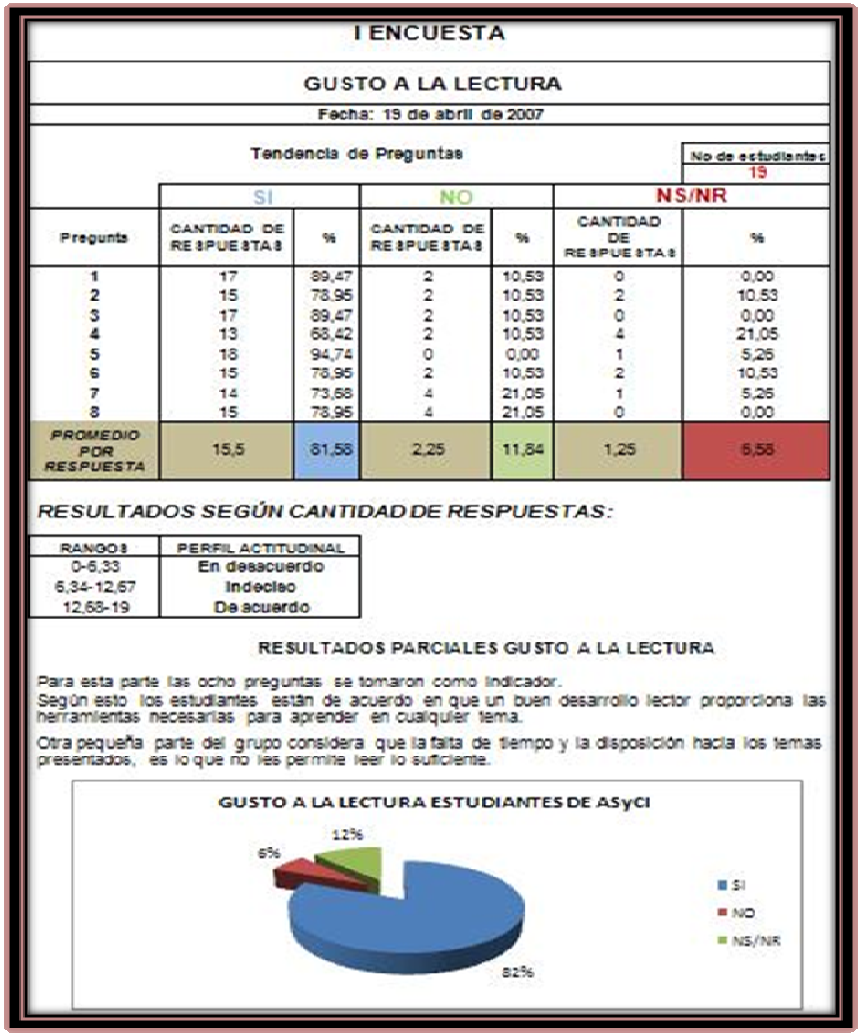
Figura 14. Entrega de evidencias

Se diseñaron dos encuestas para que los estudiantes dieran sus puntos de vista con respecto a temas de interés para el proyecto y así tener un diagnóstico que permita entender los OA a caracterizar según las necesidades y el contexto en el cual se desempeñan los estudiantes y el profesor para el desarrollo de la asignatura. Se presentan a continuación los resultados cuantitativos y cualitativos.

Los formatos de encuesta se pueden ver en el ***ANEXO A***.

A continuación se presentan los resultados:

2.2.1.2.3. I encuesta: “Gusto a la lectura – Disposición a la Asignatura”



I ENCUESTA

GUSTO A LA LECTURA

Fecha: 15 de abril de 2007

Tendencia de Preguntas

No de estudiantes: 15

	SI		NO		NS/NR	
Pregunta	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%
1	17	89,47	2	10,53	0	0,00
2	15	78,95	2	10,53	2	10,53
3	17	89,47	2	10,53	0	0,00
4	13	68,42	2	10,53	4	21,05
5	18	94,74	0	0,00	1	5,26
6	15	78,95	2	10,53	2	10,53
7	14	73,68	4	21,05	1	5,26
8	15	78,95	4	21,05	0	0,00
PROMEDIO POR RESPUESTA	15,5	81,58	2,25	11,84	1,25	6,58

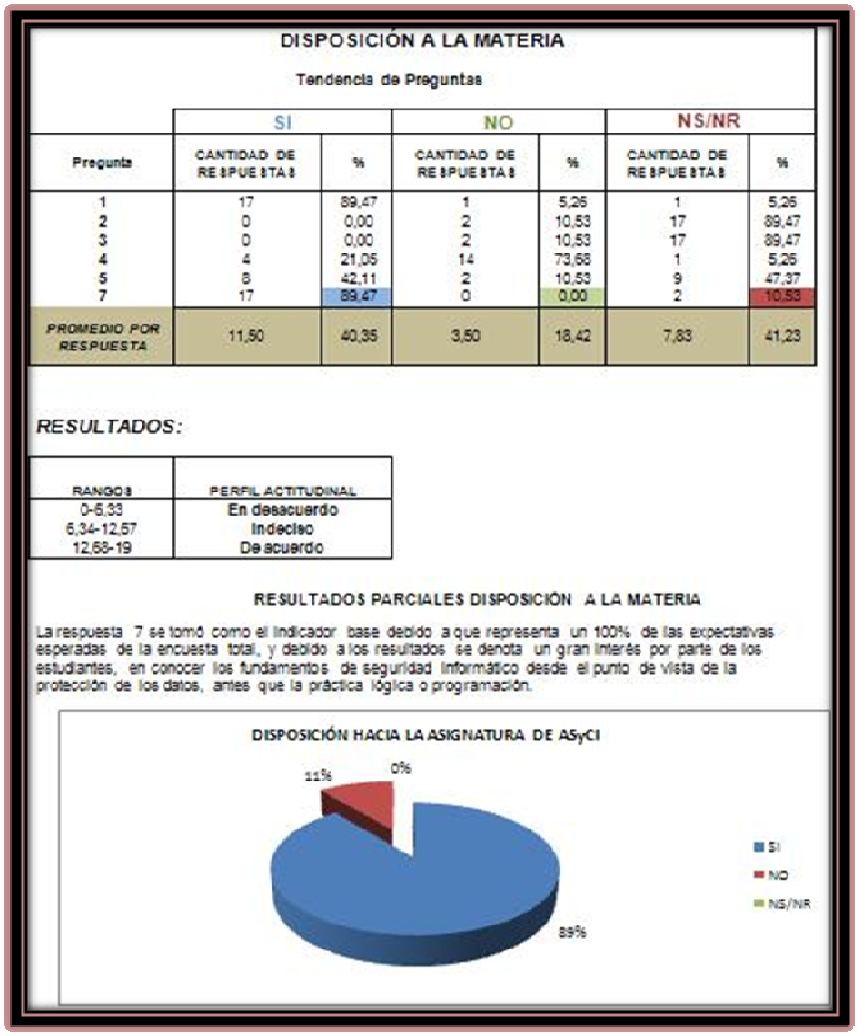
RESULTADOS SEGÚN CANTIDAD DE RESPUESTAS:

RANGOS	PERFIL ACTITUDINAL
0-6,33	En desacuerdo
6,34-12,67	Indeciso
12,68-19	De acuerdo

RESULTADOS PARCIALES GUSTO A LA LECTURA

Para esta parte las ocho preguntas se tomaron como indicador.
Según esto los estudiantes están de acuerdo en que un buen desarrollo lector proporciona las herramientas necesarias para aprender en cualquier tema.

Otra pequeña parte del grupo considera que la falta de tiempo y la disposición hacia los temas presentados, es lo que no les permite leer lo suficiente.



DISPOSICIÓN A LA MATERIA

Tendencia de Preguntas

	SI		NO		NS/NR	
Pregunta	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%
1	17	89,47	1	5,26	1	5,26
2	0	0,00	2	10,53	17	89,47
3	0	0,00	2	10,53	17	89,47
4	4	21,05	14	73,68	1	5,26
5	8	42,11	2	10,53	9	47,37
7	17	89,47	0	0,00	2	10,53
PROMEDIO POR RESPUESTA	11,50	40,35	3,50	18,42	7,83	41,23

RESULTADOS:

RANGOS	PERFIL ACTITUDINAL
0-6,33	En desacuerdo
6,34-12,67	Indeciso
12,68-19	De acuerdo

RESULTADOS PARCIALES DISPOSICIÓN A LA MATERIA

La respuesta 7 se tomó como el indicador base debido a que representa un 100% de las expectativas esperadas de la encuesta total, y debido a los resultados se denota un gran interés por parte de los estudiantes, en conocer los fundamentos de seguridad informático desde el punto de vista de la protección de los datos, antes que la práctica lógica o programación.

Figura15. Resultados cuantitativos I encuesta

RESULTADOS CUALITATIVOS GUSTO A LA LECTURA

1. La mayor parte acuden a Internet o a docentes de área.
2. La mayoría aprendió en la escuela a leer a través de diferentes métodos docentes y los recursos expuestos en su hogar.
3. La mayor parte se autocalifican sobre 5 en su aptitud para leer.
4. Cada estudiante lee según sus necesidades ya sea por sus estudios o gustos.
5. Medianamente los estudiantes siguen métodos como sacar resúmenes, subrayar palabras, leer varias veces, buscar palabras en el diccionario para asimilar mejor el texto leído.
6. Los estudiantes buscan comparar la información recibida con otras fuentes cuando no entienden los conceptos recibidos.
7. Los estudiantes releen cuando un texto les llama la atención o el tema no es muy claro.
8. La búsqueda por Internet es la más usada.

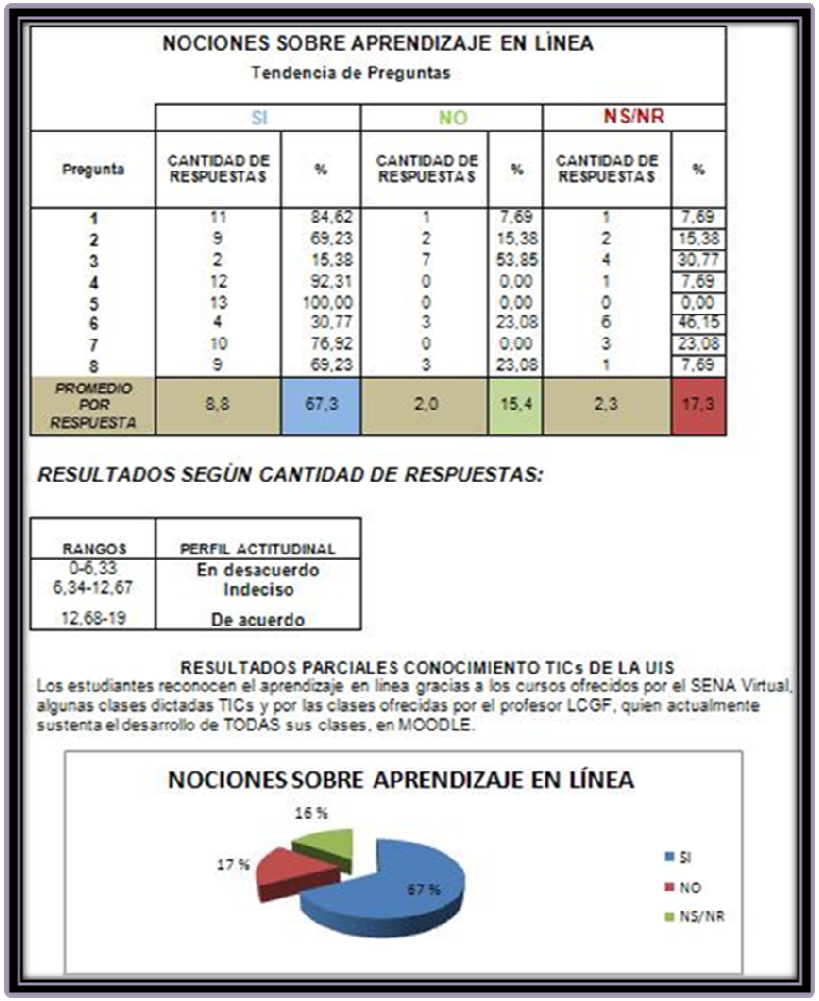
Valoración: Falta redacción e interpretación en algunas preguntas.

RESULTADOS CUALITATIVOS DISPOSICIÓN A LA ASIGNATURA

1. Usan el término en mayor medida en la posible vulnerabilidad de los datos y de la misma persona cuando se refiere a lo cotidiano.
2. Ningún estudiante dio cuenta de que la EISI cuenta con el grupo STI en el tema de Seguridad Informática.
3. Algunos estudiantes han notado que la red ha sido comprometida por diferentes medios, aunque la mayoría los desconoce.
4. Algunos han intentado vulnerar una página web por curiosidad.
5. La mayoría de estudiantes suponen que las grandes empresas deben invertir en TI para su seguridad informática.
6. Un 100% de los estudiantes matriculan esta electiva por curiosidad y las áreas que puede llegar a abarcar.
7. Con prácticas como visitas a empresas o creando aplicaciones.

Valoración: Gracias al desconocimiento estudiantil en el área de seguridad informática se están perdiendo espacios de investigación.

2.2.1.2.4. II encuesta: “Conocimiento TICs de la UIS – Nociones sobre Aprendizaje en Línea”



NOCIONES SOBRE APRENDIZAJE EN LÍNEA

Tendencia de Preguntas

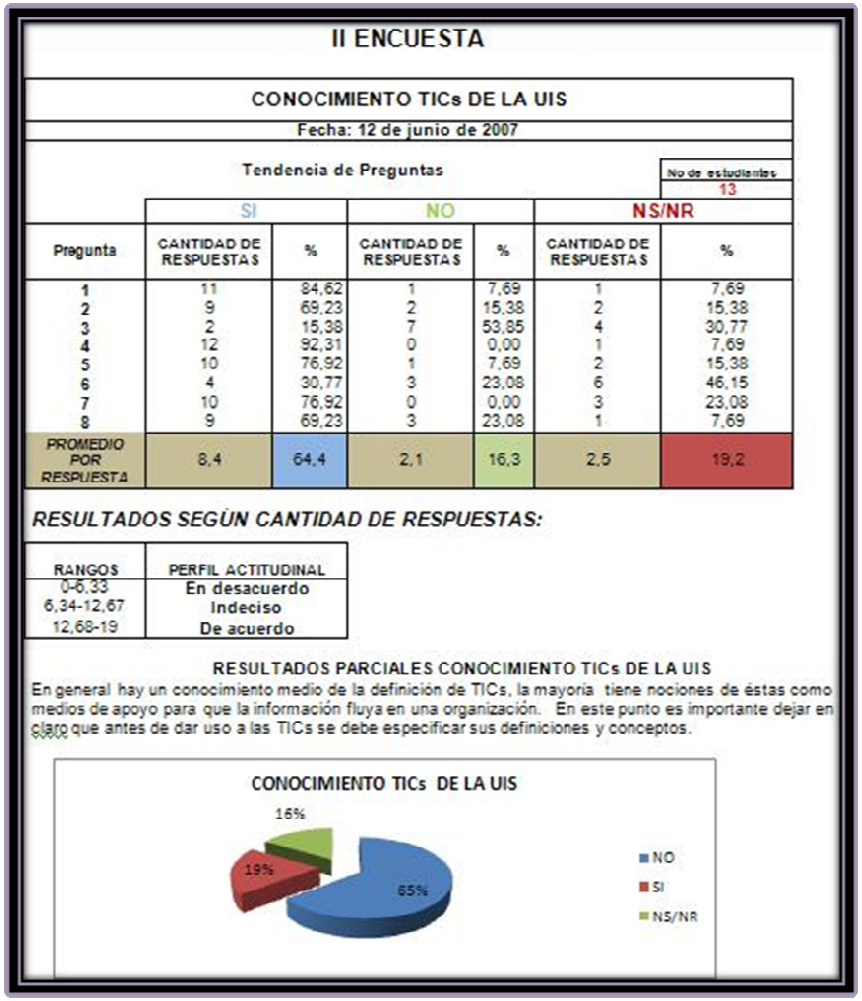
Pregunta	SI		NO		NS/NR	
	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%
1	11	84,62	1	7,69	1	7,69
2	9	69,23	2	15,38	2	15,38
3	2	15,38	7	53,85	4	30,77
4	12	92,31	0	0,00	1	7,69
5	13	100,00	0	0,00	0	0,00
6	4	30,77	3	23,08	6	46,15
7	10	76,92	0	0,00	3	23,08
8	9	69,23	3	23,08	1	7,69
PROMEDIO POR RESPUESTA	8,8	67,3	2,0	15,4	2,3	17,3

RESULTADOS SEGÙN CANTIDAD DE RESPUESTAS:

RANGOS	PERFIL ACTITUDINAL
0-6,33	En desacuerdo
6,34-12,67	Indeciso
12,68-19	De acuerdo

RESULTADOS PARCIALES CONOCIMIENTO TICs DE LA UIS

Los estudiantes reconocen el aprendizaje en línea gracias a los cursos ofrecidos por el SENA Virtual, algunas clases dictadas TICs y por las clases ofrecidas por el profesor LCGF, quien actualmente sustenta el desarrollo de TODAS sus clases, en MOODLE.



II ENCUESTA

CONOCIMIENTO TICs DE LA UIS

Fecha: 12 de junio de 2007

Tendencia de Preguntas

No de estudiantes: 13

Pregunta	SI		NO		NS/NR	
	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%	CANTIDAD DE RESPUESTAS	%
1	11	84,62	1	7,69	1	7,69
2	9	69,23	2	15,38	2	15,38
3	2	15,38	7	53,85	4	30,77
4	12	92,31	0	0,00	1	7,69
5	10	76,92	1	7,69	2	15,38
6	4	30,77	3	23,08	6	46,15
7	10	76,92	0	0,00	3	23,08
8	9	69,23	3	23,08	1	7,69
PROMEDIO POR RESPUESTA	8,4	64,4	2,1	16,3	2,5	19,2

RESULTADOS SEGÙN CANTIDAD DE RESPUESTAS:

RANGOS	PERFIL ACTITUDINAL
0-6,33	En desacuerdo
6,34-12,67	Indeciso
12,68-19	De acuerdo

RESULTADOS PARCIALES CONOCIMIENTO TICs DE LA UIS

En general hay un conocimiento medio de la definición de TICs, la mayoría tiene nociones de éstas como medios de apoyo para que la información fluya en una organización. En este punto es importante dejar en claro que antes de dar uso a las TICs se debe especificar sus definiciones y conceptos.

Figura 16. Resultados cuantitativos II encuesta

RESULTADOS CUALITATIVOS CONOCIMIENTO TICs DE LA UIS

1. En general hay un conocimiento medio de definición de TICs y gira hacia medios de apoyo para la fluidez de la información
2. Las utilizan para consultas académicas en mayor parte.
3. El total de estudiantes está de acuerdo que se aprovecharían más las TICs si los profesores desarrollaran asignaturas en el CENTIC.
4. Todos apoyan que el uso del SGA Moodle les ha permitido romper los paradigmas del aprendizaje en línea y genera mayor actividad.
5. No se conoce la mayor parte de herramientas con los que cuenta Moodle.
6. Los estudiantes creen que el CENTIC, debe generar espacios para la investigación como laboratorios.
7. Piensan la gran mayoría, que debe haber masificación a todas las carreras para el uso del CENTIC.
8. Algunos estudiantes reconocen que el sistema de reservas del CENTIC presenta errores, puestas éstas se hacen en salas que no reserva.

Valoración: El CENTIC ofrece Tecnologías de Comunicación que la mayoría de estudiantes no aprovecha. Además, Moodle se podría aprovechar más. Con la presente investigación se pretende apoyar este aspecto.

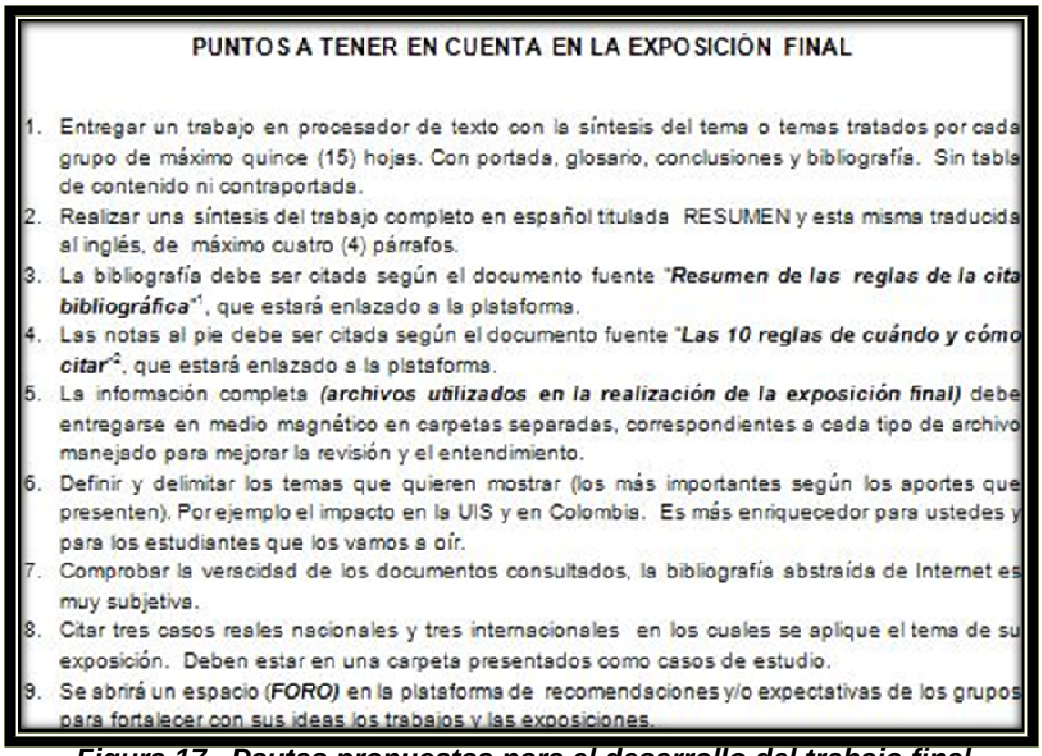
RESULTADOS CUALITATIVOS NOCIONES APRENDIZAJE EN LÍNEA

1. Explícitamente no lo saben, pero lo usan los cursos del SENA y las clases de algunos profesores que usan herramientas Web.
2. Todos están de acuerdo en que el aprendizaje en línea no reemplaza el presencial, sino que son un complemento para su auto aprendizaje.
3. Un porcentaje muy pequeño había aplicado este aprendizaje. El ProSPETIC estandariza, pero sin dejar de lado la investigación.
4. Un buen número de estudiantes creen que las herramientas para el aprendizaje en línea requieren de cierto grado de madurez.
5. Los estudiantes ven en la plataforma Moodle que se puede aprovechar mejor, algunos recursos no se ven reflejados en clase.
6. El profesor pone a disposición sus TICs, algunos foros no son respondidos por el estudiante o por el profesor.
7. Un pequeño grupo de estudiantes opina que el desarrollo de la asignatura mediante el aprendizaje en línea es una alternativa para realizar algunas actividades que presencialmente conllevan más tiempo.
8. La mayoría de estudiantes piensan que es un complemento del presencial pero le falta fuerza para permitir al estudiante interesarse más por su uso.

Falta compromiso por parte de los docentes para aplicar nuevas metodologías pedagógicas apoyadas en TICs y disciplina en los estudiantes en el uso de los recursos que ofrece el SGA. El tiempo en clase no alcanza para terminar los temas, he ahí la importancia del SGA que permite a los estudiantes desarrollar extra clase sus actividades.

Valoración: Las herramientas de mensajería instantánea disminuyen en gran medida la disposición del estudiante en clase. Desearían tener la oportunidad de visitas de expertos a clase.

2.2.1.2.5. Informe Final



PUNTOS A TENER EN CUENTA EN LA EXPOSICIÓN FINAL

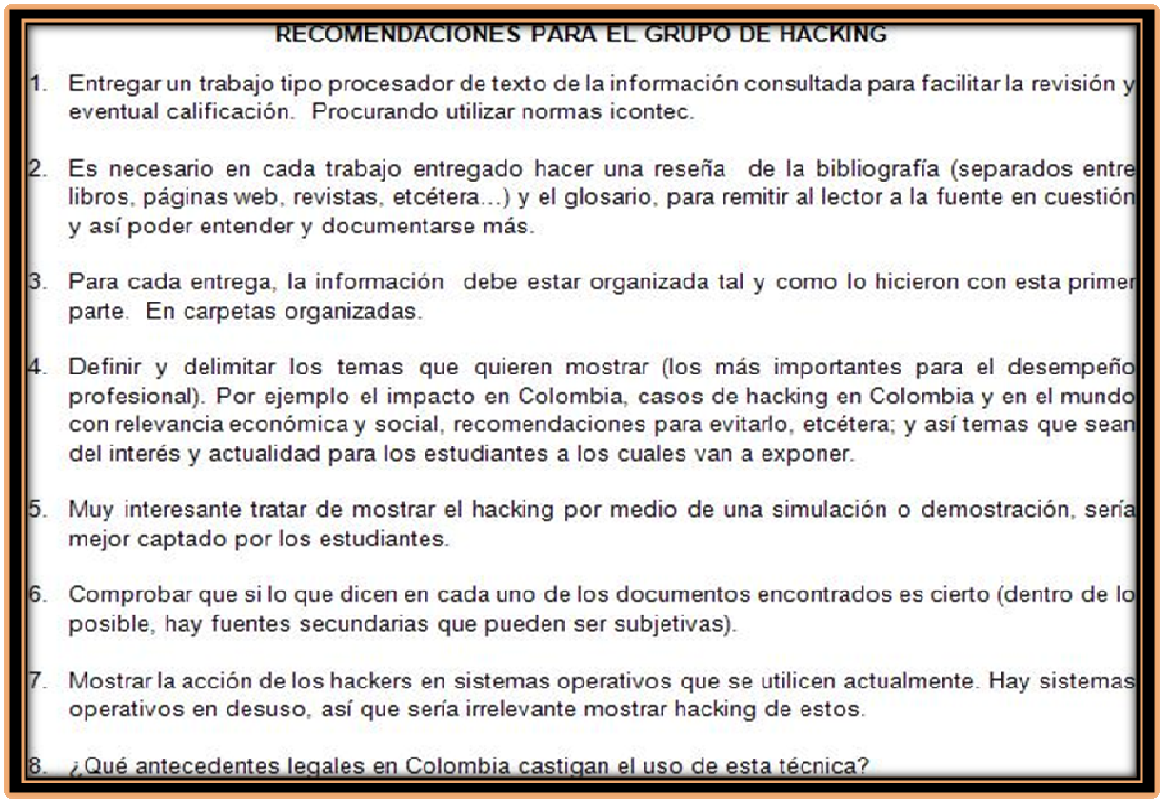
1. Entregar un trabajo en procesador de texto con la síntesis del tema o temas tratados por cada grupo de máximo quince (15) hojas. Con portada, glosario, conclusiones y bibliografía. Sin tabla de contenido ni contraportada.
2. Realizar una síntesis del trabajo completo en español titulada RESUMEN y esta misma traducida al inglés, de máximo cuatro (4) párrafos.
3. La bibliografía debe ser citada según el documento fuente "***Resumen de las reglas de la cita bibliográfica***"[1], que estará enlazado a la plataforma.
4. Las notas al pie debe ser citada según el documento fuente "***Las 10 reglas de cuándo y cómo citar***"[2], que estará enlazado a la plataforma.
5. La información completa ***(archivos utilizados en la realización de la exposición final)*** debe entregarse en medio magnético en carpetas separadas, correspondientes a cada tipo de archivo manejado para mejorar la revisión y el entendimiento.
6. Definir y delimitar los temas que quieren mostrar (los más importantes según los aportes que presenten). Por ejemplo el impacto en la UIS y en Colombia. Es más enriquecedor para ustedes y para los estudiantes que los vamos a oír.
7. Comprobar la versacidad de los documentos consultados, la bibliografía abstraída de Internet es muy subjetiva.
8. Citar tres casos reales nacionales y tres internacionales en los cuales se aplique el tema de su exposición. Deben estar en una carpeta presentados como casos de estudio.
9. Se abrirá un espacio (***FORO***) en la plataforma de recomendaciones y/o expectativas de los grupos para fortalecer con sus ideas los trabajos y las exposiciones.

Figura 17. Pautas propuestas para el desarrollo del trabajo final

2.2.1.2.5.1. Colección de fuentes bibliográficas

Se exigió el envío a través de Moodle de un archivo tipo texto en el cual los estudiantes definieran los tipos de fuentes a utilizar, cómo las clasificaron y de dónde provenían. Para efectos del proyecto se va a hacer el seguimiento al grupo de HACKING. Se presenta un aparte del archivo enviado por este grupo:

“Clasificamos la información por carpetas, los archivos con nombres referentes a su contenido y los links originales en cada página, no fueron editados, solo clasificadas. El material que se va a enviar fue recopilado todo de Internet”.



RECOMENDACIONES PARA EL GRUPO DE HACKING

1. Entregar un trabajo tipo procesador de texto de la información consultada para facilitar la revisión y eventual calificación. Procurando utilizar normas icontec.
2. Es necesario en cada trabajo entregado hacer una reseña de la bibliografía (separados entre libros, páginas web, revistas, etcétera…) y el glosario, para remitir al lector a la fuente en cuestión y así poder entender y documentarse más.
3. Para cada entrega, la información debe estar organizada tal y como lo hicieron con esta primer parte. En carpetas organizadas.
4. Definir y delimitar los temas que quieren mostrar (los más importantes para el desempeño profesional). Por ejemplo el impacto en Colombia, casos de hacking en Colombia y en el mundo con relevancia económica y social, recomendaciones para evitarlo, etcétera; y así temas que sean del interés y actualidad para los estudiantes a los cuales van a exponer.
5. Muy interesante tratar de mostrar el hacking por medio de una simulación o demostración, sería mejor captado por los estudiantes.
6. Comprobar que si lo que dicen en cada uno de los documentos encontrados es cierto (dentro de lo posible, hay fuentes secundarias que pueden ser subjetivas).
7. Mostrar la acción de los hackers en sistemas operativos que se utilicen actualmente. Hay sistemas operativos en desuso, así que sería irrelevante mostrar hacking de estos.
8. ¿Qué antecedentes legales en Colombia castigan el uso de esta técnica?

Figura 18. Recomendaciones al grupo de hacking para desarrollo de informe final

Tras una revisión al envío se hicieron las siguientes observaciones:

Estas recomendaciones fueron puestas como recurso en el SGA y entregadas físicamente a cada uno de los grupos.

2.2.1.2.5.2. Preparación

Se presentaron avances quincenales al tutor para su posterior valoración a través del SGA, tras la consecución de este paso se dio inicio al desarrollo de

la exposición final, se utilizó un wiki[54] para seleccionar las técnicas para la exposición, se propusieron:

TÉCNICAS DE EXPOSICIÓN	
DEMOSTRACIÓN	SIMULACIÓN
PREGUNTA Y/O DIÁLOGO	ILUSTRACIÓN
DEBATE	MAPAS CONCEPTUALES
JUEGO DE ROLES	PRÁCTICA DE LABORATORIO
ESTUDIO DE CASOS	LECTURAS COMENTADAS
FORO	CUESTIONARIOS TIPO ECAES
PHILIPS 6,6	TALLER
MESA REDONDA	

Tabla 11. Técnicas de exposición propuestas a los estudiantes

El grupo de hacking escogió SIMULACIÓN.

2.2.1.2.5.3. Sustentación

Cada grupo subió el archivo a través del SGA y entregó las fuentes utilizadas en un disco compacto al profesor. Se hizo una presentación relacionada con la forma como se hizo el trabajo, exposición oral de 20 minutos al grupo y una auto evaluación grupal. El grupo de HACKING utilizó el virtual PC para probar los daños de un virus, su código fuente y la forma como perpetra.

2.2.2. Colección de Fuentes Bibliográficas del Ambiente

Tiene como objetivo principal seleccionar las fuentes que servirán como soporte a los estudiantes en el desarrollo de los OA y como base bibliográfica de consulta. Actualmente la plataforma no cuenta con Objetos de Contenido clasificados, que le permitan al estudiante agilizar el desarrollo de sus actividades y aprovechamiento de información ya catalogada, se clasificarán en:

2.2.2.1.1. Primarias[55]

- LIBROS[56], PORTAL WEB DE AS y CI, PLAN DE ÁREA DE AS y CI, PORTAL WEB ICFES

[54] Actividad que posibilita la creación colectiva de documentos en un lenguaje simple utilizando un navegador web.
[55] Información sobre la que está basada la presente investigación.
[56] Libros presentes en biblioteca UIS. Ver [25] en bibliografía.

2.2.2.1.2. Secundarias[57]

- TESIS DIGITALES UIS, INVESTIGACIONES ESTUDIANTES I SEMESTRE 2007, DOCUMENTOS DIGITALES DE INTERNET.

2.2.3. Proyectos Interdisciplinarios

2.2.3.1. Estudio de Aplicabilidad

Dado que la universidad se encuentra actualmente desarrollando el ProSPETIC y que el profesor LCGF ha sido testigo del avance del mismo, la terminación con Moodle por el momento no es viable dada la trayectoria de su implementación y que los proyectos relacionados con ProSPETIC y la EISI se encuentran actualmente en la FASE 2-3.

El presente proyecto aplica en las fases de análisis y desarrollo de OA bajo el estándar SCORM y la dirección pedagógica de un experto en el área de conocimiento o UA. Esto significa que dada la interoperabilidad y portabilidad de los OA, permitiría colocarlos en el repositorio que la universidad está diseñando.

2.2.4. Exploración del Diseño Pedagógico de la UA

A través de Moodle se ofrece recursos y actividades propias del SGA como foros, tareas, quiz y wikis. La clase se desarrolla a través de 4 horas semanales en el CENTIC en el horario martes y jueves de 10 a.m. - 12 p.m. Además de un horario extra curricular que el estudiante debe cumplir para realizar las tareas que el profesor sube a la plataforma para realizar posteriormente con un plazo estipulado. También diariamente se están subiendo archivos de temas de interés, así como novedades en el desarrollo de la clase y/o eventos próximos.

Su metodología media a través de análisis de casos de estudio, evaluación a través del envío de archivos respondiendo talleres o tareas. Se generan debates entre los estudiantes relacionados con los temas de la UA para discutir a través de los foros.

2.2.5. Estudio Ambientes de Aprendizaje

2.2.5.1. Arquitectura

[57] Artículos de investigación que sobre el tema se generen.

DISPOSICIÓN ESPACIAL DE UN SALÓN "ACTIVO"

- Provee una comunicación multidireccional y las actividades son grupales o individuales, además de alternativas en actividades formales e informales. Distribución clara de los papales que juegan profesor y estudiante. No hay hegemonía por parte del profesor.

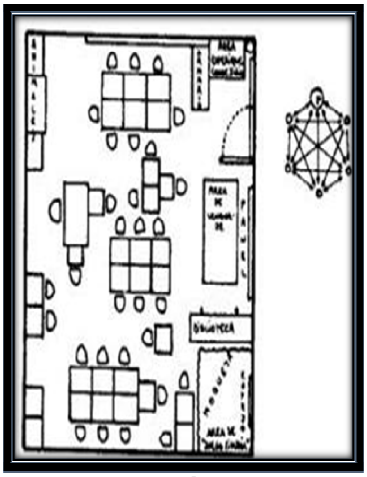


Figura 19 .Distribución espacial multidireccional

"El medio ambiente escolar ha de ser diverso, debiendo trascender la idea de que todo aprendizaje se desarrolla entre las cuarto paredes el aula. Deberán ofrecerse escenarios distintos, -ya sean construidos o naturales- dependiendo de las tareas emprendidas y de los objetivos perseguidos"(Duarte, 2003: 12).

2.2.5.2. Funcionalidades

- Permitir al profesor generar conocimiento usando TIC.
- Enfocar una perspectiva cognitiva en el estudiante.
- Contribuir con el SGA para aprovechar sus recursos.
- Adaptarse al CENTIC para lograr abrir líneas de investigación.
- Contribuir a con la propuesta metodológica al CEDEDUIS.

2.2.5.3. Necesidades

La topología actual del CENTIC según el aprendizaje activo y las competencias cognitivas no permitiría aprovechar en un cien por ciento su capacidad. La presente gráfica muestra una propuesta de distribución que propendería a conseguir estos objetivos. Ésta surgió de entablar discusiones entre el profesor, los estudiantes y el tutor.

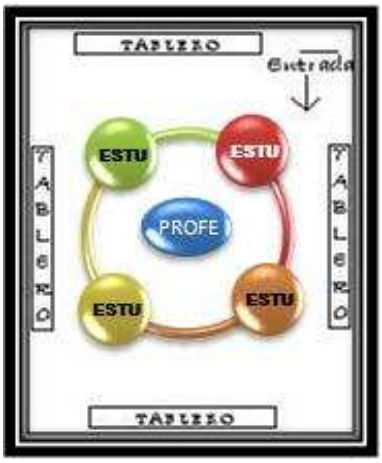
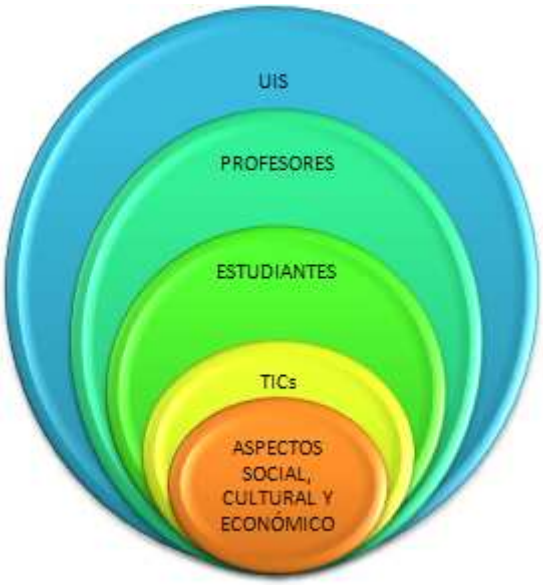


Figura 20. Propuesta de distribución espacial CENTIC

2.2.5.4. Dimensiones



La **UIS** a través del proyecto ProSPETIC, CEDEDUIS y el CENTIC tienden a la conformación de ambientes de aprendizaje, en esta dimensión recae la mayor responsabilidad debido al impacto que puede llegar a tener en los estudiantes y profesores.

Los **profesores** "…deben ser sensibles a las transformaciones sociales e institucionales…", como lo propone (CGCB, 2006: 8), para generar interés de investigación en las áreas que intervienen en un ambiente, como propuestas metodológicas, aplicación de TICs, etcétera.

Figura 21. Dimensiones del ambiente de aprendizaje

En los **estudiantes** diseñando las propuestas o proponiendo otras que converjan al enriquecimiento de UA o repositorios de OA. Por último los **aspectos sociales, culturales y económicos** que afecta a las otras por las características inherentes e inconstantes que presenta, nos permite reconocer las implementaciones que verdaderamente pueden aprovechar los estudiantes y los profesores.

2.2.5.5. Evaluación

Punto importante de un ambiente de aprendizaje pues comprende una serie de lineamientos no solamente cuantitativos sino valorativos encaminados a desarrollar las competencias de los estudiantes en cada OA, actividad y/o metodología a aplicar.

El profesor tendrá la oportunidad de valorar conocimiento[58], desempeño y organización individual o grupal, bajo el complemento de las competencias cognitivas, a través de las actividades desarrolladas, *ver numeral 2.2.7.1. Además de la* autoevaluación y *coevaluación intragrupo*[59] que generan una valoración activa entre estudiantes.

[58] Técnicamente se define como heteroevaluación, basada en la auto y coevaluación.
[59] Evaluación entre los estudiantes en grupos no mayores de cinco integrantes.

2.2.6. Competencias Cognitivas

2.2.6.1. Selección y Clasificación de Competencias

Con la instrucción pedagógica del profesor en el área de conocimiento se presentan las competencias cognitivas que propende la UA:

Generales:

- Describir casos de estudio
- Comprender la importancia de los casos de estudio
- Manejar fuentes de información
- Indagar referencias bibliográficas que apliquen a la UA
- Articular los recursos ofrecidos por el SGA
- Fundamentar en contexto los temas de la UA
- Entender la metodología de mapas conceptuales
- Realizar mapas conceptuales
- Explicar de forma escrita y/u oral los mapas conceptuales
- Hacer síntesis de lecturas complementarias
- Analizar los efectos de los roles dentro del juego
- Identificar los roles correspondientes en el juego
- Generar alternativas subjetivas en los juegos de roles
- Aplicar los conceptos aprendidos al desarrollo de los OA
- Resolver las preguntas TIPO ECAES en el tiempo propuesto
- Trabajar en equipo y en forma autónoma
- Desarrollar trabajo interdisciplinar
- Comunicar en forma oral y escrita a través del SGA
- Inferir conocimiento a través de las diferentes actividades de los OA
- Fomentar escenarios de sustentación grupal
- Organizar espacios de crítica y autocrítica
- Suscitar inquietudes
- Tomar decisiones en contexto
- Diseñar y planificar metodologías instructivas de exposición
- Relacionar la terminología de la UA con los OA
- Deducir información a partir de una simulación

A continuación se presentan las competencias cognitivas específicas a los temas a desarrollar:

FIRMA Y CERTIFICADO DIGITAL[60]				
C [61]	CR [62]	COMPETENCIAS COGNITIVAS		
		INTERPRETATIVA	ARGUMENTATIVA	PROPOSITIVA
a	IS [63]	Recordar las clases de certificados Entender causas de terminación de certificado Identificar certificado digital Comparar clave simétrica y asimétrica Examinar marco legal de firma en otros países Comprender modelo de riesgos ejecución de PKI Reconocer transacciones que aplican firma y certificado Entender la definición de PKI Definir las desventajas de firma y certificado Relacionar las obligaciones de CA, firmante y firmador	Fundamentar las clases de certificados Analizar partes de un certificado digital Definir certificado digital Entender clave pública y clave privada Relacionar marco legal de firma en otros países Sustentar una propuesta de disminución de costos en una empresa aplicando PKI Explicar los campos de aplicación de firma y certificado Describir la estructura de una PKI Analizar las desventajas de firma y certificado Describir obligaciones de la CA, firmante y firmador	Proyectar las clases de certificados Deducir las características de un certificado Representar certificado Evaluar las formas de utilización de las claves Comparar marco legal de firma en otros países Proponer alternativas al modelo de riesgos de aplicación de PKI Evaluar los campos de aplicación de firma y certificado Describir el funcionamiento PKI[64] Sustentar las desventajas de firma y certificado Representar las obligaciones de la CA, firmante y firmador
c	IS, FC	Comprender la definición de firma digital Investigar la ley 527 de 1999 y el decreto 1747 de 2000 Analizar la definición de entidad certificadora[65] Entender el procedimiento para generar un certificado Comprender cómo aplicar PKI en una organización Analizar la función de firma y certificado digital Analizar un contrato de manejo de firmas y certificados Clasificar los dispositivos físicos de almacenamiento de certificados Indagar los impactos en los usuarios de firma y certificado	Clasificar las características de la firma digital Comprender la ley 527 de 1999 y el decreto 1747 de 2000 Reconocer los aspectos básicos de una CA Describir el funcionamiento de un certificado Analizar factibilidad de aplicar PKI en organización Exponer la función de la firma y el certificado digital Identificar las partes relevantes de un contrato de manejo de firmas y certificados Recordar los dispositivos físicos para almacenamiento de certificados Demostrar la importancia de la póliza digital	Explicar la definición de firma digital Explicar la ley 527 de 1999 de Colombia y el decreto 1747 de 2000 Relacionar las funciones de una CA Representar el proceso de autenticación de documentos digitales Plantear estrategias de aplicación de PKI en una organización Sustentar la función de firma y certificado digital Representar un contrato de manejo de firmas y certificados Describir los dispositivos físicos para almacenamiento de certificados Diseñar estrategias de seguridad a posibles ataques a firmas y certificados
d 2	IS	Entender definiciones clave simétrica y asimétrica Comparar firma digital VS manuscrita	Comparar definiciones clave simétrica y asimétrica Describir los beneficios del uso de la firma digital	Definir subjetivamente clave simétrica y asimétrica Sustentar la vigencia de la firma digital

Tabla 12. Competencias cognitivas UA: Firma y Certificado digital

[60] De ahora en adelante firma y certificado
[61] Término definido como Componente
[62] Término definido como Contenido Referencial
[63] Corresponde al área de *Ingeniería Aplicada ó Ingeniería de Sistemas para este caso,* evaluable en el examen ECAES
[64] Abreviatura del término inglés Public Key Infrastructure ó Infraestructura de Clave Pública
[65] Del término inglés Certification Authority ó CA de ahora en adelante

HACKING				
C	CR	COMPETENCIAS COGNITIVAS		
		INTERPRETATIVA	ARGUMENTATIVA	PROPOSITIVA
a	IS	▪ Entender definición de puerta trasera ▪ Comprender los términos hacking y hacker ▪ Reconocer los fallos en seguridad en TI ▪ Definir la Ingeniería Social ▪ Clasificar las TI afectadas en una organización hackeada ▪ Examinar las técnicas descendientes de hacking ▪ Analizar el manejo de contraseñas en usuarios finales ▪ Discutir la legislación colombiana correspondiente a seguridad informática en Colombia ▪ Reconocer transacciones electrónicas comprometidas por hacking ▪ Analizar las implicaciones de hacking en una organización	▪ Reconocer puertas traseras utilizadas por los hackers ▪ Definir hacking y hacker ▪ Describir los errores de diseño de las TI ▪ Observar los modelos de la Ingeniería Social ▪ Representar costos implicados por el hacking en una organización ▪ Diferenciar las técnicas descendientes de hacking ▪ Presentar alternativas de seguridad en las contraseñas ▪ Explicar el impacto de la legislación colombiana en el tema de seguridad informática ▪ Explicar las transacciones vulneradas a través de hacking ▪ Describir las responsabilidades de empleados y organización en los ataques hacking	▪ Formular políticas que mitiguen ataques en las TI ▪ Representar las vulnerabilidades de hacking y hacker ▪ Proponer alternativas en el desarrollo de TI ▪ Clasificar las implicaciones de la Ingeniería Social ▪ Comparar los costos VS beneficios en la implementación de un plan de seguridad informático en una organización ▪ Proyectar solución a las técnicas descendientes hacking ▪ Proponer alternativas de manejo de datos ▪ Evaluar el impacto de las implicaciones legales respecto a la seguridad informática ▪ Evaluar las aplicaciones TI empleadas en las transacciones electrónicas ▪ Definir los deberes proactivos de la organización y los empleados ante ataques hacking
c	IS, FC	▪ Analizar las actitudes de un hacker ▪ Explicar los artículos 195, 199 , 271 y 272 del Código Penal Colombiano ▪ Analizar la definición de hacking ▪ Entender los procedimientos utilizados por hackers	▪ Identificar los perfiles de un hacker ▪ Estimar las implicaciones de los artículos 195, 199 , 271 y 272 del Código Penal Colombiano ▪ Reconocer los aspectos básicos de hacking ▪ Describir los procedimientos utilizados por los hackers	▪ Especificar incongruencias en TI aprovechadas por hackers ▪ Reconocer las falencias de los artículos 195, 199 , 271 y 272 del Código Pena ▪ Relacionar las funciones de hacking ▪ Representar los procedimientos utilizados por los hackers
d2	IS	▪ Analizar la situación actual de las empresas en el área de seguridad informática ▪ Analizar el protocolo TCP/IP ▪ Evaluar el impacto en las TI ▪ Analizar el comportamiento de los empleados en el manejo de las TI de la organización ▪ Relacionar las obligaciones de organización, TI y empleados	▪ Ilustrar las medidas preventivas utilizadas por las empresas colombianas en el área de seguridad ▪ Especificar las posibles deficiencias del TCP/IP ▪ Reconocer las vulnerabilidades de TI ▪ Explicar las políticas utilizadas por las organizaciones para el manejo de las TI de sus empleados ▪ Describir las obligaciones de organización, TI y empleados	▪ Presentar un análisis de requerimientos en el área de seguridad informática en las empresas colombianas ▪ Comparar las alternativas de solución para mejorar el TCP/IP ▪ Presentar estrategias de diseño correctivo en las TI ▪ Diseñar un plan de recomendaciones para el correcto desarrollo de las TI en una organización ▪ Representar las obligaciones de organización, TI y empleados

Tabla 13. Competencias cognitivas UA: Hacking

PHISHING				
C	CR	COMPETENCIAS COGNITIVAS		
		INTERPRETATIVA	ARGUMENTATIVA	PROPOSITIVA
a	IS	Entender la definición de phishing Reproducir las vulnerabilidades de las transacciones en línea Analizar las características que comprometen un sitio web bancario Analizar los procedimientos del usuario final en transacciones bancarias Analizar papel de empleados de entidades bancarias que salvaguardan información privada	Clasificar las características de phishing Clasificar los puntos débiles de las transacciones bancarias en línea Realizar un cuadro comparativo de diferentes sitios web bancarios Comparar las formas de utilización de TI de los usuarios finales Describir funciones de empleados de entidades bancarias que salvaguardan información privada	Plantear un diseño en las web de transacciones bancarias Enumerar soluciones para las transacciones bancarias en línea Formular plan de manejo para usuarios de sitios web bancarios Realizar un informe de controles aplicables en los usuarios finales Diseñar estrategias de reforma en el papel de los empleados que salvaguardan información confidencial
c	IS, FC	Interpretar los modelos de generación de confianza en el usuario para transacciones bancarias en línea Entender a través de los casos de estudio las implicaciones de phishing y sus implicaciones Comprender a través de lecturas comentadas los tipos de técnicas utilizadas en el phishing	Discutir la calidad de modelos de generación de confianza en el usuario para transacciones bancarias en línea Clasificar a través del caso de estudio, las implicaciones del phishing Argumentar a través de lecturas comentadas los tipos de técnicas utilizadas en el phishing	Plantear puntos que permitan mejorar un modelo de generación de confianza en el usuario de transacciones bancarias en línea Discutir a través del caso de estudio las implicaciones del phishing Generar preguntas para resolverlas a través de un foro y discutir en grupo
d 2	IS	Analizar las variables que intervienen dentro del modelo transaccional bancario en línea Examinar la pro actividad educativa de las entidades bancarias a los usuarios en sus servicios en línea Comprender el modelo de expansión de phishing en el usuario Analizar estatutos legales relacionados con el usufructo de información personal Analizar las medidas propuestas por las entidades bancarias para la disminución de phishing	Clasificar las variables que intervienen dentro del modelo transaccional bancario Construir escenarios para analizar la pro actividad educativa de los a los usuarios en sus servicios en línea Generar pautas que permitan evitar la expansión del phishing en el usuario Relacionar los actuales estatutos legales con las técnicas utilizadas para el usufructo a través de información personal Clasificar las propuestas bancarias de disminución de ataques de phishing	Demostrar la validez de las variables que intervienen dentro del modelo transaccional bancario. Reconstruir la pro actividad educativa de los bancos para mejorar sus servicios Evaluar la aplicabilidad de pautas de prevención en el usuario final Proponer alternativas legales para disminuir el usufructo a través de ataques phishing Generar alternativas de solución a las propuestas bancarias de disminución de ataques de phishing

Tabla 14. Competencias cognitivas UA: Phishing

SISTEMAS DE DETECCIÓN DE INTRUSOS				
C	CR	COMPETENCIAS COGNITIVAS		
		INTERPRETATIVA	ARGUMENTATIVA	PROPOSITIVA
a	IS	▪ Definir las características inherentes de los S.D.I ▪ Identificar la arquitectura de un S.D.I ▪ Analizar la topología de un S.D.I ▪ Entender la función de un S.D.I dentro de una organización ▪ Examinar la arquitectura lógica de un S.D.I ▪ Investigar los antecedentes de los S.D.I ▪ Analizar la aplicabilidad de un S.D.I en una organización ▪ Exponer los tipos de respuestas de un S.D.I ▪ Investigar las limitaciones de un S.D.I ▪ Nombrar los tipos de ataques a una red ▪ Definir los problemas de aplicación de los S.D.I en una organización ▪ Identificar las formas de administración de un S.D.I	▪ Clasificar las características de los S.D.I según su función ▪ Agrupar la arquitectura de un S.D.I ▪ Reconstruir la topología de un S.D.I ▪ Explicar si un S.D.I es indispensable en una organización ▪ Definir los elementos de la arquitectura de un S.D.I ▪ Discutir los antecedentes de los S.D.I ▪ Ejemplificar la aplicabilidad de un S.D.I en una organización ▪ Explicar los tipos de respuestas de un S.D.I. ▪ Describir las limitaciones de los S.D.I ▪ Describir los ataques a una red ▪ Categorizar los problemas de aplicación de los S.D.I en una organización ▪ Analizar los efectos de la administración de un S.D.I	▪ Comparar las características con la función que debe cumplir un S.D.I. ▪ Ilustrar la arquitectura de los S.D.I ▪ Justificar la topología de un S.D.I ▪ Ilustrar el futuro funcional de los S.D.I ▪ Comparar diferentes arquitecturas para comprobar su funcionalidad ▪ Identificar los problemas de los S.D.I a través de sus antecedentes ▪ Proponer alternativas para la aplicabilidad de un S.D.I en una organización ▪ Proponer otros tipos de respuestas posibles en un S.D.I ▪ Plantear limitaciones presentadas en los S.D.I ▪ Presentar soluciones a los ataques de una red ▪ Justificar los problemas de aplicación de los S.D.I en una organización ▪ Proyectar aspectos relevantes de los S.D.I que converjan a su correcta administración
c	IS, FC	▪ Analizar la definición de S.D.I ▪ Describir los tipos de S.D.I ▪ Investigar los estándares para S.D.I ▪ Investigar los tipos de detección de los S.D.I ▪ Indagar por el/los S.D.I implementados en la universidad o en universidades del país	▪ Comparar la definición S.D.I a través de varias fuentes ▪ Clasificar los tipos de S.D.I ▪ Indagar si los S.D.I cumplen con el/los estándares internacionales ▪ Explicar subjetivamente los tipos de detección de los S.D.I ▪ Presentar un informe de resultados del S.D.I aplicado en la/las universidad del país	▪ Explicar la definición de S.D.I ▪ Exponer los tipos de S.D.I ▪ Explorar las falencias en los S.D.I, dados los estándares internacionales ▪ Evaluar subjetivamente los tipos de detección de los S.D.I ▪ Evaluar la implementación del S.D.I en la/las universidades del país
d 2	IS	▪ Conocer los S.D.I comerciales y no comerciales ▪ Comprender los requerimientos y responsabilidades corporativas necesarias para desarrollar un proyecto de S.D.I	▪ Valorar los S.D.I comerciales y no comerciales ▪ Indagar proyectos de S.D.I en una organización	▪ Sustentar si las funciones de los S.D.I comerciales y los no comerciales son suficientes ▪ Evaluar proyectos de S.D.I aplicados con una organización

Tabla 15. Competencias cognitivas UA: Phishing

2.2.7. Metodologías de Aprendizaje Activo

2.2.7.1. Actividades complementarias

Actividades que servirán de apoyo a los estudiantes para entender y apoyar los OA de aprendizaje y que servirán como punto de partida para reconocer el verdadero impacto de éstos en los estudiantes, pues es ahí donde radica la importancia en la creación de los OA como son mapas conceptuales, imágenes enriquecidas, etcétera.

2.2.7.1.1. Metodología Philips 6.6

Esta metodología consiste en la conformación de grupos de seis estudiantes para resolver una situación problema en un lapso de seis minutos. Luego de pasado el tiempo se discute entre cada grupo las diferentes perspectivas dadas para llegar a una conclusión.

2.2.7.1.2. Imágenes Enriquecidas

Son herramientas de aprendizaje, pueden ser dibujos, diagramas o gráficos enriquecidos con texto que buscan explicar una situación, problema. Su éxito radica en la percepción humana que se realiza a través de ésta ya que los textos no permiten lograr su nivel de representación.

2.2.7.1.3. Exposiciones

Presentaciones organizadas de un tema de la UA o de un OA como tal, les permitirá a los estudiantes mejorar las competencias argumentativas e interpretativas. Se deja al profesor el desarrollo final de la misma dada las características del grupo o de los temas.

2.2.7.1.4. Mapas conceptuales[66]

Son representaciones gráficas conceptuales relacionadas que forman proposiciones, tiende a unos objetivos, entre los que se destaca: "…refuerzo de los conceptos que han sido vistos en clase o estudiados individualmente", según (Caro, 2003: 4), permite aprovechar las competencias argumentativas, propositivas e interpretativas.

2.2.7.1.5. Debates

[66] Para una mejor referencia diríjase a [26] en bibliografía.

Metodología que permite el desarrollo grupal e individual de las competencias argumentativas e interpretativas con actividades como comunicación oral y trabajo en equipo. El estudiante debe apropiar una información ya descrita para refutarla según sus capacidades.

2.2.7.1.6. Foros

Discusión grupal sobre un tema soportado en el SGA donde cada estudiante da su punto de vista para generar un debate final conversacional. La participación por parte del estudiante en este tipo de actividades es fundamental, es por esto que es necesario darle un carácter valorativo por parte del profesor para generar interés.

2.2.8. Ficha Temática

Parte importante del presente proyecto pues presenta los objetivos, las competencias a evaluar, la duración y las fuentes bibliográficas de la actividad propuesta para el OA, ver ANEXO B para la plantilla y el numeral 3.1.2 para su implementación en el diseño de los O.A. Servirá como guía al estudiante en el desarrollo de los OA.

2.2.9. Análisis SGA Moodle

Es una herramienta que permite al profesor actualmente administrar cualitativa y cuantitativamente un ambiente de aprendizaje en línea para la materia de Seguridad Informática y al estudiante acceder y desarrollar recursos.

En su actual proceso de reestructuración la materia no cuenta con una infraestructura curricular que permita al profesor disponer de los temas de forma ordenada y clara en la UA. El presente proyecto aboca una oportunidad para enriquecerla mediante la implementación de OA que aprovechen la interacción profesor - estudiante. La implementación del SGA Moodle acarrea los siguientes costos para el grupo STI:

- **FECHA DE INICIO DE LA PLATAFORMA:** 2001
- **SERVIDOR** = 350.000 al año
- **ADMINISTRACIÓN=** 150.000/mes, Ingeniero Ernesto Galvis Amarú

CAPÍTULO III

3. OBJETOS DE ARENDIZAJE TEMÁTICOS
3.1. ETAPA DE GENERACIÓN
3.1.1. Análisis

3.1.1.1.1. Caso de estudio

Metodología (Parikh, 2002)[67] de investigación cualitativa que permite a través de las actividades complementarias, *ver numeral 2.2.7*, presentar una situación en contexto, en cuatro etapas (Ortiz, 2005):

1. Organización del tema
2. Recolección de datos
3. Análisis de datos
4. Redacción del caso de estudio

3.1.1.1.2. Juego de roles

Metodología que le permite interpretar y desarrollar un rol individual o grupal al estudiante, el cual desempeña un perfil sustentado en las actividades complementarias, *ver numeral 2.2.7,* para reforzar sus competencias cognitivas. El rol de cada integrante puede ser desarrollado de forma subjetiva. Esta metodología permite desarrollar el trabajo equipo pues su objetivo es el de colaborar más no competir.

3.1.1.1.3. Cuestionario tipo ECAES

A partir del Marco de Fundamentación Conceptual y Especificaciones de Prueba para los programas de Ingeniería de Sistemas del país (ACOFI, 2005: 5), se diseñarán preguntas relacionadas con la UA para evaluar sus competencias cognitivas: Definición pruebas ECAES:

> *"pruebas académicas de carácter oficial y obligatorio y forman parte, con otros procesos y acciones, de un conjunto de instrumentos que el Gobierno Nacional dispone para evaluar la calidad del servicio público educativo" y, dentro de ese marco, las pruebas deben "comprobar el grado de desarrollo de las competencias de los estudiantes que cursan el último año de los programas académicos de pregrado que ofrecen las instituciones de educación superior".*

[67] Documento original de la cita.

3.1.1.1.4. Simulación

Es el proceso de diseñar un ambiente real para realizar experiencias a través de medios digitales, comprender sus relaciones, o evaluar nuevas estrategias dentro de los límites impuestos por el conjunto de características que lo componen. Se conllevan actividades de discusión para lograr conclusiones y realimentación de la misma.

Se realiza un análisis preliminar del sistema a simular para determinar las limitantes, variables y los resultados que se esperan. Luego surge la comprobación del modelo y posteriormente la interpretación para su ulterior realimentación.

3.1.2. Diseño

La UA hace parte del contenido curricular de la materia Seguridad Informática la cual se dicta en las cuatro últimas semanas del semestre. Cada tema está vinculado a una semana de trabajo presencial académico de 4 horas, las cuales son divididas en sesiones de 2 horas más 16 horas no presenciales. En base a esto se diseña la ficha temática para presentar los objetivos, enunciado, competencias cognitivas, bibliografía, duración y las actividades complementarias para el desarrollo de los OA. Se elaboró un ejemplo ilustrativo de la ficha temática. Además de un demo para explicar los componentes de la misma que estará disponible en el SGA. ***Ver Anexo B.***

Se utilizarán los recursos ofrecidos por Moodle para que el profesor LCGF de la valoración respectiva a los OA.

3.1.2.1.1. Caso de estudio

Se diseñó el siguiente caso de estudio para dar a conocer el tema de Firma y Certificado Digital, en relación a los riesgos y los controles que existen y debe tener en cuenta una organización, además de los beneficios que inciden al aplicar esta tecnología.

ORGANIZACIÓN DEDICADA A LOS SERVICIOS DE INVERSIÓN, FIDEICOMISO[68] Y FONDOS MUTUOS

[68] Es un contrato por el cual una persona destina ciertos bienes a un fin lícito determinado, encomendando la realización de ese fin a una institución fiduciaria.

El Analista de Aplicaciones Informáticas presenta una propuesta al Comité de Tecnologías de Información del Departamento Informático con intermediación de una CA (Autoridad de Certificación) reconocida y segura, para aplicar PKI (*Public Key Infraestructure*) en la organización con el fin de disminuir costos, mejorar sus servicios electrónicos y vincular más usuarios. Actualmente cuenta con tres mil asesores que se conectan a la intranet de la organización para revisar la información personal y financiera del cliente. El Analista considera las siguientes características de la organización:

- Directrices del negocio
- Migración de aplicaciones a PKI
- Instalación, operación e impacto para los asesores y el usuario final

La CA ofrece póliza de seguros, respaldo de asistencia por seis meses del grupo aplicativo PKI. Lo anterior avalado por una RA (Autoridad Registradora)[69]. Además, las subsiguientes oportunidades de negocio:

- Confirmación de la integridad y calidad de la información enviada y recibida.
- Seguridad en el tiempo de la información.
- Confirmación de la privacidad de la información.
- Aumento en el valor agregado de los bienes y servicios de la organización.
- Minimización de costos de búsqueda de nuevos clientes.
- Aumento de la capacidad de respuesta.
- Aumento de seguridad de la plataforma tecnológica.
- Mejorara en la productividad pues se disminuye el tiempo transaccional.
- Reducción en costos **p**apel, im**p**resión, correo **p**ostal.
- Implementación bajo las disposiciones gubernamentales[70].

Explicación de la CA al gerente de la organización:

Esta metodología aplica la criptografía de clave pública que usa un par de claves encriptadas para verificar la identidad del emisor (quien firma) y el receptor (quien verifica la firma) para asegurar la privacidad (encripción).

Componentes importantes de la PKI:

[69] Entidad Certificadora raíz, casi siempre perteneciente a la rama estatal. Certificadora de sí misma.
[70] Algunos países exigen a las organizaciones presentaciones de registros electrónicos.

Autoridades de Certificación (CA o Certification Authorities): Vinculan la clave pública a la entidad registrada para su identificación. Una CA es a su vez identificada por otra CA creándose una jerarquía de confianza.

Autoridades Registradores (RA o Registration Authoritites): Ligan entes registrados a figuras jurídicas, extendiendo la accesibilidad de las CA.

Autoridades de Fechado Digital (TSA o Time Stamping Authorities): Vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en ese instante (resolverían el problema de la exactitud temporal de los documentos electrónicos).

Los Repositorios: Estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el de listas de revocación de certificados.

Los Usuarios Y Entidades Finales: Poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones (validar firmar digitales, cifrar documentos, etcétera.)

Pregunta el gerente a la CA:

- ¿De dónde saldrán los recursos para la aplicación de PKI?
- ¿Cómo se determinará la efectividad de costos de PKI?
- ¿Cómo se probará la PKI sin afectar el negocio?
- ¿Se tienen en cuenta los costos de consultoría?

Explicación de la CA al gerente de la organización acerca de PKI:

Analicemos las aplicaciones más afectadas con la aplicación de PKI:

- Correo electrónico seguro
- Transacciones electrónicas seguras
- Archivos firmados electrónicamente
- Firma única

Definición entregada por el analista al gerente:

ARQUITECTURA BÁSICA

Una Infraestructura de Clave Pública (Public Key Infrastructure en inglés) es la combinación de productos de hardware y software, políticas y procedimientos para proveer un nivel adecuado de seguridad en transacciones electrónicas a través de redes públicas, como Internet.

Se basa en identificaciones digitales conocidas como “certificados digitales”, los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública. Debido a la característica impersonal involucrada en este tipo de tecnología – sin intercambio de documentos físicos– es que se hace necesario contar con medios que garanticen una efectiva identificación y autenticación. Generalmente una estructura de PKI consiste en:

• Una política de seguridad
• Una Autoridad Certificante
• Un sistema de administración de certificados
• Un conjunto de aplicaciones que hacen uso de la tecnología PKI

Los certificados, según sus comprobaciones, se dividen en cuatro:

a) Clase 1: Corresponde a los certificados más fáciles de obtener y verifican solamente el nombre y la dirección de correo electrónico del titular.

b) Clase 2: La Autoridad Certificadora comprueba además el permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.

c) Clase 3: Se comprueba la Clase 2 y además el crédito de la persona o empresa mediante un servicio.

d) Clase 4: Son todas las comprobaciones anteriores con la verificación del cargo o la posición de una persona dentro de una organización.

Según la finalidad, los certificados electrónicos se dividen en:

a) SSL para cliente: Usados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, se expiden normalmente a un particular o asesor de empresa.

b) SSL para servidor: Usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden a la empresa propietaria del servidor. La presencia de éste certificado es imprescindible para establecer comunicaciones seguras.

c) S/MIME: Usados en servicios de correo firmado y cifrado, se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, proporcionando Autenticación, Integridad y No Rechazo.

d) De firma de objetos: Usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje que se deba ejecutar en red.

e) Para AC: Identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado.

PKI puede ser soportado en un solo servidor o en servidores por separado. Aplicaciones de código abierto para gestión de PKI:

- Microsoft Windows 2000 Certificate Services, OpenCA, SunONE Certificate Server

La arquitectura PKI tendrá que ajustarse a la infraestructura existente en la organización, como por ejemplo la ubicación de los servidores PKI, las aplicaciones con las que contará la PKI y los centros de aplicación de usuarios. Se propone una CA subsidiaria para que la CA raíz o RA (Registration Authorities) quede fuera de línea. A mayor CA subsidiarias mayor costo de operación de PKI. Partes de un certificado digital:

- Número de serie del Certificado emitido por la Autoridad Certificadora
- Algoritmo usado por la Autoridad Certificadora que valida el Certificado
- Nombre de la autoridad generadora del Certificado
- Validez del Certificado
- Nombre del Propietario del Certificado
- Clave pública del Propietario y Algoritmo usado
- Extensiones Usadas
- Firma Digital de la Autoridad Certificadora
- Algoritmo de Firma Digital que fue usado por la Autoridad Certificadora

¿Qué seguridad me ofrece la PKI? Pregunta el gerente a CA

- El Sistema Gestor de Certificados digitales cuenta con control de acceso.
- Ubicación del equipo informático sobre el que trabajará la CA
- Autenticación al administrador para emisión de certificados
- Tipos de documentos a firmar
- Almacenamiento y backups de los documentos firmados
- Integración a las aplicaciones existentes a la PKI
- Posibilidad de leer el contenido antes de ser firmado
- Sobre con el manual de usuario y nombre de usuario con su respectiva contraseña para identificarse antes de firmar, entregado personalmente
- Comprobación de solicitudes, pueden hacer solicitudes falsas

Recomendaciones para el uso de PKI, según la CA

COMPROMISO DE CLAVE PRIVADA DE USUARIO: Cuando la clave privada sea comprometida, ya sea por robo o pérdida, el certificado digital deberá ser revocado para evitar el mal uso de la clave.

COMPROMISO DE CLAVE PRIVADA DE AGENCIA CERTIFICADORA: Si la clave privada de la Autoridad Certificadora es comprometida, todos los certificados validados y generados por esa agencia certificadora serán revocados.

EXPIRACIÓN DEL CERTIFICAD: Un certificado siempre tiene un tiempo de vida finito o fecha de vencimiento.

ALMACENAMIENTO DE CERTIFICADO: TOKEN, elemento físico, como por

Figura 22. Dispositivo TOKEN

ejemplo una tarjeta inteligente en el que se incorpora, la clave privada del suscriptor y el certificado digital correspondiente a la misma. Cada certificado podrá tener un soporte físico distinto, según especifique CA.

El TOKEN tiene un Nivel de Seguridad *ALTO*, portando la llave el usuario. Es un dispositivo *USB* que asegura compatibilidad (Plug and Play) con los computadores de escritorio y portátiles. No necesita periféricos adicionales.

ADMINISTRACIÓN DEL CERTIFICADO

a) El Certificado digital es personal e intransferible
b) Memorice su PIN (Personal Identification Number) y destruya el sobreflex
c) No permita que otras personas conozcan el PIN o clave
d) Conserve el dispositivo TOKEN siempre en su poder.
e) No emplee el dispositivo para almacenar datos u otros fines.
f) Si extravía su dispositivo solicite la revocación del certificado
g) El PIN almacenado en el TOKEN únicamente puede ser cambiado por el suscriptor del certificado. CA no almacena ni asigna los PIN.

OTRAS RECOMENDACIONES ORGANIZACIONALES:

- Ubicar los equipos informáticos en salas con acceso restringido
- Filtrar los puertos con firewalls y fortalecerlos con S.D.I
- Revisar los archivos de logs periódicamente
- Entender el valor jurídico de la PKI y por ende de la firma digital

¿Cómo firmo un documentos digital?, pregunta el gerente a la CA.

1. El administrador de la PKI entrega en las manos del usuario un sobre con las credenciales digitales (identificación y contraseña, TOKEN).

2. Tras una conexión segura a través de Internet el usuario ingresa a la interfaz de la CA, para revisar los documentos pendientes a firmar.

3. La interfaz revisa en la base de datos el/los documentos pendientes para descargarlos en formato PDF y así enviarlos al receptor del documento.

4. Se envía un mensaje de correo electrónico al receptor para que este confirme la identidad del emisor del documento.

5. Se responde mediante un acuse de recibo cifrado y firmado

Funciones de la CA, según la misma CA. Explicadas al gerente:

***** *Admisión de solicitudes*. El usuario completa un formulario y lo envía a la autoridad de certificación solicitando un certificado.

* *Autentificación del usuario*. Verificar la identidad del requirente antes de firmar la información proporcionada por él mismo.

* *Generación de certificados*. Recibida la solicitud y validados los datos, generamos el certificado correspondiente para firmar con su clave privada.

* *Emisión de los certificados* de usuarios registrados y validados por RA.

* *Revocación de los certificados* que ya no sean válidos (Se genera una CRL - lista de certificados revocados).

* *Renovación de certificados.*

* *Salvaguardar los certificados* en el repositorio de certificados.

Propuesta del Analista: Estudio de la NORMA TÉCNICA ISO/IEC 17799:2000, para analizar lo dicho por la CA.

SEGURIDAD EN APLICACIONES DEL SISTEMA

OBJETIVO: Evitar la pérdida, modificación o uso inadecuado de datos de los usuarios en los sistemas de aplicación.

1. *Autenticación de mensajes*: Se debería establecer la autenticación de mensajes para aplicaciones en las que hay información por proteger, por ejemplo, transferencia electrónica de fondos, contratos, etcétera.

2. *Validación de los datos de salida*: Se debería validar los datos de salida de un sistema de aplicación para garantizar el procesamiento.

CONTROLES CRIPTOGRÁFICOS

OBJETIVO: Proteger la confidencialidad, autenticidad de la información.

El Analista opina que la PKI se rige a la norma ISO/IEC 17799:2000.

Impacto en el usuario y en TI, según el Analista:

EN EL USUARIO
- Inscripción para expedición de un certificado
- Ubicación geográfica de los usuarios móviles para capacitación
- Configuración cliente de correo electrónico para certificados digitales
- ¿Cuántos usuarios deben recibir certificados? Entre internos y externos

SOPORTE Y ADMINISTRACIÓN DE LA CA
Estará a cargo de un grupo interdisciplinario dirigido por el Analista de Aplicaciones Informáticas el cual la CA capacitará para:

- Inscripción inicial del usuario para la obtención del certificado digital
- Aprobación del certificado
- Administración de vida de certificado, revocación, renovación y reemplazo
- Capacitación íntegra al grupo interdisciplinario de la organización

EN LA INFRAESTRUCTURA TECNOLÓGICA
- Servidor de la CA físicamente asegurado
- Los mensajes firmados digitalmente utilizan más recursos
- Abrir puertos estrictamente necesarios para la aplicación PKI.
- Upgrades de seguridad

COSTOS

- Ahorro de costos, evitación de costos, eficiencia, efectividad del negocio.

CUMPLIMIENTO

- Oportunidades de negocio abiertas por la implantación de PKI.
- Por regulación gubernamental, mayor participación de nuevos socios.

RIESGOS

- Identificación de la información valiosa para la organización.
- Pérdidas de productividad, pérdida indirecta, implicaciones legales.

CUESTIONARIO PARA LOS ESTUDIANTES

1. ¿Es necesario conocer el negocio para entender la aplicación de PKI?
2. ¿Qué beneficios le trae la aplicación de una PKI a la organización?
3. ¿Qué desventajas para el negocio, trae la aplicación de la PKI?
4. ¿La incorporación de PKI se debe acondicionar a las aplicaciones con las que cuente la organización o sobre una nueva aplicación? ¿Lo anterior se debe basar en costos o en actualización de T.I?
5. ¿Qué aplicaciones de la organización usarían PKI?
6. ¿Se debe aplicar una PKI comercial o código abierto?
7. ¿Qué dispositivo físico, de los existentes actualmente en el mercado, permitiría de forma segura almacenar las claves de los usuarios?
8. ¿Qué puertos seguros se deben habilitar para las comunicaciones?
9. ¿Qué especificaciones técnicas debe tener el servidor de la PKI?
10. ¿Cuáles son las funciones de los componentes de una PKI?
11. ¿Cómo proteger una clave privada?
12. ¿Qué clases de certificados existen?
13. ¿Beneficios firma holográfica VS digital?
14. ¿Beneficios documento impreso VS digital?
15. ¿Hay implementaciones de PKI en Colombia?
16. ¿La CA aplica el decreto 1747 de 2000?
17. ¿Se han aplicado los controles necesarios mínimos exigidos por la NORMA ISO/IEC 17799 para la aplicación de la PKI?
18. ¿Se interrumpe la continuidad del negocio con la aplicación de PKI?
19. ¿Qué alternativas de capacitación debe adoptar la CA en el usuario?
20. ¿Qué presupuesto permitirá a la empresa implantar una PKI?
21. ¿Qué personal será necesario para la aplicación de la PKI?
22. ¿Qué plan de contingencia se puede aplicar ante fallo en la PKI?
23. ¿Estado de la organización antes y después de la aplicación de PKI?
24. ¿Es necesaria una VPN (Red Privada Virtual)?

25. ¿Qué costos se evita la organización al aplicar PKI?
26. ¿Qué áreas del derecho informático intervienen en implantar una PKI?
27. ¿Qué principios de protección de datos se comprometen sin la PKI?
28. ¿Qué tipos de fraudes se pueden presentar al implantar una PKI?
29. ¿Qué niveles de riesgo no fueron tenidos en cuenta al aplicar la PKI?
30. ¿En Colombia existen CA?

Análisis del caso de estudio en grupo, conformación del grupo a través de un WIKI. Cada grupo debe analizar y posteriormente desarrollar el caso de estudio, respondiendo las preguntas propuestas para el mismo, se deben identificar las características fundamentales del caso de estudio.

La primera etapa se desarrolla en dos (2) horas de clase, deben documentarse a través de las fuentes bibliográficas dispuestas en el ambiente, para sustentar en las otras 2 horas de clase. Se apoyará la realización del caso de estudio a través una actividad tipo FORO, para que los estudiantes manifiesten sus interrogantes y los puedan resolver entre sí, antes de la sustentación.

Deben representar a través de un mapa conceptual la estructura del caso de estudio y de todos sus componentes, así como la solución a las preguntas, según las concepciones del grupo.

En la segunda etapa deben exponer verbalmente el Mapa Conceptual generado por cada grupo. Se generará un archivo por grupo según las especificaciones del profesor, en el cual se reportarán la experiencia, el Mapa Conceptual y la forma como lo desarrollo el grupo. Será subido a través de un recurso de la plataforma para la revisión y valoración del profesor.

3.1.2.1.2. Juego de roles

Se diseñó el siguiente juego de roles para dar a conocer el tema de Hacking al estudiante, en relación a los riesgos que pueden existir en una empresa cuando no se aplican políticas de seguridad informática acordes que permitan una adecuada seguridad en el uso de sus TI, además de los controles a tener en cuenta para no interrumpir la continuidad del negocio. El juego se va a desarrollar a través de los siguientes roles:

- ***Asesor:*** Asesor Comercial del área de afiliación
- ***Administrador***: Encargado del área de TI de la compañía
- ***Gerente:*** Encargado de decidir si hace o no inversión en TI

- ***Auditor Informático***: Contratado para ver el estado de la compañía.
- ***Comandante de la DIJIN***: Especialista en normatividad jurídica de Seguridad Informática del país.

ENTREVISTA HACKEADA

Reunión de los cinco jugadores para entender el porqué el asesor ingresó sin permiso alguno, a los archivos digitales personales de los clientes de la compañía y adulteró algunos de ellos para beneficio personal.

Cada estudiante debe proponer las responsabilidades del asesor dentro de la compañía según las referencias dadas. Así como sus funciones específicas de acuerdo a las TI disponibles para desarrollar su trabajo.

AUDITOR: Se dice que el término Hacker surgió de los programadores del MIT, durante los años setenta y ochenta. El término hacker viene del verbo to hack (cortar, golpear). Con el tiempo, la palabra hacía referencia a quienes invertían todo su tiempo probando nuevas posibilidades de la recién nacida informática. Los Hackers son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones.

El hacking simplemente nació como un estado de diversión y durante muchos años a revestido diversos significados. Todos los comentarios acerca de hacking han resultado siempre acusadores y negativos. En realidad, los hackers han sido fundamentales en el desarrollo de Internet. Fueron hackers académicos quienes diseñaron los protocolos de Internet.

“Lo común es que las personas se inicien en el hacking por simple curiosidad. Por lo general, esta inquietud los lleva a probar la efectividad de ciertas herramientas para ingresar o escalar privilegios en un sistema”.

ADMINISTRADOR: La penetración de Internet en los hogares hace que el acceso a herramientas, manuales y guías relacionados con hacking estén al alcance de las manos. Esto, impulsado por la manera en que se relacionan muchas personas hoy (especialmente los jóvenes), mediante chats y otros mecanismos tecnológicos, incrementa la curiosidad.

La curiosidad no es la única razón para hacer hacking, hasta los líos románticos se convierten en una causa. “Las situaciones de infidelidad o celos impulsan al ofendido a penetrar en cuentas de correo o archivos privados”, la búsqueda de información con fines de lucro y fines terroristas.

GERENTE: ¿Qué lo llevó a tomar dicha determinación?

ASESOR: Actualmente me siento inconforme con mi remuneración.
ASESOR: ¿Cuáles son las responsabilidades del administrador de la TI?
ADMINISTRADOR: Salí un momento a realizar una consulta.
AUDITOR: Las cifras se disparan

En abril del 2006, se alertó que el uso de malware creció más del 600 por ciento en el mundo y el número de root kit aumentó un 700 por ciento. Cada día hay herramientas sofisticadas, requieren niveles bajos de conocimiento de tecnología, disponibles para cualquier persona con Internet.

COMANDANTE: Preliminar a la legislación colombiana:

La gravedad del hacking radica en que por curiosidad se puede terminar en la cárcel. Las consecuencias son proporcionales a la magnitud del daño causado y la legislación sobre el uso de medios electrónicos. Las mayores penas pueden ser de 10 años hasta prohibición del uso de Internet por un tiempo determinado. Y a nivel mundial, hay un esfuerzo por avanzar en la penalización de estas acciones.

No hay riesgo de castigo mientras no se cause daño sobre la información. Tampoco hay penalización si la acción fue hecha durante un ejercicio de la organización afectada. Esto es lo que se pretende mediante los ejercicios de hacking ético para probar niveles de seguridad y exposición en compañías.

En Colombia, el hacking no está tipificado como delito. La razón es que para la justicia del país, si una empresa pone un servidor web en Internet quiere decir que acepta que el público acceda a su información. Si un usuario encuentra el puerto abierto y analiza no está llevando a cabo ningún delito.

La actual legislación colombiana contempla algunas de estas conductas en los siguientes tipos penales: Acceso abusivo a un sistema informático (art. 195), Sabotaje (art. 199), Violación a los Derechos de Autor (art. 271 y 272).

ADMINISTRADOR: El hacking es un atentado contra la integridad, disponibilidad y confidencialidad de los recursos de las empresas y activos intangibles. El principal reto es proteger y certificar la seguridad de estos recursos. Motivo por el cual la compañía debe dedicar más recursos a la inversión en tecnología para neutralizar los efectos de los ataques a su información.

GERENTE: Las empresas gastan mucho dinero en tecnologías para proteger sus redes de computadores. Invierten en firewalls, antivirus, dispositivos de

autenticación, software de encriptación. Pero la principal vulnerabilidad podría ser nuestra propia gente. Los controles deben ir más allá de implementar infraestructura tecnológica, es necesario políticas, procedimientos y educación a nuestros asesores.

COMANDANTE: En el país los casos más comunes de accesos abusivos a los sistemas de información han sido ocasionados por los descuidos de los administradores de sistemas; sistemas desactualizados, falta de educación del usuario final, bajo nivel de seguridad en las claves y asignación de privilegios muy altos. Mientras las leyes colombianas no agraven las penas por estos delitos y las personas no tomen conciencia, los índices se sostendrán.

ASESOR: Su explicación se reduce a que un día vio la clave de acceso al servidor, asegura él que el administrador dejó sin llave el cuarto de equipos informáticos y que contaba con un listado de contraseñas a la vista.

Luego de fotocopiar la lista de claves de acceso y de dejar la hoja nuevamente en su sitio, el asesor sin conocimientos en informática descargó información de Internet relacionada con el tema de hacking para adulterar los datos de usuarios para obtener mayores bonificaciones.

ADMINISTRADOR: ¿Ha omitido algún detalle?
ASESOR: Ninguno.

AUDITOR: Propuesta de hacking ético

En este caso, una empresa puede contratar a expertos en tecnología para que traten de vulnerar sus sistemas, tal como lo haría un hacker. De esa forma, se pueden identificar los riesgos de su infraestructura tecnológica.

Cuando la empresa decide contratar un Estudio de Seguridad usualmente centra sus intereses en conseguir de su contratista la definición de los puntos vulnerables de sus redes y la solución a las vulnerabilidades encontradas en el software y en el hardware que utiliza en sus sistemas. En muchos casos ni siquiera se preguntan por el nivel de profundidad de la prueba, la correcta redacción del contrato, la definición de la política de seguridad, etcétera.

Así que lo que se encuentra en el mercado es una cantidad considerable de empresas que han invertido sumas cuantiosas en la compra de programas de software que desarrollan funciones de seguridad muy específicas (antivirus, firewalls, SDI y otros).

COMANDANTE: Política de Seguridad

Esto pasa y pasará siempre que las empresas no hayan definido clara e integralmente sus Políticas de Seguridad de Información, incluyendo controles de acceso, compra de hardware, compra de software, desarrollo *in house* de software, contratación de terceros, contratación de asesores, disposición arquitectónica de las oficinas, disposición de basuras, administración de claves, procedimientos de cifrado y otros.

Al definirla la empresa sabrá, con un nivel de precisión aceptable, qué puede, qué no puede, qué debe, que no debe, que conviene y que no conviene que sea hecho por los asesores. Sabrá qué cargos pueden usar programas de mensajería instantánea, a qué horas y en qué días debe incrementarse el tráfico de red por determinados puertos. Ese detalle debe traducirse a un lenguaje legal que permita a la empresa definir consecuencias concretas para los Incidentes de Seguridad.

En Colombia, la Información, no es considerada un bien jurídico que por sí mismo merezca la protección del estado y, porque las conductas que constituyen los incidentes de seguridad no han sido tipificadas como delitos. La falta de conocimiento e interés acerca de la Seguridad de la Información tanto del sector privado como del Congreso, se traduce en el evidente atraso de la legislación penal. Los mismos ingenieros de sistemas deben buscar que al interior de sus organizaciones sea conocido que la responsabilidad por el manejo seguro de la información compete a todo el personal, no exclusivamente a ellos. Es necesario iniciar una labor de concientización que, a través de la judicialización masiva de casos, brinde seguridad jurídica.

El desarrollo de una política de seguridad comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo y tecnologías disponibles para hacer frente a los riesgos. Debe crearse un procedimiento de auditoria de forma periódica. A continuación los desglosa y explica (los estudiantes deben explicar las siguientes políticas):

- *Identificación de los activos organizativos*
- *Valoración del riesgo*
- *Definición de una política de uso aceptable*

AUDITOR: Auditor versus delitos informáticos

✓ Actividades propias del auditor:

- Determina si se considera la situación un delito realmente

- Establece pruebas claras y precisas
- Determina los vacíos de seguridad existentes
- Informa a la autoridad correspondiente dentro de la organización
- Informa a autoridades regulatorias cuando es un requerimiento legal
- Maneja con discreción la situación y con el mayor profesionalismo posible

✓ Si no se maneja adecuadamente el delito, podría tener efectos negativos en la organización:

- Desconfianza de los asesores hacia el sistema
- Genera más delitos al mostrar las debilidades encontradas
- Pérdida de confianza de los clientes, proveedores e inversionistas
- Pierde asesores clave de la administración

✓ Resultados de la auditoria

- Revisión total del proceso involucrado
- Inclusión de controles adicionales
- Establecimiento de planes de contingencia efectivos
- Adquisición de herramientas de control

COMANDANTE: Comandante versus delitos informáticos

El auditor informático además deberá ayudar a la empresa en el establecimiento de estrategias contra la ocurrencia de delitos:

- Estándares para la auditoría interna
- Políticas organizacionales sobre la información y las TI
- Características de la organización, compensaciones a los asesores, extensión de la presión laboral, cambios recientes en la administración
- Verificación de desviaciones en el comportamiento de los datos

GERENTE: Gerente versus delitos informáticos

- Recuperación de desastres y continuidad de negocio
- Programas de concientización de usuarios
- Respaldos de datos
- Diseño e implementación de estrategias de seguridad informática
- Monitoreo de las actividades de los asesores

ASESOR: Asesor versus delitos informáticos

Los estudiantes deben explicarlas.

PREGUNTAS DEL AUDITOR AL ADMINISTRADOR:

1. ¿Qué tipo de red que se maneja en la compañía?
Red tipo estrella en donde todas las subredes de los diferentes edificios están conectados a un switch principal capa nivel 2 (enlace de datos) y enrutadores CISCO 3845 por medio de fibra óptica, en el manejo del trafico de información éstas se aíslan de las demás subredes por medio de diferentes pilas switch VILAN; en la seguridad tienen firewall CISCO ASA 5520 configurado cuidadosamente para que no se presente ningún tipo de inconveniente en el manejo de Internet que viene contratado con Telecom quien proporciona enlace de +- 32 Mbps, además cuentan con software WEBSENCE que controla accesos a paginas clasificándolas para boqueo.

2. ¿Cuántos equipos y que S.O maneja el router de la compañía?
Aproximadamente se tienen 3500 computadores y servidores con sistemas operativos Windows XP 2000, Linux Red Hat, Sun, Fedora.

3. ¿Que clase de permisos hay?
Permisos individuales dados por el administrador por pequeños periodos de tiempo y solamente el recurso que va usar de la red.

4. ¿Existen Listas Control de Acceso?
No existen listas de acceso desde Internet.

5. ¿Que controles tienen para evitar los intrusos informáticos?
Toda la seguridad la proporciona un firewall por contrato de arrendamiento, esto quiere decir que se dispone de la última tecnología y actualizaciones previas por parte de la empresa que se contrató.

6. ¿Han tenido ataques no previstos y de que tipo?
Han intentado atacar desde afuera de la red de diferentes maneras sin ningún logro porque se encuentran con un firewall prácticamente impenetrable y cada vez que intentan algo el da un reporte con la información detallada del tipo de ataque y atacante.

Se ha sabido de troyanos y gusanos en algunas partes de las subredes, donde no se tiene mucha seguridad interna pero han sido eliminados por el administrador de dicha subred sin mucho tipo de inconveniente.

7. ¿Si ha habido ataques, qué tipo de información se ha visto afectada o cuales han sido las consecuencias de dicho ataque?

Los ataques vienen de Internet sin ningún efecto para la información valiosa.

8. ¿Existe algún plan de contingencia?
Se han creado licitaciones de consultarías de seguridad y se han hecho contratos con empresas para análisis de vulnerabilidades.

9. ¿Se ha intentado buscar de algún modo las vulnerabilidades de la red de la compañía?
Todavía no pero se van hacer consultorías para buscar vulnerabilidades.

10. ¿Con qué controles cuentan para evitar ataques internos de la red?
Controles con los sistemas operativos, servidores, en el servidor opera MY Scanner Spam assassin que proporciona la seguridad para virus y demás.

AUDITOR: ¿Qué tipos de inconvenientes y/o beneficios puede presentar esta topología de la red?
ADMINISTRADOR: Responde
ASESOR: ¿Cuáles son os objetivos de la seguridad informática?
ADMINISTRADOR: Responde

COMANDANTE: Apreciaciones según lo dicho por el administrador.

Volviendo sobre la definición que trae el Código Penal, encontramos que el delito solamente se configura cuando la máquina atacada haya sido "protegida". Es necesario definir cuándo una máquina esta verdaderamente protegida por la ley, si es necesaria una infraestructura como una PKI o solamente el software que el administrador considere necesaria.

Según lo anterior, el administrador debe buscar vulnerabilidades con un S.D.I. que revise los puertos. Explica modelo de Hacking:

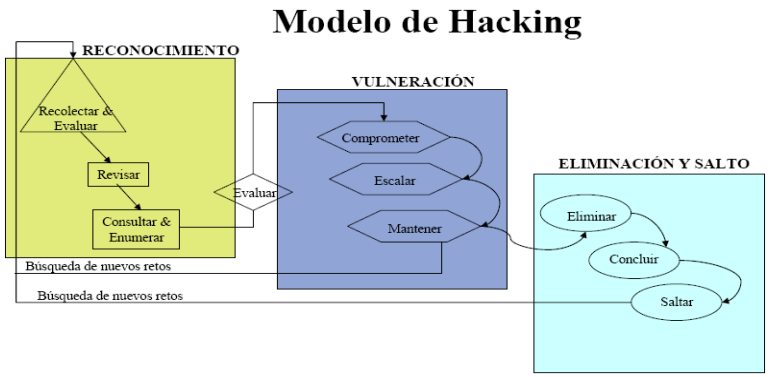


Figura 22. Modelo Hacking

En Colombia muchas universidades dictan módulos de Hacking Ético en sus diplomados, pero ninguna ofrece certificaciones. Solo Estrategia Segura Ltda., presta servicios de Hacking Ético en Colombia con Certificación.

PRINCIPALES RIESGOS

Seguridad de la Información	Asesores deshonestos
Captura de PC desde el exterior	Robo de información
Violación de e-mails	Destrucción de soportes
Violación de contraseñas	Acceso clandestino a redes
Interrupción de servicios	Intercepción de comunicaciones
Virus	Software ilegal
Incumplimiento de leyes	Falsificación de información
Robo o extravío de notebooks	Spam

AUDITOR: Explica ISO 17799 – Gestión de la Seguridad de Información

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento

GERENTE: ¿Qué es una política de seguridad informática?
AUDITOR: Responde
GERENTE: ¿Nuestra organización las contempla actualmente?
ADMINISTRADOR: Responde
GERENTE: ¿Para qué sirven?
AUDITOR: Responde
ADMINISTRADOR: ¿Cómo se elaboran?
AUDITOR: Responde
ADMINISTRADOR: ¿Cuál es su ciclo de vida?
AUDITOR: Responde
ADMINISTRADOR: ¿A quién van dirigidas?
AUDITOR: Responde
GERENTE: ¿Por qué fallan?

AUDITOR: Responde
GERENTE: ¿Qué aspectos deben considerar en nuestra organización?
AUDITOR: Responde
ADMINISTRADOR: ¿Cuáles son las mejores prácticas que la organización debe implantar, según la NORMA ISO 17799?
AUDITOR: Responde
ADMINISTRADOR: ¿Cuáles son las funciones de la gerencia y del auditor según la NORMA ISO 177799?
AUDITOR: Responde
GERENTE: ¿Qué niveles de riesgo compromete el asesor? ¿Por qué?
ADMINISTRADOR: Responde
AUDITOR Refuta con un gráfico según sus conocimientos:

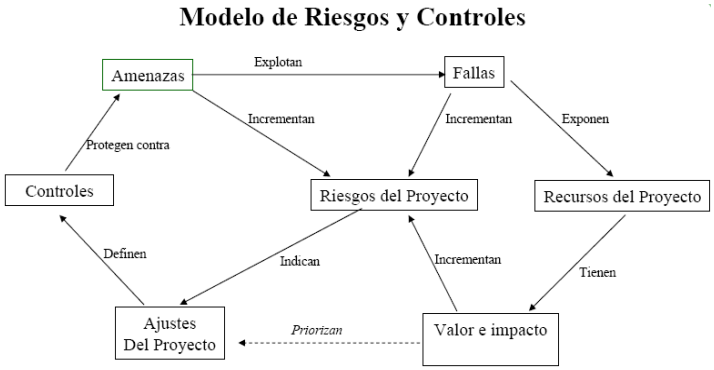


Figura 23. Modelo de riesgos y controles en Sistemas Informáticos

GERENTE: ¿Qué principios de protección de datos vulneró el asesor?
ADMINISTRADOR: Responde
COMANDANTE: Reseña del Código Penal Colombiano

NUEVO CÓDIGO PENAL COLOMBIANO
TITULO III
DELITOS CONTRA LA LIBERTAD INDIVIDUAL Y OTRAS GARANTÍAS

CAPITULO SÉPTIMO*:* De la violación a la intimidad, reserva e interceptación de comunicaciones. **Expone los artículos 192, 193, 194, 195, 196 y 197 de este capítulo.**

CAPITULO SEXTO*: De* las defraudaciones. **Expone los artículos 256, 257 y 258 de este capítulo.**

GERENTE: ¿Qué artículos atañen a las acciones del asesor?
COMANDANTE: Explica los artículos que recaen sobre el asesor.
AUDITOR: Explicación de los problemas en la investigación**:**

- Cambio de la información

ADMINISTRADOR: Expone los problemas en la investigación que a su juicio no fueron tenidas en cuenta.

GERENTE: ¿Cuáles son las repercusiones legales para el asesor?

AUDITOR, ADMINISTRADOR Y COMANDANTE: Responden.

Resolución del juego de roles en grupo, conformación del grupo a través de un WIKI. Cada integrante del grupo debe apropiarse de un rol, analizarlo y desarrollarlo a través de soluciones subjetivas y/o propuestas de manejo en la situación propuesta y en situaciones críticas propuestas por ellos mismos. Se deben identificar las cualidades, defectos, pros y contras del rol jugado dentro del grupo.

En las dos (2) primeras horas de clase deben documentarse a través de las fuentes bibliográficas dispuestas en el ambiente, para sustentar en las otras dos (2) horas de clase. Se apoyará la realización del juego de roles a través una actividad tipo FORO, disponible para que los estudiantes manifiesten sus interrogantes y los puedan resolver entre sí, antes de la sustentación.

Deben desarrollar la metodología Philips 6.6, para exponer verbalmente sus roles y posteriormente debatirlos para conocer las expectativas de cada grupo y sus soluciones. Además de seleccionar cada integrante un rol alternativo y justificarlo. Se generará un archivo por grupo según las especificaciones del profesor, en el cual se reportarán la experiencia, el caso de estudio resuelto y la forma de desarrollo de la metodología Philips 6.6. Será subido a través de un recurso de la plataforma para la revisión y valoración del profesor.

3.1.2.1.3. Cuestionarios tipo ECAES

Se desarrolló la metodología de cuestionario tipo ECAES para adentrar al estudiante en el tema de Sistemas de Detección de Intrusos y permitirle reconocer sus conocimientos y capacidad de razonamiento para con la miscelánea de preguntas que se proponen. Se diseñarán veinte preguntas distribuidas así:

NÚMERO PREGUNTA	INDICADOR		
	COMPONENTE	COMPETENCIA	NIVEL DE COMPLEJIDAD
1	d2	Interpretativa	MEDIO
2	d2	Interpretativa	MEDIO
3	d2	Interpretativa	BAJO
4	d3	Propositiva	ALTO
5	d2	Interpretativa	MEDIO
6	d3	Interpretativa	MEDIO
7	d3	Interpretativa	MEDIO
8	d2	Interpretativa	MEDIO
9	d2	Interpretativa	MEDIO
10	d3	Argumentativa	ALTO
11	d3	Interpretativa	MEDIO
12	d2	Interpretativa	ALTO
13	d2	Argumentativa	MEDIO
14	d3	Propositiva	ALTO
15	d2	Interpretativa	BAJO
16	d2	Interpretativa	MEDIO
17	d3	Interpretativa	MEDIO
18	d2	Interpretativa	ALTO
19	d3	Argumentativa	MEDIO
20	d3	Argumentativa	MEDIO

Tabla 16. Resumen de preguntas ECAES

Para mejor información sobre convenciones, ver ANEXO C.

1. Los ataques que se realizan a los sistemas y que están encargados de obtener información sin realizarle cambio alguno ni modificaciones, pero capturan logins, ips y passwords de usuarios se conocen como:

A. Snooping y downloading.
B. Jamming o flooding.
C. Eavesdropping y packet sniffing. **CLAVE**
D. Tampering o data diddling.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red. Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red.

2. El spoofing se caracteriza por ser un tipo de ataque para obtener información e ingresar en otro sistema; su función es:

A. Actuar en nombre de otros usuarios. **CLAVE**
B. Desactivar o saturar los recursos del sistema.
C. Obtener claves que permitan ingresar a servidores.
D. Obtener información sin modificarla.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos.

3. A través de la ingeniería social se puede acceder a sistemas o dispositivos, así como también formar parte del proceso de obtención de información, ataque y penetración. Esto se asemeja a un:

A. Cracker
B. Hacker **CLAVE**
C. Firewall
D. Phisher

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama relacionada con la informática. Además, su función se basa en construir y solucionar problemas que atenten contra la vulnerabilidad de un sistema o aplicación.

4. En los siguientes SDI basados en detección de usos indebidos, ¿Cuál cree que sería el más adecuado para proceder cuando se detecta que un usuario está ingresando al sistema desde dos direcciones diferentes?

A. La detección basada en modelos
B. Los análisis de transición entre estados
C. Las reglas de comparación y emparejamiento de patrones
D. Los sistemas expertos **CLAVE**

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Los sistemas expertos son llamados así porque emulan el comportamiento de un experto en un dominio concreto.

5. ¿Cuál de los siguientes no es un tipo de troyano según el efecto que causan en el sistema?

A. Acceso remoto
B. Troyanos ARP **CLAVE**
C. Deshabilitadores de programas de seguridad
D. Troyanos FTP

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Los troyanos ARP explotan la interacción de la IP y el protocolo de Ethernet y no acceden directamente a un equipo.

6. Para implementar un S.D.I es necesario tener en consideración varios aspectos como topología, infraestructura y T.I. con las que cuenta una organización. Además si es necesaria una solución Software, Hardware o una combinación de éstas dos. Existen tres tipos de S.D.I a aplicar:

A. HHIDS, NNIDS y DDIDS
B. HIDSS, NIDSS y DIDSS
C. HIDS, NIDS y DIDS **CLAVE**
D. HIIDS, NIIDS y DIIDS

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Son las abreviaturas de Sistemas de Detección de Intrusos en Host, en Red y Distribuidos en su orden.

7. Los SDI basados en detección de anomalías se basan en la premisa de que cualquier ataque o intento de ataque implica un uso anormal de los sistemas, existen aproximaciones, una de ellas utiliza métodos estadísticos donde el detector observa las actividades de los elementos del sistema y genera para cada uno un perfil, cuál de los siguientes tipos de datos se emplean para elaborar los perfiles:

A. Genéricas
B. Categóricas **CLAVE**
C. Alfabéticas
D. Distribución de los archivos de auditoria

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Son aquellas cuyo resultado es una categoría individual y miden la frecuencia relativa o la distribución de una actividad determinada.

8. Cuando se presenta un ataque de Jamming o Flooding en el sistema se presenta una de las siguientes reacciones:

A. Realizará acciones diferentes a las que le pide la máquina anfitriona
B. Se activan los recursos del servidor
C. Provocará la baja temporal del servicio del servidor **CLAVE**
D. Ninguna de las anteriores

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

9. Un SDI o IDS es un instrumento de seguridad informática que intenta determinar o monitorear las anomalías presentadas en el tráfico de una red para reconocer los intentos de intrusión de un agente humano o lógico con el fin comprometer la confidencialidad, integridad o disponibilidad de las TI de una organización. Según esto, un SDI tiene como objetivo:

A. Avisar en tiempo real de los ataques que se producen en las infraestructuras TIC **CLAVE**
B. Buscar datos previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre la red
C. Sustituir las políticas de seguridad de la información de una organización
D. Documentar las amenazas lógicas experimentadas por la organización

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: El objetivo de los S.D.I es prevenir los ataques más no detenerlos, aunque si pueden generar respuestas a algunos de ellos.

10. Los SDI están basados en el reconocimiento de patrones que le permitan discriminar entre un ataque verdadero y uno falso. Dentro de una organización que desea aplicar esta herramienta para integrarla a su plataforma de TI, se puede relacionar como limitante:

A. La aparición de "falsos positivos”
B. La aparición de "falsos negativos"

C. El efecto “Ventana de Vulnerabilidad”
D. Aplicaciones desarrolladas a la medida de las necesidades de la organización **CLAVE**

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Las diversidad de aplicaciones dificultarían la generación de firmas para el S.D.I y el tiempo trascurrido desde de la materialización de una amenaza hasta que se desarrolle una protección, interrumpirían la continuidad del negocio y por limitantes para su aplicación.

11. Es muy importante dejar en claro que los S.D.I presentan cierta tolerancia a fallos o capacidad de respuesta ante situaciones inesperadas debido al carácter altamente dinámico de un entorno informático. A partir de estas premisas, cuál requisito debe tener en cuenta una organización al aplicar un SDI:

A. El SDI ha de ejecutarse continuamente sin supervisión humana
B. Interoperabilidad e integración
C. Que permita la detención de ataques
D. Velocidad en las redes **CLAVE**

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: La velocidad de su red es un factor relevante debido a la capacidad que tendrá el S.D.I de revisar los paquetes de información. A mayor velocidad mayor dificultad del S.D.I. para revisarlos.

12. Como una herramienta adicional que pueda ayudar a resolver los problemas y limitaciones de los SDI, existen acercamientos que hacen uso de algunas ramas de la ciencia, con la intención de evitar la aparición de falsos positivos/negativos así como mejorar sus capacidades de detección ante nuevos ataques. Una de estas es:

A. Ingeniería Biomédica
B. Minería de Datos **CLAVE**
C. Esteganografía
D. Telemática

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Según referencias de investigaciones como “Real Data Mining-based Intrusion Detection”, su aplicación estaría dada en la detección de anomalías utilizando técnicas de

Clasificación, Episodios Frecuentes, Asociación de Valores (correlaciones) y Análisis adaptativos.

13. Actualmente se deben analizar y diseñar requerimientos en la organización que generan responsabilidades corporativas necesarias para completar exitosamente un proyecto de SDI. La más importante es:

A. Análisis de la infraestructura de red **CLAVE**
B. Descargar los programas en los puestos de trabajo
C. Distribución de la estructura laboral
D. Generación de Políticas Organizacionales

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: El análisis en la infraestructura de red de la organización permite saber que SDI es el que mejor aplica para ala organización.

14. En una organización existen factores gerenciales necesarios para completar exitosamente un proyecto de S.D.I. que hacen que los mismos permanezcan aplicados en la organización y no generen sobre costos innecesarios. La más importante es:

A. Sistemas Operativos a proteger.
B. Seguridad física y control de acceso a los recursos.
C. Establecimiento de políticas de seguridad corporativas. **CLAVE**
D. Seguir las mejores prácticas en diseño de T.I.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Es una habilidad que todos los gerentes deben rescatar pues éstas le permiten mantener sus TI seguras y acorde a las necesidades de la organización.

15. Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático, esto se refiere más exactamente a:

A. Supervisión de logs.
B. Ingreso al departamento de TI de una organización.
C. Uso del computador de un compañero de trabajo en la organización.
D. Acceso no autorizado a un sistema con la intención de perpetrar un ataque a una red informática. **CLAVE**

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: La intrusión permite al atacante acceder a privilegios de administrador para violar o desactivar los mecanismos de seguridad.

16. Un S.D.I puede presentar dos tipos de respuestas, la primera denominada pasiva y la segunda activa, esto es porque:

A. La primera es relacionada con notificaciones al administrador y la segunda es accionada automáticamente por el SDI
B. La primera es relacionada con notificaciones automáticas y la segunda analiza los patrones de la intrusión solamente.
C. La primera es accionada automáticamente por el SDI debido a los patrones de las intrusiones y la segunda está relacionada con notificaciones hechas al administrador.
D. Ninguna de las anteriores.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Las respuestas activas son las que se accionan automáticamente y las pasivas son notificaciones al administrador, estas son los dos tipos de respuestas ante una intrusión.

17. La topología de un S.D.I puede variar dependiendo del administrador del servidor, decisiones organizacionales y de la arquitectura del S.D.I, se aconseja una forma de ubicación debido a la seguridad que aporta:

A. Existen dos formas de ubicación del mismo, antes del firewall, después del firewall.
B. Existen tres formas de ubicación del mismo, antes del firewall, después del firewall y un sistema híbrido de los dos anteriores. **CLAVE**
C. Existe una forma de ubicar del mismo, antes del firewall.
D. Existe una forma de ubicación del mismo, en cada host.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Las topologías de red dependen de muchos factores y su ubicación es una decisión organizacional debido a los costos que contrae su aplicación. Pero la ubicación más idónea para asegurar la información corresponde a esta forma.

18. Los SDI tienen diversas fuentes de información con las cuales logra recoger los eventos para analizar los diferentes tipos de paquetes que proceden y salen de una red, una de estas no corresponde a este tipo de fuente:

A. Paquetes de red
B. Eventos del Sistema Operativo
C. Software de Aplicación
D. Certificado digital **CLAVE**

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: El Certificado Digital permite identificar una persona o entidad en transacciones electrónicas, además, es un documento digital con el cual una autoridad de certificación garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

19. Las inversiones en TIC dentro de una organización, como un S.D.I, proveen aparte de valor agregado al negocio, seguridad a la información, ya que:

A. Permiten poner a prueba el estado de las medidas de seguridad implantadas por la organización. **CLAVE**
B. Disminuyen la cantidad de falsos positivos.
C. Da mayor credibilidad a sus servicios transaccionales.
D. Constituyen parte integral de este tipo de servicios.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: Los costos de no aplicación son mayores que los costos por adquisición de TICs, ya que contribuyen a la continuidad del negocio.

20. El administrador de un servidor considera que no es necesario el S.D.I ya que cuentan con un FIREWALL costoso, su afirmación según un gerente de organización es cierta, porque:

A. Las TI no se han visto comprometidas hasta el momento. **CLAVE**
B. Confía plenamente en el criterio del Administrador.
C. Los costos de inversión en las mismas son considerables.
D. Es más fácil arriesgar la continuidad del negocio que invertir en más TIC.

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE: El firewall no es suficiente como política de seguridad pues no permite vigilar otro de tipo de intrusiones que el S.D.I si logra captar y el primero deja puertos abiertos.

Actividad individual. Los estudiantes utilizarán las dos (2) primeras horas de clase para analizar las fuentes bibliográficas disponibles en el ambiente de aprendizaje, relacionadas con el tema de S.D.I.

Cada estudiante tendrá un tiempo límite de una hora y veinte minutos, equivalente a 4 minutos por pregunta para responderlas durante la segunda sesión de clase equivalente a dos (2) horas. Al finalizar el ejercicio se presentarán las respuestas.

Se apoyará la resolución de las preguntas tipo ECAES a través de una actividad tipo FORO en el cual se debatirán las respuestas y las preguntas hechas para una eventual realimentación donde la participación será tenida en cuenta en la evaluación del profesor a los estudiantes. Se generará un archivo en el cual se reportará la experiencia. Será subido a través de un recurso de la plataforma para la posterior revisión y valoración del profesor.

3.1.2.1.4. Simulación

Se desarrolló la metodología de Simulación para permitir al estudiante analizar dos portales bancarios para compararlos y entender sus diferencias, falencias, fortalezas y oportunidades que ofrecen a los usuarios. Se seleccionaron portales financieras electrónicos debido a que los ataques de phishing las están afectando en gran medida. Se diseñaron dos interfaces personalizadas de portales bancarios en línea. El primer banco se denominó ***BANCO1*** y el otro ***BANCOSEGURO.***

CARACTERÍSTICAS DE LA INTERFAZ DE BANCO1

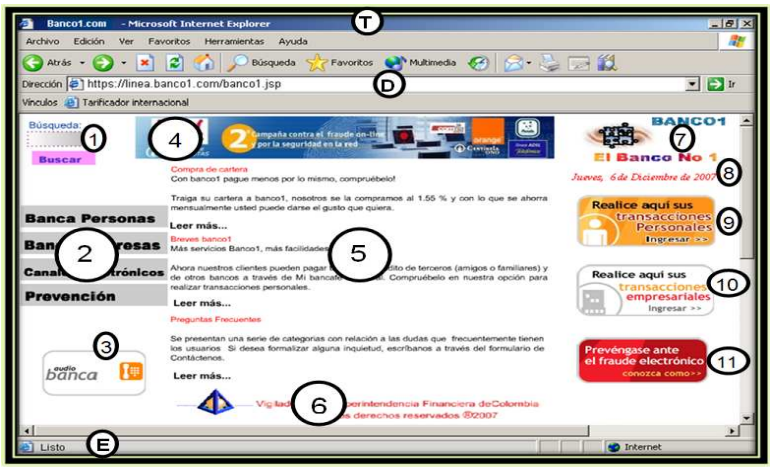


Figura 24. Ventana de Internet Explorer de banco1

Barra de título: (T)

- Corresponde al nombre del banco.

Barra de dirección: (D)

- Indica la dirección del banco y HTTPS indica que es una conexión segura.

Barra de estado: (E)

- Indica que la conexión está lista y la página se ha cargado.

VENTANA DE NAVEGACIÓN

1. Esta interfaz presenta una herramienta de búsqueda con respecto a los temas tratados dentro del portal.
2. Cuatro botones que transportan al usuario a los módulos de información correspondiente a transacciones y medidas de prevención.
3. Una opción que permite al usuario conocer las líneas telefónicas de atención al cliente ante posibles fraudes o engaños.
4. Presenta banner publicitarios.
5. En la página principal hay tres vínculos de información al usuario.
6. Logo de la superintendencia Financiera de Colombia, entidad encargada de vigilar las acciones de las entidades financieras del país.
7. El logo del banco en la parte superior derecha.
8. La fecha actual.
9. Un botón de transacciones personales.
10. Un botón de transacciones empresariales.
11. Un botón que presenta información sobre medidas de seguridad.

CARACTERÍSTICAS DE LA INTERFAZ DE BANCOSEGURO

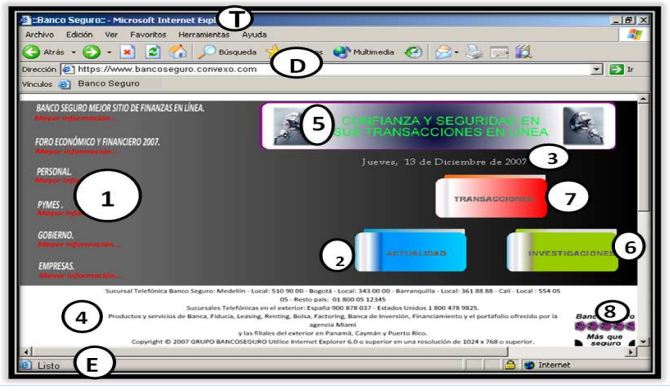


Figura 25. Ventana de Internet Explorer de Bancoseguro

Barra de título: (T)

- Corresponde al nombre del banco.

Barra de dirección: (D)

- Indica la dirección correspondiente al banco y HTTPS indica que es una conexión segura.

Barra de estado: (E)

- Indica que la conexión está lista y la página se ha cargado, además del candado que representa la confidencialidad en las transacciones.

VENTANA DE NAVEGACIÓN

1. Menú principal de la página del banco.
2. Botón actualidad en relación a sus servicios.
3. La fecha actual.
4. Espacio de líneas telefónicas de atención al cliente ante fraudes.
5. Presenta banner publicitarios.
6. Botón que muestra las investigaciones a la fecha de las implementaciones en el tema de seguridad electrónica.
7. Un botón de transacciones.
8. Logo del banco.

Los estudiantes deben analizar las características inherentes a las páginas bancarias respecto a la seguridad según las políticas nacionales e internacionales para entender si éstas cumplen o no con sus obligaciones.

CUESTIONARIO

Según lo analizado para cada una de las interfaces responda falso o verdadero el cuestionario con según corresponda y sustente a través de la imagen enriquecida:

1. ¿Un banner puede provocar un ataque de phishing?
2. ¿Las entidades bancarias deben hacer Análisis de Vulnerabilidades?
3. ¿Los usuarios se percatan de la seguridad aplicada a los portales bancarios, al realizar sus transacciones?
4. ¿Las páginas bancarias del país ofrecen canales de denuncia para los usuarios afectados?
5. ¿La legislación colombiana permite la disminución de este delito?

6. La empresa colombiana AZUAN presenta un software que permite a un único usuario configurar su computador para realizar transacciones financieras. ¿Es útil?
7. ¿Los usuarios tienen en cuenta los criterios dispuestos para saber si una página es verídica?
8. ¿La redacción en los portales bancarios son criterio de su fidelidad?
9. ¿Se puede evitar la ingeniería social sobre los usuarios?
10. ¿Los usuarios desconfían del uso de tecnologías en línea?
11. ¿Las VPN se pueden acercar a seguridad en informática de alto nivel?
12. ¿Los encargados de Seguridad Informática de las entidades financieras permiten el phishing?
13. ¿Es útil un LiveCD o CD Autónomo para evitar el phishing?
14. ¿Es la ingeniería social la forma de combatir las vulnerabilidades en TI?
15. ¿Un Subdominio permite saber a un usuario si está en un lugar seguro?
16. ¿El uso de ventanas hijas externas o emergentes es seguro?
17. ¿El uso de ventanas que ocultan la barra de estado es seguro?
18. ¿Las entidades financieras en Colombia invierten en seguridad informática?
19. ¿Un usuario verifica el uso de un certificado válido en una página?
20. ¿El SSL/TSL asegura la integridad de la información enviada?
21. ¿Los mensajes SMS permiten el desarrollo del phishing?
22. ¿Actualmente se toman precauciones en los servidores DNS?
23. ¿Los portales Web bancarios deben realizar auditorias?
24. ¿El phishing se da por la asimetría entre entidades, clientes, desarrolladores y diseñadores?
25. ¿Logra la informática forense contrarrestar el phishing?
26. Los controles propuestos en la norma ISO/IEC 17799 en cuanto a los riesgos por el acceso de terceras partes, ¿contribuyen a una disminución de ataques phishing?
27. ¿Las entidades bancarias reconocen las normas técnicas de seguridad informática?
28. ¿Es necesario el correo para la comunicación cliente – entidad?
29. ¿Se vulnera algún principio de protección de datos con el phishing?
30. ¿Las políticas de seguridad informática propuestas por ASOBANCARIA, sirven como referente para desarrollar políticas internas?

Análisis de la simulación en grupo, conformación del grupo a través de un WIKI. Cada grupo analizará y desarrollará el cuestionario titulado: “CUESTIONARIO SOBRE LA SIMULACIÓN”.

Esta primera etapa será desarrollada en dos (2) horas de clase, teniendo como soporte las fuentes bibliográficas dispuestas. Además, se apoyará la realización de la simulación a través de un foro para que los estudiantes manifiesten sus interrogantes y los resuelvan.

En las dos (2) horas siguientes de clase desarrollarán la imagen enriquecida en la cual se plasmarán las respuestas al cuestionario. Se generará un archivo en el cual reportarán la experiencia, la imagen enriquecida y su desarrollo, éste será subido a través de un recurso de la plataforma para revisión y valoración por parte del profesor, según sus especificaciones.

3.1.3. Implementación

3.1.3.1.1. Casos de estudio

Éste OA se catalogará en el Tema 7 de la plataforma de AS y CI, denominado ***DEJANDO CERTIDICADO Y FIRMA DIGITAL EN LA UIS*** desglosado de la siguiente manera:

Figura 26. Unidad de Aprendizaje: Firma Digital

3.1.3.1.2. Juego de roles

Éste OA se catalogará en el Tema 8 de la plataforma de AS y CI, denominado ***HACKEANDO ACADÉMICAMENTE*** desglosado de la siguiente manera:

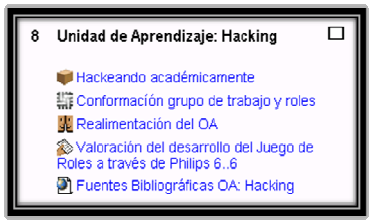


Figura 27. Unidad de Aprendizaje: Hacking

3.1.3.1.3. Cuestionarios tipo ECAES

Éste OA se catalogará en el Tema 9 de la plataforma de AS y CI, denominado ***APRENDIENDO DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS*** desglosado de la siguiente manera:

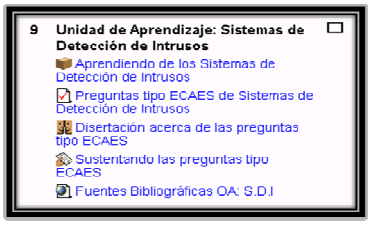


Figura 28. Unidad de Aprendizaje: S.D.I

3.1.3.1.4. Simulación

Éste OA se catalogará en el Tema 10 de la plataforma de AS y CI, denominado ***PESCANDO EN EL MUNDO DEL PHISHING*** desglosado de la siguiente manera:

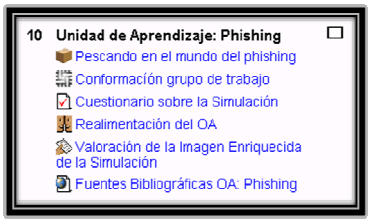


Figura 29. Unidad de Aprendizaje: Phishing

3.2. ETAPA DE MONTAJE

3.2.1. Metodología

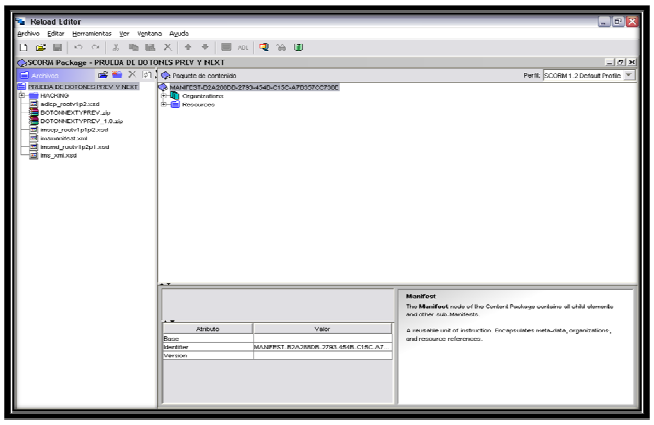


Figura 30. Interfaz Gráfica de RELOAD EDITOR.

3.2.2. Acoplamiento con Moodle

Se desarrollaron OA para visualizarse en equipos con pantallas de 17 pulgadas, permitiendo presentar los OA bajo las siguientes características:

- Resolución óptima pantalla para visualización: 1024*768
- Resolución opcional pantalla para visualización: 1152*864
- Tamaño de la ventana de los OA aplicados en Moodle: 770*520

3.2.3. Pruebas

Los OA de aprendizaje son empaquetados con el software RELOAD EDITOR versión 2.0.2., con reseña en (CRUZ, 2006: 211), el cual es utilizado para estandarizar los OA en Moodle y permitir su interoperabilidad entre otras características. El icono para el recurso SCORM en Moodle es 

Se tuvieron en cuenta las características de los OA explicadas en (CRUZ, 2006: 187) para su desarrollo y aplicación.

Figura 32. Estructurando el SCORM en Moodle

CAPÍTULO IV

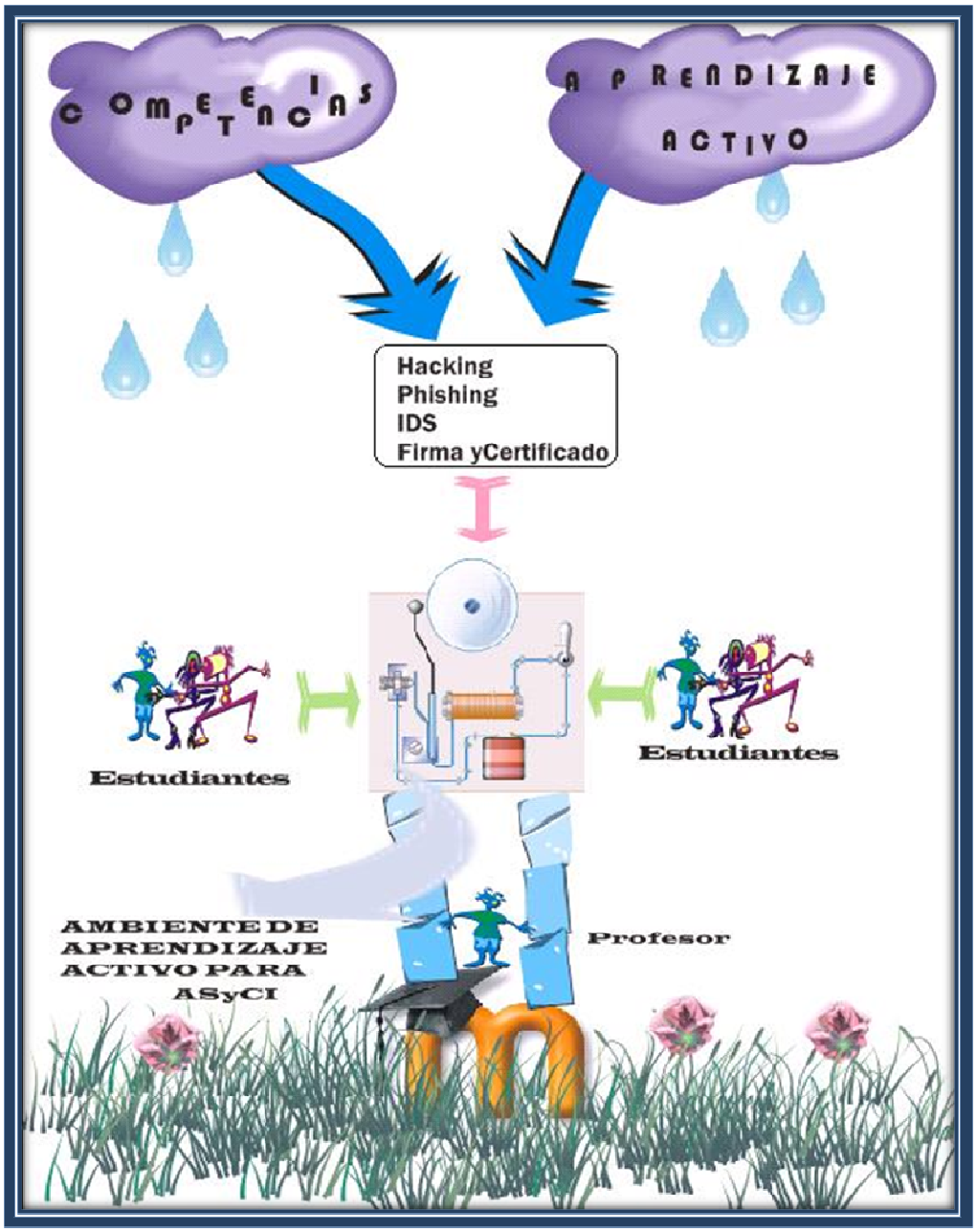


Figura 33. Estructura A^2- AS y CI

4. METODOLOGÍA DE DESARROLLO DEL A^2 – AS y CI

4.1. PROTOTIPADO EVOLUTIVO Y UML

- ***SELECCIÓN PROTOTIPADO EVOLUTIVO[71]***

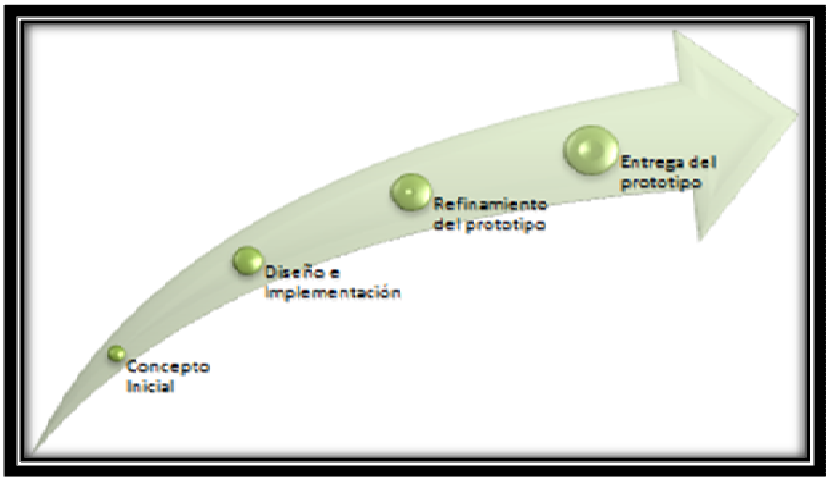


Figura 34. Topología del Modelo Evolutivo para el desarrollo de software

Es importante reconocer el contexto en el que se va a desarrollar el software, es por esto que se ha diseñado el ambiente a través del proceso que define el ciclo de vida del prototipado evolutivo pues según lo analizado, las necesidades del proyecto y el tiempo estipulado, permitirán desarrollarlo para lograr los objetivos propuestos desde un comienzo. Además basado en las siguientes premisas:

Capacidades del Modelo	Comportamiento Prototipado Evolutivo
Bajos conocimientos de requerimientos	Excelente
Baja comprensión de la arquitectura	Medio
Fiabilidad del software	Medio
Desarrollo del software	Excelente
Planificación predefinida	Malo
Poco tiempo de gestión	Medio
Modificaciones en el proceso	Excelente
Signos de progreso	Excelente

Tabla 17. Capacidades Modelo Evolutivo

[71] Analizado del documento:" Ciclos de vida de desarrollo de Software-Parte II. Grupo STI "

A partir de lo anterior y dadas las circunstancias del proyecto debido a su constante evolución y renovación por las áreas que lo complementan como son el Diseño Gráfico, la Pedagogía y la Ingeniería del Software, es que se vio la necesidad de recurrir a este modelo para lograr un prototipo que finalmente se asemejara a lo que el profesor desde un principio propuso para esta Unidad de Aprendizaje.

- ***DESCRIPCIÓN UML[72]***

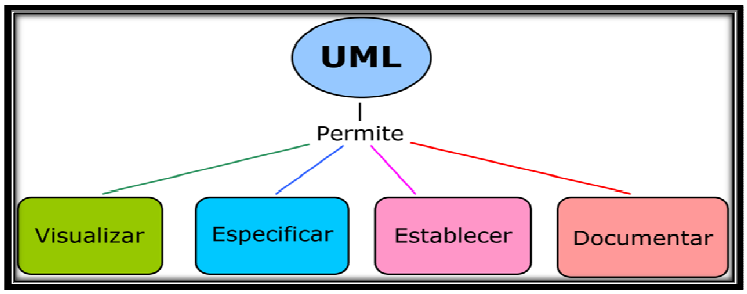


Figura 35. Descripción UML

UML es una herramienta que permite a los desarrolladores presentar sus aplicaciones en un lenguaje estándar y a los usuarios la posibilidad de entender lo que éste desea hacer con sus requerimientos. Es importante dejar en claro la importancia de la función que cumple UML como soporte de planeación para cada las etapas de análisis y diseño del desarrollo de software, es así como podemos describir su definición:

"Es un lenguaje para visualizar, especificar, construir y documentar los artefactos de un sistema que involucra una gran cantidad de software, desde una perspectiva orientada a objetos".

Además permite:

- Representar a través de gráficos, el proceso de modelado aplicado a los proyectos software. Combina los gráficos con una semántica bien definida lo que permite elaborar modelos totalmente claros en el lenguaje común.

- Especificar los componentes del análisis, diseño e implementación que deben realizarse al desarrollar proyectos de software.

- La generación de código a partir de un modelo en UML compatible con muchos lenguajes de programación.

[72] Para mayor referencia véase [27] en bibliografía.

- Documentar módulos que componen las aplicaciones además de código ejecutable.

4.1.1. Análisis del Prototipo

4.1.1.1. Partes del prototipo

Básicamente el ambiente de aprendizaje está comprendido por: ***SGA MOODLE, Estándar SCORM, RELOAD Y OA***

4.1.1.2. Actores

Son los usuarios de los casos de uso y desarrollan roles cuando interactúan con los casos de uso. Sus funciones son desglosadas en el caso de uso.

4.1.1.3. Casos de Uso

Es la descripción de las acciones de un sistema a través de los requerimientos de un usuario. Permite generar sistemas acordes a las necesidades del usuario final. A continuación se presenta el caso de uso del prototipo:

4.1.1.4. Diagrama de Actividades

Permite presentar las actividades de forma simplificada a través de un diagrama, las actividades son representadas a través de un rectángulo de puntas redondeadas. Al desarrollarse una actividad, se continúa con la siguiente actividad. Está compuesto por una serie de símbolos, entre los cuales se encuentran:

- Una flecha representa la transición entre dos actividades.
- Un círculo relleno representa el punto de inicio
- Una diana el punto final.

4.1.1.5. Fase de Desarrollo

Se instaló un SGA personalizado con fines de prueba, a través de éste se ensayarán las conexiones a las Bases de Datos Moodle, los OA de los temas

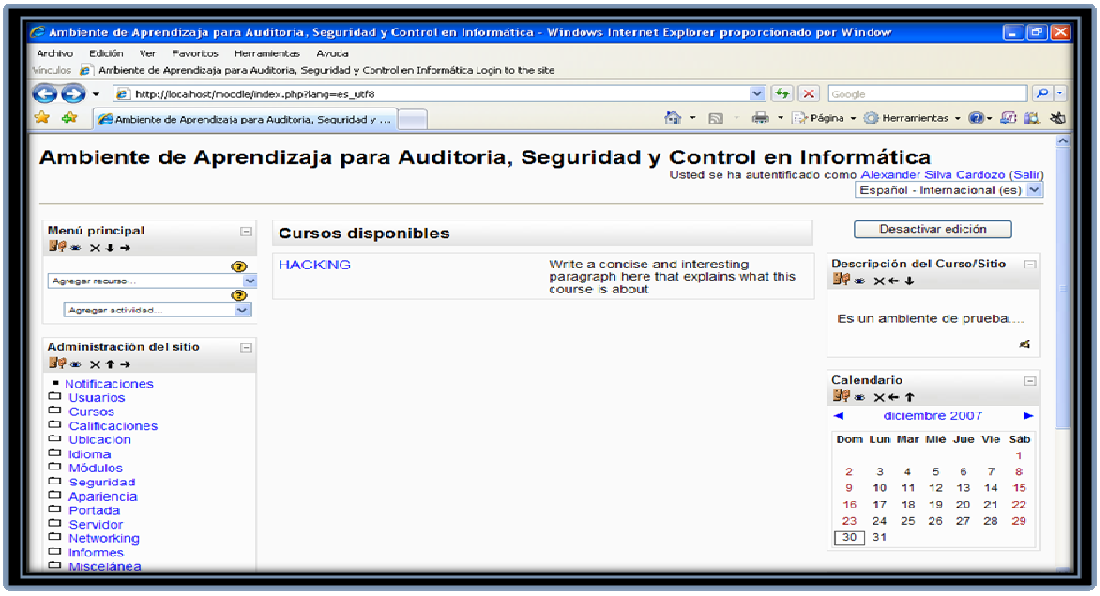


Figura 36. Portada SGA Moodle de prueba

a desarrollar empaquetados con RELOAD EDITOR y montados, las actividades como cuestionarios, las fuentes bibliográficas, la documentación, etcétera. A continuación un aparte de la fase de desarrollo.

4.1.1.6. Refinamiento del Prototipo

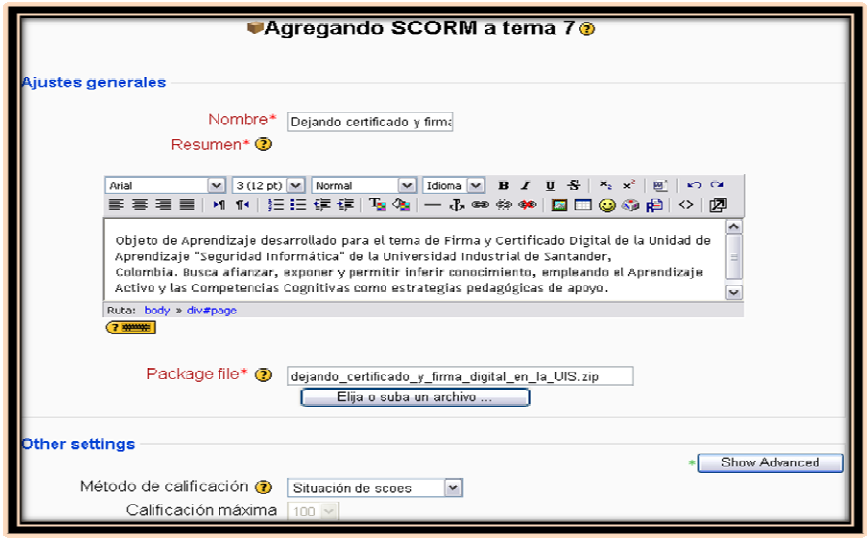


Figura 37. Agregando una actividad SCORM en Moodle

4.1.2. Diseño del Prototipo

4.1.2.1. Consideraciones

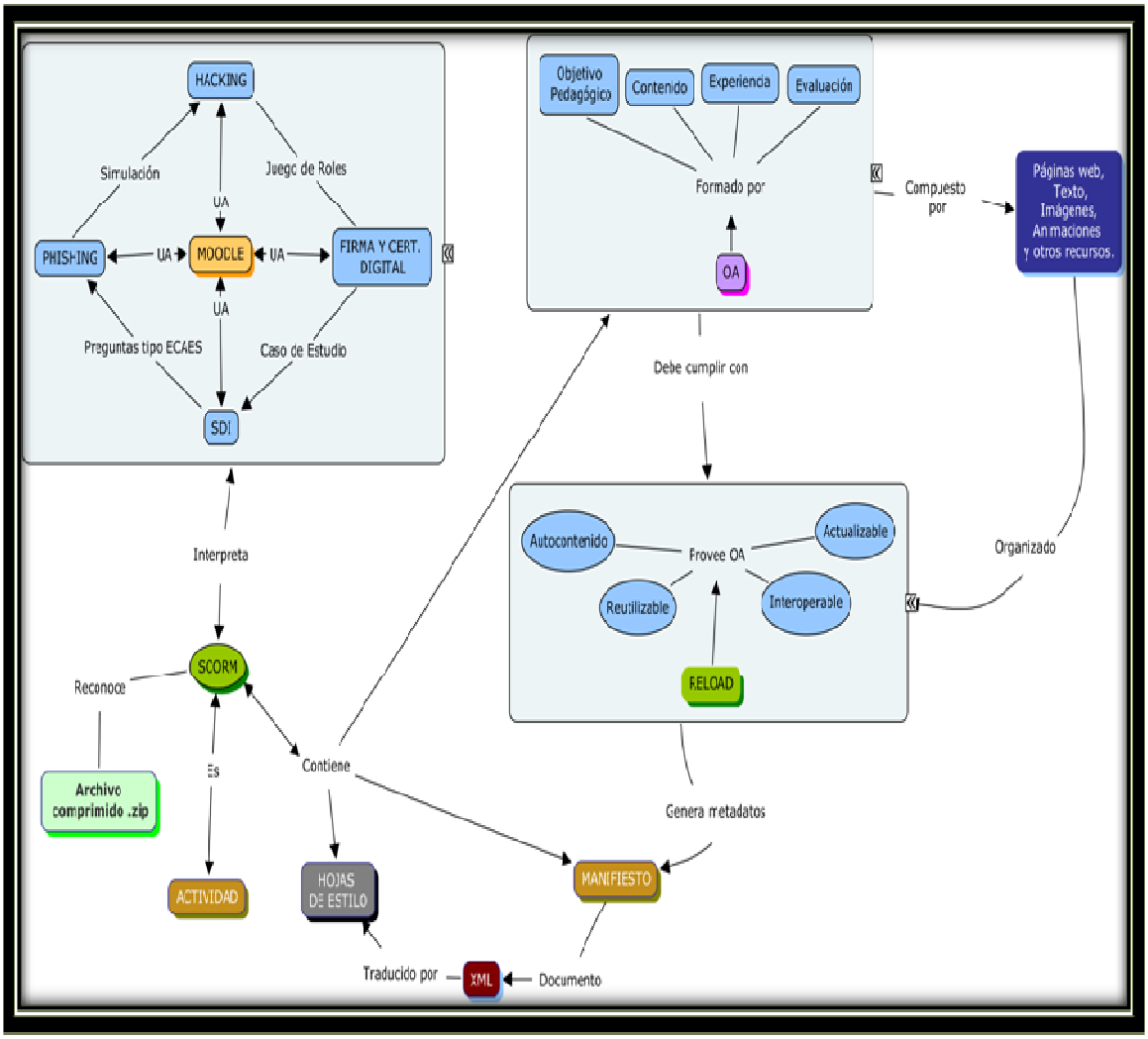


Figura 38. Partes del prototipo

4.1.2.2. Diagrama de estados de sus Componentes

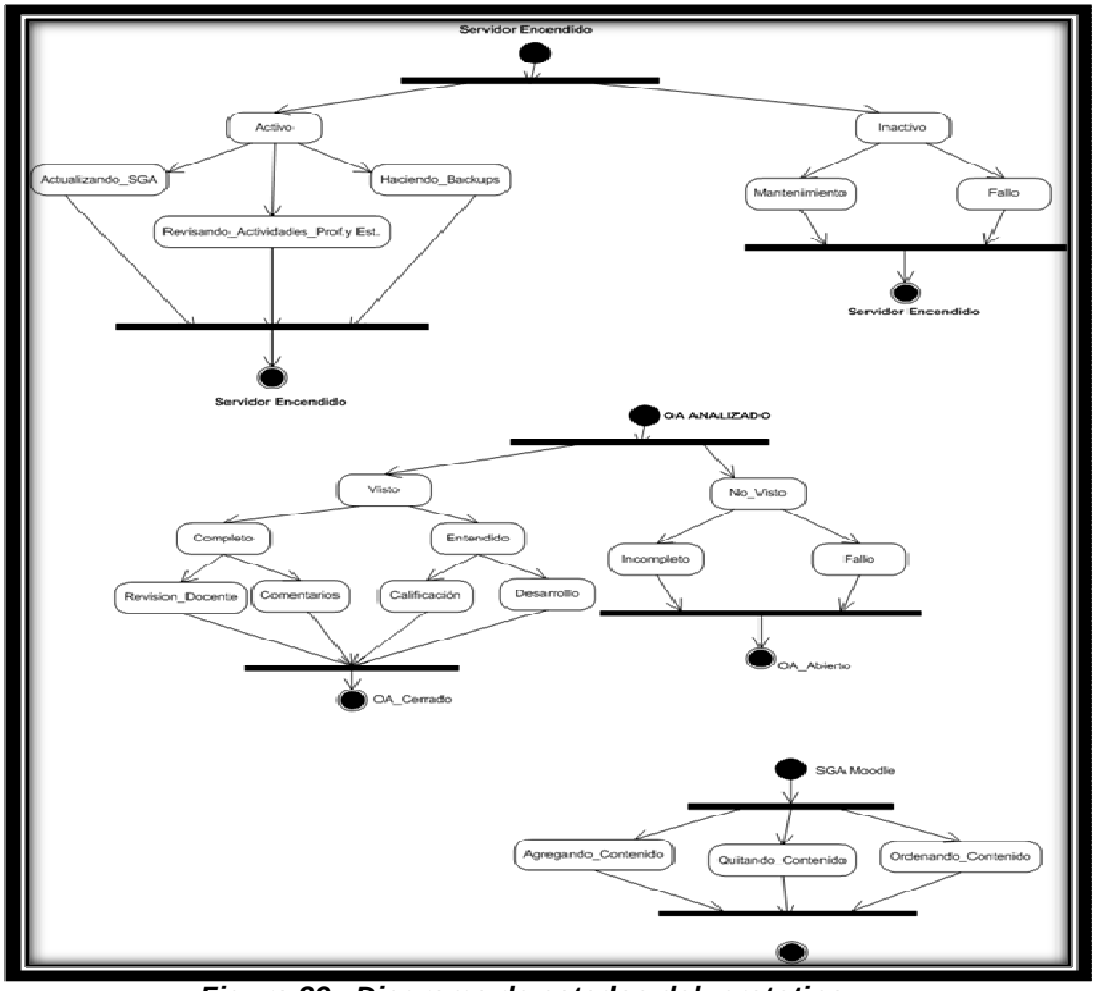


Figura 39. Diagrama de estados del prototipo

4.1.2.3. Actores

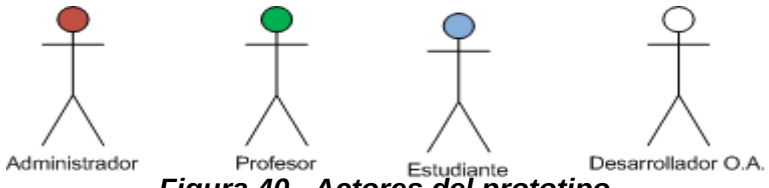


Figura 40. Actores del prototipo

4.1.2.4. Casos de Uso

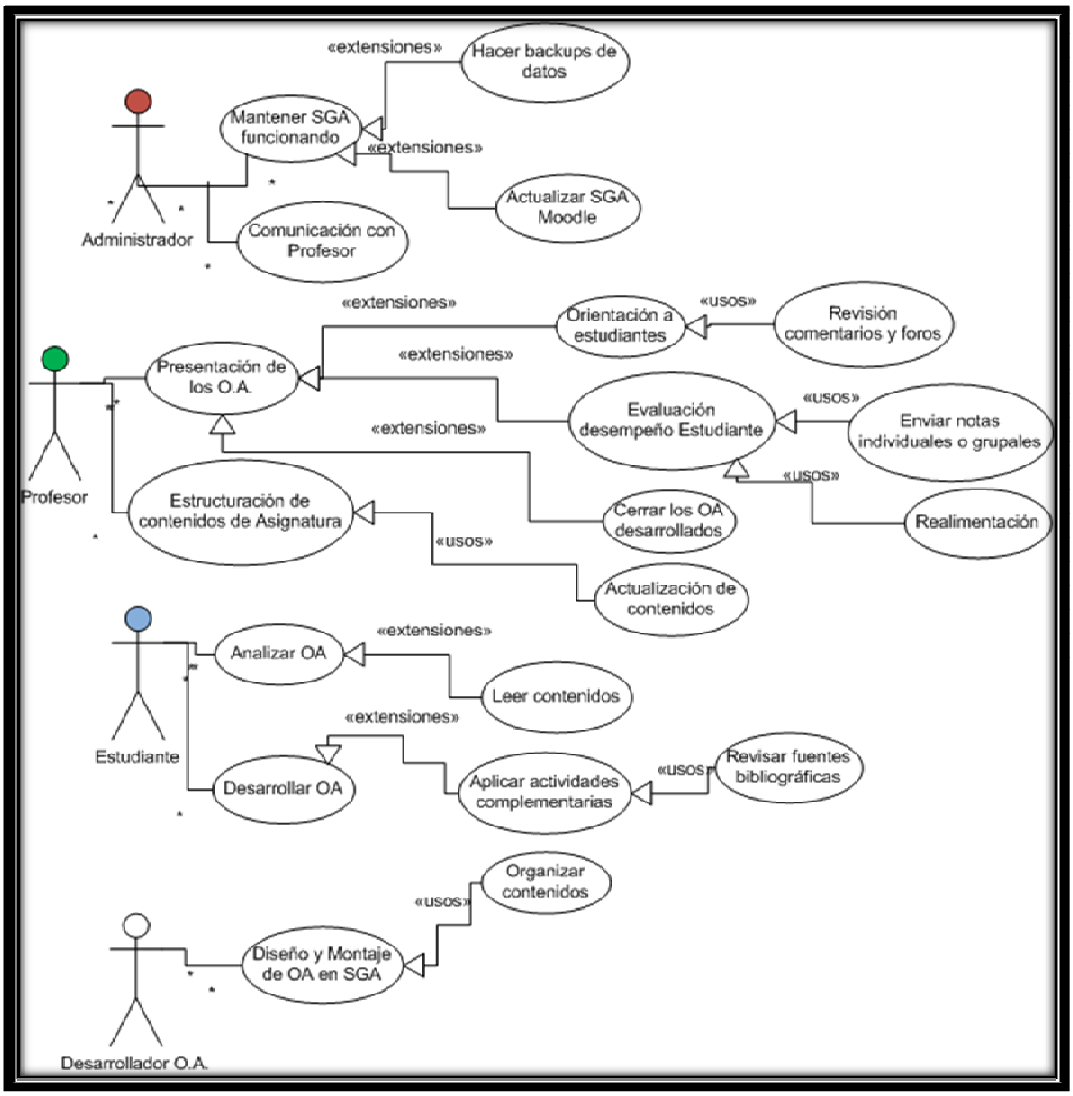


Figura 41. Caso de uso del prototipo

1.2.1.5. Diagrama de Actividades

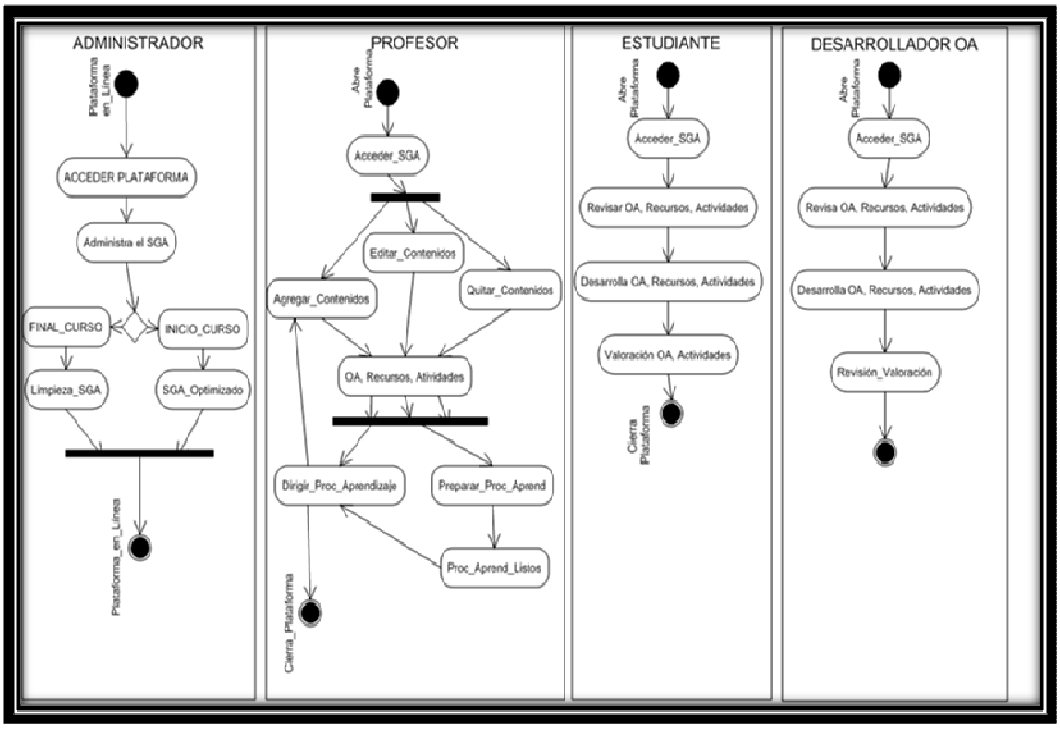


Figura 42. Diagrama de actividades del prototipo

4.1.2.6 Interfaz Según Estándar SCORM

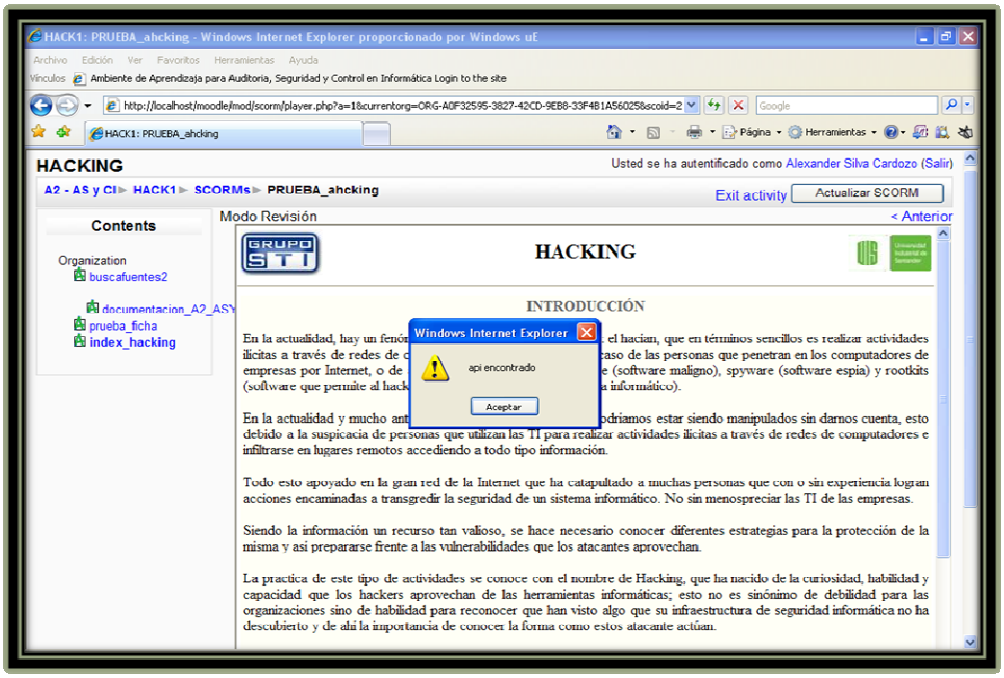


Figura 43. Interfaz SCORM del prototipo

4.1.2.7. Base de Datos Mysql

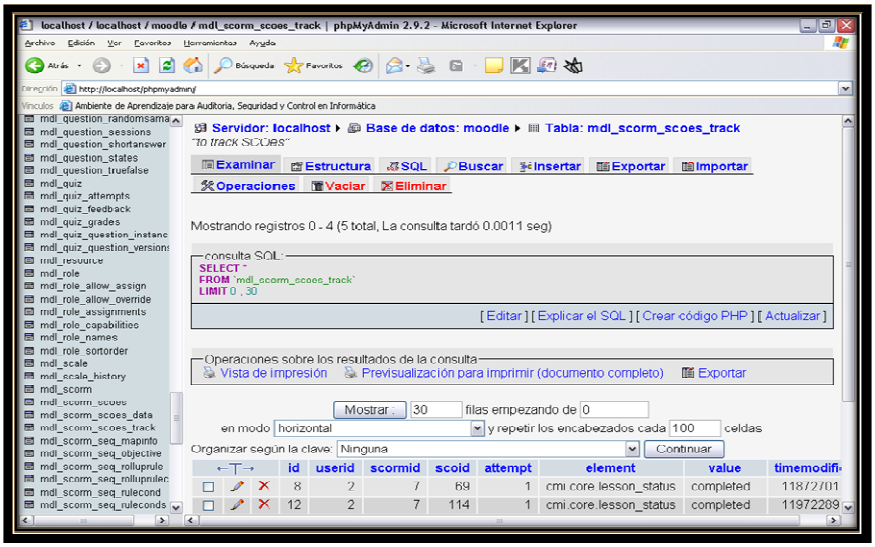


Figura 44. Bases de Datos MYSQL

4.1.2.8. Refinamiento del diseño

Tras diferentes pruebas y desarrollos se llegó a un prototipo beta:

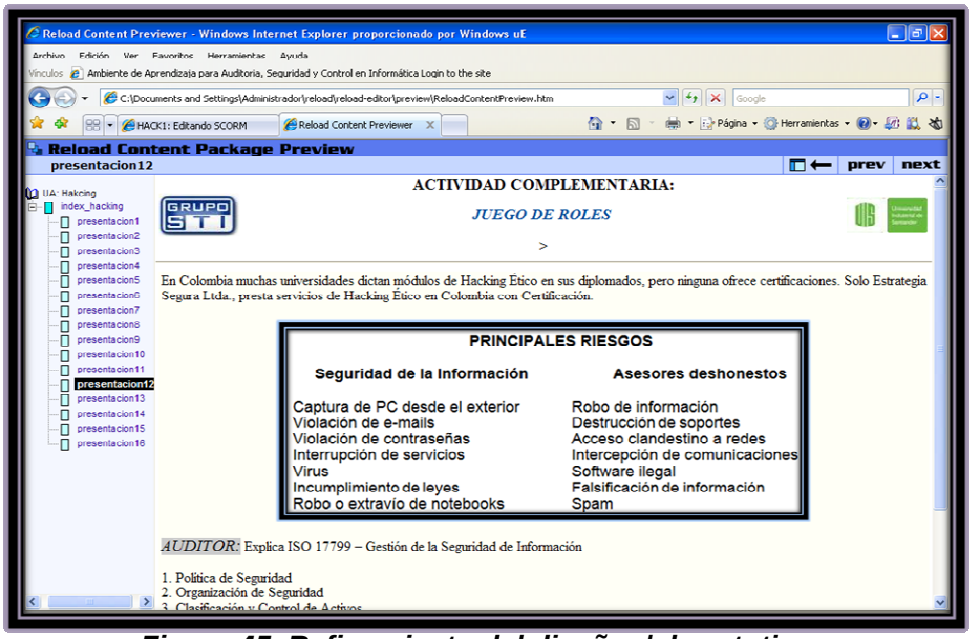


Figura 45. Refinamiento del diseño del prototipo

4.1.3. Implementación

4.1.3.1. Según el estándar SCORM

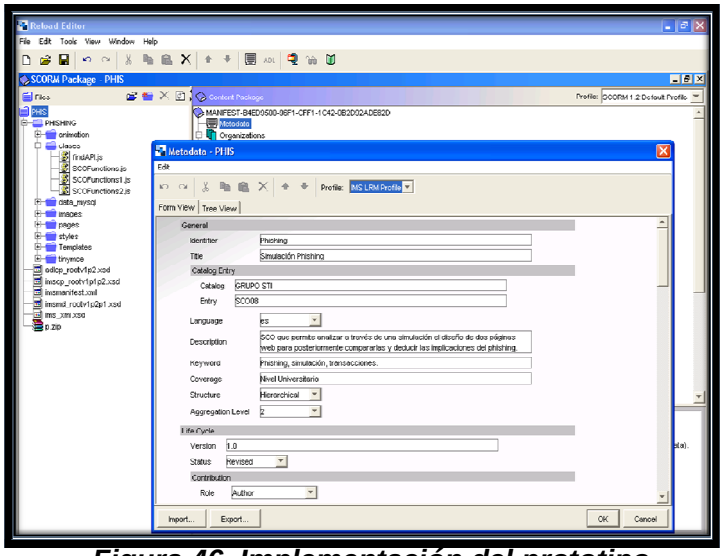


Figura 46. Implementación del prototipo

4.1.3.2. Interacción con Moodle

Figura 47. Interactuando con Moodle

4.1.4. Puesta En Marcha

4.1.4.1. Pruebas de usuarios

Debido a que la asignatura de Seguridad Informática está fuera de las Asignaturas Electivas durante el segundo semestre de 2007, se deja el repositorio de O.A., así como las actividades complementarias dispuestas en la plataforma de AS y CI para el apoyo de ésta. En "Acerca de A^2 - AS y CI" se deja la documentación necesaria para su aplicación y desarrollo.

4.1.4.2. Formato de Evaluación a las pruebas

Se diseñó una actividad tipo cuestionario en el SGA Moodle, el cual pretende verificar los OA realizados y reconocer las recomendaciones por parte de los estudiantes. Este cuestionario estará disponible en la plataforma de la asignatura, se describe a continuación:

1. ¿El lenguaje de los OA es coherente para la asignatura de Seguridad Informática?
2. ¿Los contenidos provistos en la Unidad de Aprendizaje están acorde a su temática?
3. ¿Los O. A. permiten extender los conocimientos de la UA?
4. ¿Es eficiente la metodología de aprendizaje activo?
5. ¿Son un factor importante en el aprendizaje las competencias cognitivas?
6. ¿Las fuentes bibliográficas permiten complementar el contenido de los OA?
7. ¿Qué dificultades presentan los OA?
8. ¿Qué recomendaciones deduce a partir de lo visto en los OA?
9. ¿Qué tipo de contenido agregaría a los OA?
10. ¿Qué actividades complementarían los OA?

CONCLUSIONES

- La aplicación de competencias cognitivas en el desarrollo de Objetos de Aprendizaje permite desarrollar habilidades en el estudiante como la comprensión de lectura, expresión oral y escrita, así como también la construcción de conocimiento empírico.

- Los Sistemas de Gestión de Aprendizaje son una herramienta por explorar que permite al profesor y gestionar roda la información concerniente a una materia y las actividades que permiten desarrollar el aprendizaje en línea.

- La Universidad Industrial de Santander gira actualmente hacia el aprovechamiento del aprendizaje en línea a través de los diferentes proyectos de las escuelas que convergen de una u otra manera, indiferente de sus metodologías, hacia una educación ciento por ciento en línea, siempre y cuando el profesor y la asignatura lo ameriten.

- Las pruebas de estado ECAES que actualmente se imparten no incluye la asignatura de Seguridad Informática dentro de sus parámetros, pero el proyecto aplica sus componentes debido a que el profesor considera que un área de impacto en el ámbito informático y social requiere ser aplicada.

- El diseño de los Objetos de Aprendizaje no son un indicador final en el desarrollo de la educación en línea, pues las diferentes metodologías y tecnologías actualmente están implicando más áreas en su aplicación.

- Es importante recalcar en el papel que juega el profesor para el desarrollo y aplicación de los Objetos de Aprendizaje puesto que su conocimiento permite que éstos se generen alrededor de un contexto pedagógico capaz de desarrollar las competencias cognitivas en el estudiante.

- El estudiante como eje central de las metodologías de aprendizaje propuestas, se debe estimular para que los objetivos que desde un comienzo fueron propuestos se cumplan.

RECOMENDACIONES

- Comprometer a los profesores y estudiantes para el correcto desarrollo, aplicación y evaluación de los Objetos de Aprendizaje diseñados por los estudiantes de pregrado para lograr aplicar diferentes metodologías de aprendizaje que permitan un conocimiento empírico y activo.

- Desarrollar Objetos de Aprendizaje para los temas a evolucionar debido a la importancia para el área de Auditoria, Seguridad y Control en Informática que implican, pues son temas en constante actualización y aplicación en el mundo real.

- Animar a los estudiantes de las diferentes escuelas de la universidad, para seguir ampliando el repositorio de Objetos de Aprendizaje de la Universidad para compartirlos y aplicarlos.

- Capacitar a los profesores en el desarrollo de nuevas metodologías de aprendizaje que les permita generar contenidos más atractivos para sus estudiantes.

- Hacer un balance entre, el desarrollo de Sistemas de Gestión de Aprendizaje o la implementación de Sistemas de Gestión de Aprendizaje de libre Licencia listos para aplicar como Moodle.

- En el caso del Sistema de Gestión de Aprendizaje Moodle es importante reconocer los recursos que ofrece para aplicar nuevos O.A. y nuevas características que hagan de éste un Sistema más dinámico y atractivo para los estudiantes.

BIBLIOGRAFÍA

[DUARTE2003] Duarte Duarte, Jakeline. Docente de la Universidad de Antioquia, *AMBIENTES DE APRENDIZAJE UNA APROXIMACIÓN CONCEPTUAL.* Colombia. Revista Iberoamericana de Educación (ISBN: 1681-5653). 2003. [Recurso Electrónico], http://www.rieoei.org/deloslectores/524Duarte.PDF. [Acceso Septiembre 2007].

[CASTRILLÓN2006] Castrillón Ojeda, Carolina. Prototipo Para El Desarrollo De Programas De Especialización Basados En Ambientes Virtuales De Aprendizaje. UIS. Escuela de Ingeniería de Sistemas e Informática. Tesis (posgrado) Año: 2006, págs. 35-36. http://chorlito.uis.edu.co/tesis/2006/119501.pdf. [Acceso Agosto de 2007].

[ACOFI2005] ACOFI- Asociación Colombiana De Facultades De Ingeniería. Marco De Fundamentación Conceptual Especificaciones De Prueba Ecaes Ingeniería De Sistemas Versión 6.0. Julio De 2005. Pág. 22. [Recurso Electrónico].http://200.14.205.63:8080/portalicfes/home_2/rec/arc_4394.pdf Julio de 2007. [Acceso Agosto de 2007].

[RUIZ2006] Valencia Ruiz, Daniel Mauricio. HERRAMIENTAS DE APRENDIZAJE ACTIVO EN LAS ASIGNATURAS DE INGENIERÍA ESTRUCTURAL. Pontificia Universidad Javeriana. 2006. 25 pp. Recurso electrónico. http://redalyc.uaemex.mx/redalyc/pdf/477/47710106.pdf. [Acceso Septiembre de 2007].

[PEÑA2006] UIS. Proyecto "Soporte Al Proceso Educativo Uis Mediante Tecnologías De Información Y Comunicación – ProSPETIC"-Resumen Ejecutivo. Bucaramanga, 2006. [Recurso Electrónico]. 16 pp. http://eia.udg.es/~clarenes/docs/ResumenProsPETIC.pdf. [Acceso Agosto 2007].

[CARO2003] Caro Spinel, Silvia, Reyes Ortiz, Juan Carlos. PRÁCTICAS DOCENTES QUE PROMUEVEN EL APRENDIZAJE ACTIVO EN INGENIERÍA CIVIL. Universidad de los Andes, Bogotá, Colombia. http://revistaing.uniandes.edu.co/pdf/Rev18-7.pdf. [Acceso Septiembre de 2007].

[TIBANÁ] Tibaná, H Gerardo. ADAPTACIÓN DEL DISEÑO INSTRUCCIONAL EN LA CONSTRUCCIÓN DE AMBIENTES VIRTUALES DE APRENDIZAJE: CASO UNIVERSIDAD DE LOS ANDES. 2003. pp. 10.

[Recurso Electrónico]. http://ava.uniandes.edu.co/avaUploads/adminUploads/TIBANA_DisenoInstruccionalUniandes.pdf. [Acceso Octubre de 2007].

[CRUZ2006] Estrada, Cruz Nicolás. DISEÑO INSTRUCCIONAL BASADO EN COMPETENCIAS MEDIADO POR TICs. PARA LA ASIGNATURA ANÁLISIS NUMÉRICO I DEL PROGRAMA ACADÉMICO DE LA EISI, UIS. 2006. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2006/121775.pdf . [Acceso Octubre de 2007].

[LIZCANO2006] Lizcano Reyes, Rafael Neftalí. Es- Ava: Ambiente Virtual De Aprendizaje De Soporte A La Educación Superior, UIS. Escuela de Ingeniería de Sistemas e Informática. Tesis (posgrado) Año: 2006. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2006/119969.pdf. [Acceso Septiembre de 2007].

[VÁSQUEZ2006] Serrano Vásquez, Rafael Enrique. La Multimedia Como Estrategia De Enseñanza En La Construcción De Competencias Cognitivas, Procedimentales y Actitudinales En Anestesiología, UIS. Centro para el Desarrollo de la Docencia en la UIS - CEDEDUIS. Tesis (posgrado) Año: 2006. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2006/120890.pdf. [Acceso Agosto de 2007].

[VALDIVIESO] Valdivieso Villamizar, José Luis. Módulo Básico De Apoyo A La Enseñanza De La Lógica Borrosa Soportado En Un SGA Como Estrategia De Formación, UIS. Escuela de Ingeniería de Sistemas e Informática. Tesis (pregrado) Año: 2007. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2007/122581.pdf. [Acceso Noviembre de 2007].

[ANGULO] Angulo Mendoza, Omar Argemiro. Módulo De Apoyo Al Aprendizaje De Los Conceptos De Derivación E Integración Contextualizados En La Temática De Física “Cinemática De La Partícula”, Soportado en el SGA Moodle, UIS. Escuela de Ingeniería de Sistemas e Informática. Tesis (pregrado) Año: 2006. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2006/121774.pdf. [Acceso Noviembre de 2007].

[MENDOZA2003] Mendoza Becerra, Martha Eliana. Ambiente Computacional Para El Aprendizaje Cooperativo Basado En El Método Jigsaw, UIS. Escuela de Ingeniería de Sistemas e Informática. Tesis (pregrado) Año: 2003. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2003/112559.pdf. [Acceso Noviembre de 2007].

[FERNÁNDEZ1999] Tejada Fernández, José. Documento publicado en dos artículos de la **Revista Herramientas**, *Acerca de las competencias profesionales* (I), núm. 56 (pp. 20-30) y *Acerca de las competencias profesionales* (II) 57 (8-14) .1999. http://dewey.uab.es/pmarques/dioe/competencias.pdf. [Acceso Noviembre de 2007].

[SUÁREZ2005] Suárez Arroyo, Benjamín. La formación en competencias: un desafío para la educación superior del futuro. Barcelona, 2005. [Recurso electrónico] http://www.mec.es/universidades/eees/files/LaFormacionCompetencias.pdf [Acceso Agosto de 2007].

[BARBOSA2006] Barbosa H, Juan Carlos. Diplomado en Formulación de Proyectos de Virtualización. Colombia. Universidad Javeriana. 2006. [Recurso electrónico]. http://recursostic.javeriana.edu.co/multiblogs/ava.php [Acceso Agosto de 2007].

[ZAPATA2003] Zapata Ros, Miguel. Sistemas de gestión del aprendizaje – Plataformas de Teleformación. 2003. [Recurso Electrónico]. http://www.um.es/ead/red/9/eval_SGA_1.pdf. [Acceso Septiembre de 2007].

[TRÍAS2004] Trías, Fernanda. Las Tecnologías de la Información y la Comunicación en la formación docente. UNESCO. Francia. 2004. 243 pp. [Recurso electrónico] http://unesdoc.unesco.org/images/0012/001295/129533s.pdf. [Acceso Noviembre de 2007].

[CGCB2006] Equipo de trabajo coordinador del CGCB. *ORIENTACIONES CURRICULARES PARA UN CGCB EN CARRERAS DE INGENIERÍA*. Proyecto de Mejoramiento de la Enseñanza de la Ingeniería Facultad de Ingeniería, Universidad Nacional de Cuyo-*Argentina.* 2006-2008. http://www.fing.uncu.edu.ar/catedras/archivos/cgcb/orientaciones.pdf. [Acceso Agosto de 2007].

[ORTIZ2005] Ortiz Prada, Lyda Zugelly. Propuesta de un Sistema para el Desarrollo del Plan de Contingencias de Tecnologías de Información en las Organizaciones, UIS. Tesis (pregrado) Año: 2005. [Recurso electrónico]. http://chorlito.uis.edu.co/tesis/2005/118040.pdf.[Acceso Septiembre de 2007].

[0] Página Web oficial del SGA Moodle. [Recurso Electrónico] http://www.moodle.org. [Acceso Agosto de 2007].

[1] Página Web del grupo de Investigación de la UIS – STI. [Recurso Electrónico] http://www.gruposti.org. [Acceso Enero de 2008].

[2] Página Web que presenta el modelo COBIT. [Recurso electrónico]. http://www.siu.edu.ar/infosiu/&edicion=5&nota=36[Acceso Septiembre de 2007].

[3] Departamento de Informática, Ingeniería del Software II. Universidad de Oviedo, España. Auditoria de Sistemas de Información, http://di002.edv.uniovi.es/~sevilla/is2/AuditoriaSI.pdf. [Acceso Septiembre de 2007].

[4] Página Web que presenta un curso de Auditoria en México. [Recurso electrónico]. http://www.auditoria.com.mx/descarga/ASI%20SvcCursos.pdf. [Acceso Septiembre de 2007].

[5] Página Web que presenta la Auditoria en Cuba. [Recurso electrónico]. www.alfa-redi.org/rdi-articulo.shtml?x=6958. [Acceso Septiembre de 2007].

[6] Página Web que presenta la Auditoria en Chile [Recurso Electrónico] http://www.eici.ucm.cl/Academicos/ygomez/descargas/Aud_Seg_Sist/programa2005auditoria.doc. [Acceso Septiembre de 2007].

[7] Página Web que presenta programa de Riesgo Tecnológico en la Icesi – Colombia. [Recurso Electrónico] http://www.icesi.edu.co/esn/contenido_programas.jsp?id=icesi3educc20. [Acceso Septiembre de 2007].

[8] Página Web que presenta programa de Auditoria en la Eafit - Colombia. [Recurso Electrónico].http://www.eafit.edu.co/EafitCn/Administracion/Posgrados/AuditoriaSistemas/Index.htm Agosto de 2007. [Acceso en Septiembre de 2007].

[9] Página Web que presenta programa de Seguridad de la Información en la Uniandes - Colombia. [Recurso Electrónico] http://sistemas.uniandes.edu.co/manager.php?id=899. [Acceso en Septiembre de 2007].

[10] Página Web que presenta programa de Auditoria en la Unipiloto - Colombia. [Recurso Electrónico] http://www.unipiloto.edu.co/index.php?section=199. [Acceso Septiembre de 2007].

[11] Página Web que presenta programa de Seguridad en la Pontificia Bucaramanga - Colombia. [Recurso Electrónico] http://www.upbbga.edu.co/programas/diplo_seginfo/seginfo.html. [Acceso Septiembre de 2007].

[12] Página Web que presenta el marco general referente a las pruebas ECAES. [Recurso Electrónico] http://www.icfes.gov.co. [Acceso Septiembre de 2007].

[13] Página Web que presenta el plan de área de Ingeniería de Sistemas en la UIS [Recurso Electrónico] http://cormoran.uis.edu.co/eisi/eisi.jsp?IdServicio=S100. [Acceso Septiembre de 2007].

[14] Página Web que presenta los aspectos técnicos del estándar SCORM. [Recurso Electrónico]. dokeos.e-abc.com.ar/courses/EABC020/document/Elearning_Review/ScormTec.ppt?cidReq=EABC020[Acceso Septiembre de 2007].

[15] Página oficial de la Oficina del Aprendizaje Distribuido Avanzado. [Recurso electrónico]. http://www.adlnet.gov. [Acceso Septiembre de 2007].

[16] Página Web que presenta un Manual de buenas prácticas para desarrollo de OA. [Recurso electrónico]. http://www.aproa.cl/1116/articles-68370_recurso_1.pdf. [Acceso Septiembre de 2007].

[17] Página Web que presenta un documento relacionado al tema de OA. [Recurso electrónico]. http://www.cudi.edu.mx/primavera_2004/presentaciones/Lourdes_Galeana.pdf. [Acceso Septiembre de 2007].

[18] Página Web de la ACIS relacionada al tema de Inseguridad Informática. [Recurso electrónico]. http://www.acis.org.co/archivosAcis/Inseguridad.doc. [Acceso Septiembre de 2007].

[19] Página Web que presenta un documento sobre la Seguridad en Redes. [Recurso electrónico]. http://www.pwc.com/uy/spa/pdf/SeguridadRedesInternas.pdf. [Acceso Septiembre de 2007].

[20] Página Web que presenta un documento sobre Riesgos de Información desde el puesto de Trabajo. [Recurso electrónico].

http://www.robotiker.com/castellano/noticias/eventos_pdf/49/Jose_Francisco_Ruiz.pdf. [Acceso Septiembre de 2007].

[21] Página Web sobre el estudio de Virus Informático. [Recurso electrónico]. http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml. [Acceso Septiembre de 2007].

[22] Página Web de la ACIS relacionada al tema de Informática Forense. [Recurso electrónico]. http://www.acis.org.co/fileadmin/Revista_96/dos.pdf. [Acceso Septiembre de 2007].

[23] Página Web que presenta artículo relacionado al Peritaje Informático. [Recurso electrónico]. http://www.alfa-redi.org/ar-dnt-documento.shtml?x=728. [Acceso en Septiembre de 2007].

[24] Página Web que presenta documento del tema Esteganografía. [Recurso electrónico]. http://www.hpn-sec.net/death/articles/int_esteg/Estega.pdf. [Acceso Septiembre de 2007].

[25] Rodríguez Vega, JORGE. Superutilidades – Hackers. Biblioteca UIS. MC. Graw. Hill. Primera edición. 721 pp. 2003.

Ávila de Barón, CECILIA. PKI – Infraestructura de Claves Públicas. Biblioteca UIS. MC. Graw. Hill. 511 pp. 2002.

[26] Página Web que presenta documento relacionado al uso de Mapas Conceptuales. [Recurso electrónico]. cmc.ihmc.us/cmc2006Papers/cmc2006-p249.pdf. [Acceso Octubre de 2007].

[27] Página Web que presenta documento relacionado al tema UML. [Recurso Electrónico] http://www.infomanuales.com/Manuales/UML/UML.asp. [Acceso Diciembre de 2007].

ANEXOS

Anexo A. FORMATO DE ENCUESTA I y II

Formato de las encuestas aplicadas a los estudiantes de AS y CI del I semestre de 2007.

I ENCUESTA INDICADOR DISPOSICIÓN HACIA LA ASIGNATURA SEGURIDAD INFORMÁTICA
AS y CI I SEMESTRE 2007

NOMBRE: _____ ***FECHA:***

Elija y responda según sus preconceptos. Si elige NS/NR debe dar un por qué de su respuesta.

ESPECÍFICOS

¿Utiliza el término "seguridad"? SI ☐ NO ☐ NS/NR ☐

¿En qué o para

¿Hay grupos de investigación de Seguridad Informática en la UIS? SI ☐ NO ☐ NS/NR ☐

¿Cuáles?

¿Es segura la red en TICS de la UIS? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿Ha vulnerado la seguridad de una página web? SI ☐ NO ☐ NS/NR ☐

¿Cómo?

¿Las empresas colombianas invierten en seguridad informática? SI ☐ NO ☐ NS/NR ☐

¿Conoce alguna?

¿Por qué eligió esta asignatura?

¿La asignatura hasta ahora ha respondido a sus expectativas? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿Qué quitaría o agregaría a la asignatura?

I ENCUESTA INDICADOR GUSTO A LA LECTURA
AS y CI I SEMESTRE 2017

NOMBRE: _____ **FECHA:**

Elija y responda según sus preconceptos. SI elige NS/NR debe dar un por qué de su respuesta.

GENERALES

¿Busca solución a sus problemas académicos? SI ☐ NO ☐ NS/NR ☐

¿Cómo?

¿Fue fácil para usted aprender a leer? SI ☐ NO ☐ NS/NR ☐

¿Cómo aprendió?

De 1 a 10 califique su disposición para leer ___

¿Por qué?

¿Experimenta diferentes tipos de lectura? SI ☐ NO ☐ NS/NR ☐

¿Cuáles?

¿Por qué?

¿Aprende cuando lee? SI ☐ NO ☐ NS/NR ☐

¿Cómo?

¿Asume actitud crítica ante la información recibida? SI ☐ NO ☐ NS/NR ☐

¿Cómo?

¿Revisa los escritos después de leerlos? SI ☐ NO ☐ NS/NR ☐

¿Para qué?

¿Maneja diferentes fuentes de información? SI ☐ NO ☐ NS/NR ☐

¿Cuáles?

II ENCUESTA - INDICADOR CONOCIMIENTO TICs DE LA UIS
AS y CI I SEMESTRE 2007

NOMBRE: _____ **FECHA: 12 de junio de 2007**

Elija y responda según sus preconceptos. Si elige NS/NR debe dar un por qué de su respuesta.

¿Conoce el término "Tecnologías de la Información y la Comunicación" -TICs? SI ☐ NO ☐ NS/NR ☐

¿Para qué son?

¿Maneja las TICs de la UIS? SI ☐ NO ☐ NS/NR ☐

¿En qué tipo de actividades?

¿Genera la UIS suficiente publicidad para incentivar el uso de sus TICS? SI ☐ NO ☐ NS/NR ☐

¿Cómo mejoraría?

¿Usted aprovecha las TICs en clase de Seguridad? SI ☐ NO ☐ NS/NR ☐

¿Cómo?

¿Usa correctamente el profesor las TICs de Seguridad Informática? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿Son suficientes las TICs ofrecidas en el CENTIC? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿Se podría generar más demanda de las TICS del CENTIC? SI ☐ NO ☐ NS/NR ☐

¿Cómo?

¿Agregaría o quitaría algo en el CENTIC? SI ☐ NO ☐ NS/NR ☐

¿Qué?

II ENCUESTA - INDICADOR NOCIONES SOBRE APRENDIZAJE EN LÍNEA

¿Sabe qué es el aprendizaje en línea? SI ☐ NO ☐ NS/NR ☐

¿Lo usa actualmente?

¿Es el aprendizaje en línea un aporte a su aprendizaje personal? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿Alguna vez había utilizado el aprendizaje en línea en la UIS, antes de ver la asignatura de Seguridad? SI ☐ NO ☐ NS/NR ☐

¿Cuándo?

¿Estimula el aprendizaje en línea su pensamiento crítico? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿La plataforma Moodle de Seguridad aprovecha el aprendizaje en línea? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿El profesor facilita a sus estudiantes la participación activa en el aprendizaje en línea? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

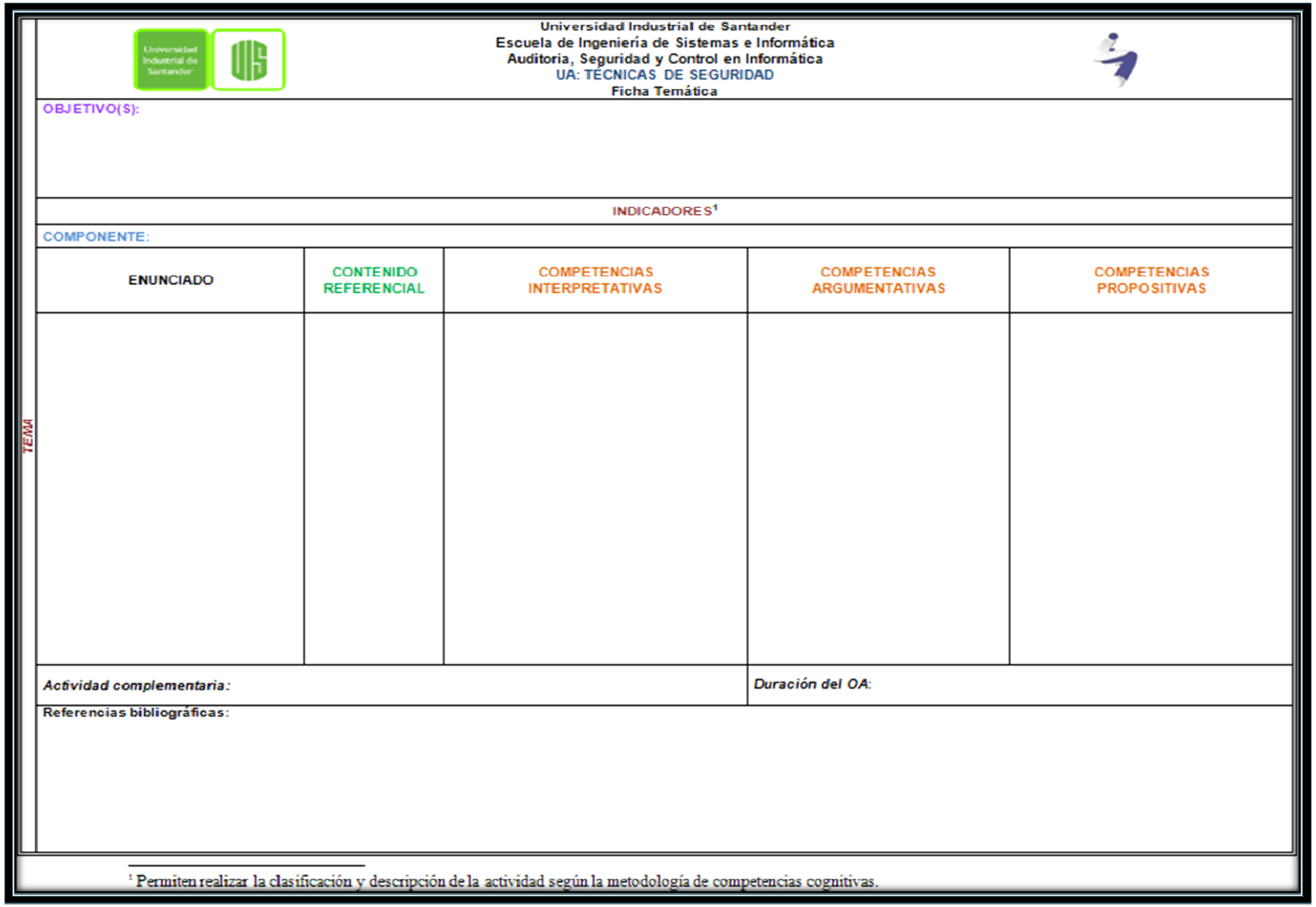
¿Es importante el aprendizaje en línea de los estudiantes de Seguridad? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

¿Prefiere el aprendizaje en línea al presencial? SI ☐ NO ☐ NS/NR ☐

¿Por qué?

Anexo B. Plantilla de Ficha Temática



Universidad Industrial de Santander
Escuela de Ingeniería de Sistemas e Informática
Auditoria, Seguridad y Control en Informática
UA: TECNICAS DE SEGURIDAD
Ficha Temática

OBJETIVO(S):

INDICADORES[1]

COMPONENTE:

TEMA

ENUNCIADO	CONTENIDO REFERENCIAL	COMPETENCIAS INTERPRETATIVAS	COMPETENCIAS ARGUMENTATIVAS	COMPETENCIAS PROPOSITIVAS

Actividad complementaria:	*Duración del OA:*

Referencias bibliográficas:

[1] Permiten realizar la clasificación y descripción de la actividad según la metodología de competencias cognitivas.

Anexo C. Formato Elaboración Preguntas ECAES 2007

CIUDAD	Bucaramanga
FECHA	Enero de 2007
INSTITUCIÓN	Universidad Industrial de Santander
NOMBRE AUTOR	Luis Carlos Gómez Florez

CONTEXTO (SITUACIÓN DE LA CUAL SE DESPRENDEN TRES O MAS PREGUNTAS, TENIENDO EN CUENTA QUE PARA CADA PREGUNTA SE DILIGENCIA UN FORMATO APARTE)

PREGUNTA No. _____

INDICADOR	DESCRIPCIÓN
COMPONENTE:	
ÁREA DE FORMACIÓN:	
COMPETENCIA:	Interpretativa/Argumentativa/Propositiva
CONTENIDO REFERENCIAL:	
NIVEL DE COMPLEJIDAD:	

ENUNCIADO (Adjuntar gráficas si es necesario)

OPCIONES DE RESPUESTA
A.
B.
C.
D.

CLAVE:

PERTINENCIA DE ESTA PREGUNTA EN EL ECAES

JUSTIFICACIÓN DE LA OPCIÓN VALIDA O CLAVE; PROCESO DE SOLUCIÓN, DESDE SU CLASIFICACIÓN EN COMPONENTE, CONTENIDO REFERENCIAL Y COMPETENCIA.

JUSTIFICACIÓN OTRAS OPCIONES