UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
SISTEMA DE UNIVERSIDAD VIRTUAL

“Diseño de un objeto de aprendizaje para evaluar competencias específicas del Módulo I del Diplomado en Seguridad Informática impartido por la Universidad Politécnica de Pachuca”

Proyecto terminal de carácter profesional que para obtener el grado de:

MAESTRÍA EN TECNOLOGÍA EDUCATIVA

Presenta:

RUBÍ YURIANA BAUTISTA GARCÍA

Directora del Proyecto Terminal:

MTE Elsa Martínez Olmedo

Pachuca de Soto, Hidalgo, Enero 2015.

SISTEMA DE UNIVERSIDAD VIRTUAL
DE LA UAEH

Acta de revisión

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
Dirección del Sistema de Universidad Virtual

I.S.C. Rubí Yuriana Bautista García,
Candidata a Maestra en Tecnología Educativa.
P R E S E N T E:

Por este conducto le comunico el jurado que le fue asignado a su Proyecto Terminal de Carácter Profesional denominado: "Diseño de un objeto de aprendizaje para evaluar competencias específicas del Módulo I del Diplomado en Seguridad Informática impartido por la Universidad Politécnica de Pachuca", con el cual obtendrá el Grado de Maestra en Tecnología Educativa y que después de revisarlo, han decidido autorizar la impresión del mismo, hechas las correcciones que fueron acordadas.

A continuación se anotan las firmas de conformidad de los integrantes del jurado:

PRESIDENTE:	M.E. FERNANDO GUTIERRREZ ASCENCIO.
PRIMER VOCAL:	M.T.E. ELSA MARTÍNEZ OLMEDO.
SECRETARIO:	M.D.V.MARÍA ISABEL MORALES ISLAS.
SUPLENTE 1:	M.T.E. CITLALI RAMOS BAÑOS.
SUPLENTE 2:	M.A. LUCINA MONZALVO SERRANO.

Sin otro asunto en particular, reitero a usted la seguridad de mi atenta consideración.

A T E N T A M E N T E
"AMOR, ORDEN Y PROGRESO"
Pachuca, Hgo., a 25 de noviembre de 2014.

Mtra. Alejandra Hernández Silva.
Coordinadora de la Maestría en Tecnología Educativa

Torres Politécnicas S/N
Carretera Pachuca-Actopan Km 1+500, Col. La Loma
Pachuca de Soto, Hidalgo, México, C.P. 42184
Teléfono: 52 01 77 2 71 73 00 Ext. 5000
info@uaeh.edu.mx

www.uaeh.edu.mx

DEDICATORIA

A Dios,

Por acompañarme y guiarme a lo largo de mi vida,
además de darme siempre la fortaleza espiritual y física.

A Moctezuma, mi padre,

Por enseñarme que jamás debo darme por vencida,
siempre estarás en mi corazón…

In memoriam

A Irma, mi madre,

Por enseñarme a soñar y cumplir cada sueño juntas,
por tu apoyo absoluto y fe en mí,
más que mi madre mi amiga incondicional…Gracias!

A Jorge, mi esposo,

Por tu apoyo constante, paciencia y confianza en mí,
por ser mi compañero de camino…Por siempre!

A Nenetl, mi hija,

Eres mi mayor tesoro que Dios me dio,
cada triunfo es de ambas… Te amo!

A todos ustedes les dedico este producto de un esfuerzo conjunto.

Rubí Yuriana Bautista García

AGRADECIMIENTOS

Gracias a mi madre por compartir conmigo desde pequeña el amor a la educación, por enseñarme a amar esta profesión y acompañarme siempre en el camino de mi vida.

A mi familia principalmente le reconozco todo ese tiempo que me permitieron dedicarle a este sueño, por consecuencia me perdí de muchos acontecimientos familiares, gracias por su constante apoyo, cariño y perseverancia a lo largo de todo este tiempo.

Gracias a mi maestra Elsa Martínez Olmedo, mi directora de tesis, por su valiosa orientación, tolerancia, apoyo, consejos y ánimo que me brindó en todo el proceso desde el comienzo hasta su culminación. Un merecido reconocimiento hacia usted por ayudarme a levantar cada vez que me derrumbaba, gracias por confiar en mí, sin su apoyo no hubiera sido posible este proyecto.

Agradezco a todas aquellas personas que tuvieron hacia mi paciencia y respeto por cada momento de arranque, ira, irritación, desesperación y arrebato en este proceso, debido a la saturación de actividades que disfruto.

A la Universidad Politécnica de Pachuca que me permitió realizar mi investigación y mi proyecto.

Gracias

Rubí Yuriana Bautista García

ÍNDICE

RELACIÓN DE TABLAS, DIAGRAMAS Y FIGURAS

TABLAS

DIAGRAMAS

FIGURAS

FORMATOS

RELACIÓN DE ANEXOS

SIGLARIO

ANUIES: Asociación Nacional de Universidades e Instituciones Superiores.

CEDyTE: Coordinación de Educación a Distancia y Tecnología.

DESECO: Definition and selection of competencies.

DRAE: Diccionario de la Real Academia Española.

EBC: Educación Basada en Competencias.

FODA: Fortalezas, Oportunidades, debilidades y amenazas.

MSU: Montana State University

OA: Objeto de aprendizaje.

UPP: Universidad Politécnica de Pachuca.

RESUMEN

Los estudiantes hoy en día necesitan desarrollar habilidades, destrezas y conocimientos, para aprovechar la efectividad y eficacia de la era de Información. La alfabetización informacional y tecnológica son componentes fundamentales para las competencias laborales, profesionales y personales; de una manera significativa es el éxito académico y el incremento de oportunidades hacia los estudiantes. Tomando esto como referencia, la Coordinación de Educación a Distancia y Tecnología (CEDyTE) forma parte de la Universidad Politécnica de Pachuca (UPP) universo donde se elaborará la investigación de este proyecto; se propone el diseño de un objeto de aprendizaje para evaluar las competencias adquiridas del Módulo I del Diplomado en Seguridad Informática, modalidad virtual. En la fase de diseño del objeto de aprendizaje se utilizará el modelo instruccional Análisis, Diseño, Desarrollo, Implementación y Evaluación (ADDIE) el cual permitirá tener una estructura lógica y funcional en la elaboración de cada uno de los apartados del objeto de aprendizaje, suele parecer muy sencillo porque solo hay que llevar a cabo cinco pasos en concreto pero cada uno lleva su propio análisis incluyendo todos los aspectos que giran alrededor de esté. Para la fase de investigación y análisis de datos, se plantea un método cualitativo, mediante un diseño de investigación de estudio de caso, utilizando como instrumento cuestionarios para la recolección de datos oportunos sobre la evaluación por competencias.

Logrando como resultado un objeto de aprendizaje diseñado mediante la herramienta Dreamweaver, para su fácil acceso y operabilidad de este en cualquier arquitectura de hardware o software. La orientación del objeto de aprendizaje es la estimación de diferentes habilidades, destrezas y competencias que cumple el participante específicamente del Módulo I el Diplomado, esto conlleva a que los participantes tengan un mejor desarrollo profesional o simplemente pueda reforzar las competencias que no ha logrado desarrollar aún.

Palabras Claves: *Competencias, Evaluación de competencias, Modalidad Virtual, Objeto de Aprendizaje, Seguridad Informática.*

ABSTRACT

Students today need to develop skills, abilities and knowledge to leverage the effectiveness and efficiency of the era of information. The informational and technological literacy are key components for industrial, professional and personal skills; in a meaningful way is academic success and increased opportunities to students. Taking this as a reference, the Coordination of Distance Education and Technology (CEDyTE) is part of the Polytechnic University of Pachuca (UPP) universe where research of this project will be developed; the design of a learning object is proposed to evaluate the skills acquired Module I of the Diploma in Computer Security, virtual mode. In the design phase of the learning object model instructional Analysis, Design, Development, Implementation and Evaluation (ADDIE) which will enable a logical and functional structure in the development of each of the sections of the learning object is used, usually sounds simple because only out five steps to bring on concrete but each carries its own analysis including all aspects revolving around is. For the phase of research and data analysis, a qualitative method is proposed by a research design case study using questionnaires as a tool to collect timely data on skills assessment.

Achieving results in a learning object designed by Dreamweaver tool for easy access and operability of this at any hardware or software architecture. The orientation of the learning object is to estimate different abilities, skills and competencies that meets the participant specifically Diploma Module I, this entails that participants have a better professional development or just can strengthen the powers has failed to develop further.

Keywords: *Competencies, skills assessment, Virtual mode, learning object, Computer Security*.

CAPÍTULO I. PLANTEAMIENTO DEL PROYECTO

I.1 Presentación

El presente proyecto titulado: "*Diseño de un objeto de aprendizaje para evaluar competencias específicas del Módulo I del Diplomado en Seguridad Informática impartido por la Universidad Politécnica de Pachuca".*

La Coordinación de Educación a Distancia y Tecnología (CEDyTE) de la Universidad Politécnica de Pachuca (UPP) cuenta con una oferta educativa de diplomados únicamente orientados a la capacitación de los participantes y se ambiciona obtener diplomados con valor curricular por lo que se necesita evaluar realmente las competencias específicas de dicho diplomado para que puedan aplicarlas los participantes de manera eficiente en su vida laboral.

Dentro de la oferta, se encuentra el Diplomado en Seguridad Informática, que consta de 6 Módulos y cuyo objetivo es dirigir a los participantes a desarrollar competencias en Seguridad Informática. Sin embargo, no se cuenta con un instrumento para evaluar las competencias adquiridas en el diplomado, por lo que se propone el desarrollo de un objeto de aprendizaje pare evaluar competencias; con la finalidad de que los participantes conozcan los alcances de las competencias adquiridas en el diplomado.

El estudio se basa en la línea 1 de ***Investigación Evaluativa en modalidades alternativas a la presencial,*** la cual comprende el análisis, enfoque y tendencias teórico – prácticas encaminadas a la propuesta de modelos de evaluación de la calidad de programas educativos virtuales, mixtos o presenciales con apoyo de TIC; 2ª opción de ***Propuesta de mejora, con diseño e instrumentación del proyecto de forma parcial.***

En el Capítulo I se aborda el planteamiento del proyecto identificando las áreas con problema y la aplicación que tendrá, antecedentes del Diplomado en la CEDyTE, justificación de la elaboración del objeto de aprendizaje para la evaluación de competencias. De igual forma encontraremos los objetivos generales y específicos; y por último las metas a las que se quiere llegar para resolver la problemática encontrada.

En el capítulo II se construye una visión del marco teórico que sustenta la investigación. Se presentan algunas reflexiones en torno a los temas tratados en el proyecto, aportes teóricos y conceptuales, experiencias formales sobre los objetos de aprendizaje, competencias y evaluación de estas.

El Capítulo III describe el fundamento teórico de competencias y su estructura, evaluación y evaluación por competencias en entornos virtuales; así como el diseño de un objeto de aprendizaje para pasar posteriormente al diseño instruccional ADDIE el cual es utilizado para el desarrollo del objeto de aprendizaje donde se desarrollan las unidades evaluativas.

En el Capítulo IV se expone el producto elaborado para darle solución a la problemática del proyecto. El Objeto de Aprendizaje (OA) está constituido por 18 actividades que evaluarán cada una de las 5 unidades que integran el Módulo I, diseñando los objetivos y estrategias pedagógicas de cada unidad y el desarrollo de los contenidos serán parte del objeto de aprendizaje.

El último Capítulo V se presenta las experiencias adquiridas en el desarrollo del objeto de aprendizaje, así como las conclusiones de la investigación.

I.2 Diagnóstico

Hoy en día la necesidad de que los estudiantes tengan una educación integral y de calidad es de suma importancia, por tal motivo se pretende que el alumno cuente con las habilidades y competencias necesarias poder tomar decisiones en su vida profesional y laboral.

La Universidad Politécnica de Pachuca (UPP) se encuentra ubicada en el municipio de Zempoala, Hidalgo, a 20 minutos de la Ciudad de Pachuca, actualmente cuenta con la Coordinación de Educación a Distancia y Tecnología la cual tiene como propósito desarrollar oferta educativa de capacitación en la modalidad a distancia, basados en prácticas de vanguardia pedagógica y tecnológica, acorde a las exigencias del mundo globalizado, así como proyectos de investigación en el área de Tecnología Educativa.

Brinda diferentes opciones de oferta educativa enfocadas a las necesidades, expectativas y demandas de la sociedad en general, y particular de la UPP, como los son los diplomados en línea de:

- Diplomado en Innovación de Medios
- Diplomado en Seguridad Informática.

El Diplomado en Seguridad Informática en modalidad virtual tiene como propósito proveer una visión de cómo las TIC pueden ser herramientas del cambio hacia la innovación de la función pública y apoyar el desarrollo de la sociedad de la información; conjuntamente propiciar una reflexión sobre la importancia de la Seguridad Informática en el sector público.

La CEDyTE forma parte de la UPP y expone la propuesta de desarrollar un objeto de aprendizaje para evaluar competencias del Módulo I del Diplomado en Seguridad Informática; debido a la carencia que existe de materiales educativos que apoyen a la evaluación por competencias profesionales; los resultados de la evaluación confirmarán las competencias adquiridas por el participante al término del Diplomado; al mismo tiempo dicha coordinación ambiciona que el Diplomado cuente con un valor curricular para el participante.

La coordinación a distancia solicita a la autora de este proyecto terminal elaborar una adaptación de evaluación por competencias que permita la reflexión formativa y sea posible relacionarlo a otros Diplomados similares.

Aunque esto no es tan simple, ya que conocimientos y competencias no son dominios contrarios o excluyentes, se tendría que hablar de transferencias y conocimientos que amplíen la competencia para la práctica profesional.

El propósito del instrumento de evaluación es asegurar que los estudiantes logren las competencias exigidas al nivel de calidad requerido del Módulo I.

Para determinar las necesidades y las acciones a desarrollar, se aplicaron dos cuestionarios. El cuestionario número 1 se aplicó a los alumnos próximos a egresar de la carrera de Ingeniería en Software y el cuestionario número 2 a la Coordinadora a Distancia. Dichos instrumentos servirán principalmente para apoyar la realización del diagnóstico y reunir algunos de los datos necesarios acerca de las Fortalezas, Oportunidades, Debilidades

y Amenazas para la elaboración de la matriz de FODA, que se complementará con cuestionarios a directivos, docentes y alumnos para recabar opiniones y experiencias.

Otro objetivo de los instrumentos es recabar la información sobre las competencias que poseen los alumnos sobre Seguridad Informática. Se determinó la aplicación de estos cuestionarios a estudiantes de Ingeniera en Software próximos a egresar; ya que en su momento cursaron una materia con valor curricular en su ingeniería denominada Seguridad Informática que les ayudó a desarrollar algunas competencias sobre el tema.

El cuestionario número 1 se aplicó de forma presencial a la muestra de 6 alumnos de una población de 30, dicho cuestionario cuenta con 4 preguntas en total (Véase Anexo 1), de las cuales 3 son preguntas abiertas sobre la opinión de cada uno de los alumnos sobre la realización de evaluación por competencias, así como su importancia en el Diplomado en Seguridad Informática y una pregunta más de opción múltiple la cual contiene 5 competencias específicas de Seguridad Informática que creen poseer los estudiantes. La finalidad del instrumento es saber el interés e importancia que tienen los alumnos sobre las evaluaciones por competencias; además de las competencias específicas que tienen sobre seguridad informática.

Los resultados arrojados del cuestionario número 1, 4 eran varones y 2 mujeres (Véase Anexo 1 tabla.1), indica que 4 alumnos “No” han realizado una evaluación por competencias y más de 3 alumnos creen tener competencias específicas en Seguridad Informática, no obstante el 100% de los alumnos afirman la importancia de desarrollar competencias para el desarrollo en particular de sistemas de información seguros. Un aspecto muy interesante es que el 100% de los alumnos piensan sobre la importancia de realizar evaluaciones por competencias es necesaria y trascendental para comprobar o demostrar el porcentaje de competencia que ha desarrollado; además de ser una pauta para buscar nuevas técnicas e impulsar sus habilidades.

A la coordinadora de la CEDyTE se aplica el cuestionario número 2 con la finalidad de indagar a fondo la problemática, el cuestionario lo integran por 4 preguntas abiertas (Véase Anexo 2) sobre la importancia de la evaluación por competencias, técnicas efectivas y evidencias de la evaluación de competencias. Se identificó que los profesores de cada módulo les cuesta trabajo evaluar por competencias debido a que es muy diferente la evaluación por conocimiento; la importancia de realizar una evaluación por competencias en

el diplomado ya que representa para quien participe en el poner en práctica sus habilidades, destrezas y competencias, bajos ciertos criterios donde demuestren conocimientos suficientes; es importante evidenciar las competencias adquiridas de los participantes mediante actividades de aprendizaje y evaluación.

Después de recabar la información pertinente a los cuestionarios, se logra conformar una matriz FODA la cual es enriquecida con base en la observación de la autora de esta investigación en tres rubros esenciales institución, docencia y alumnos, estructurando lo que se muestra en la Tabla 1.

Tabla 1

Matriz FODA

	Fortalezas	**Debilidades**
	Institución • Se cuenta con el apoyo de las autoridades de la CEDyTE para la realización del objeto de aprendizaje. • Se cuenta con la infraestructura suficiente para su diseño e implementación del objeto de aprendizaje. **Docencia** • La experta en Seguridad Informática que apoyará en el desarrollo del objeto de aprendizaje es la autora de la investigación y también tiene conocimiento sobre la Educación Basada en Competencias. **Alumnos** • Los alumnos están dispuestos a realizar evaluaciones por competencias debido a la importancia que tiene ser competentes en su vida profesional.	**Institución** • No ha desarrollado anteriormente una evaluación sólida por competencias. **Docencia** • Las evaluaciones que actualmente se realizan son sencillas y únicamente evalúan los conocimientos teóricos adquiridos. **Alumnos** • Los alumnos no cuentan con una evaluación que les permita estimar las competencias en el Módulo I del Diplomado de Seguridad Informática.
Oportunidades	**Estrategias para el logro de objetivos FO**	**Estrategias para el logro de objetivos DO**
Institución • Creación de un Objeto de aprendizaje para evaluar competencias del Módulo I del Diplomado en Seguridad Informática. • La CEDyTE al ser parte de la UPP,	Debido al gran apoyo con el que se cuenta por parte de las autoridades de la institución y la infraestructura tecnológica con la que se cuenta, se pretende realizar el objeto de aprendizaje	Elaboración de un objeto de aprendizaje mediante el modelo ADDIE que tendrá como propósito evaluar competencias; además que se diseñarán cada una de las

por ende se basa en una Educación Basada en Competencias. • La CEDyTE implementará el Diplomado por tercera vez en el mes de septiembre. **Docencia** • La creatividad de la autora que funge como experta en Seguridad Informática, es una alternativa para generar un objeto de aprendizaje interesante y atractivo para los alumnos. **Alumnos** • Facilitará a los alumnos la implementación de las competencias de los participantes en su vida profesional. • Permitirá mejorar el desempeño de los egresados del Diplomado de Seguridad Informática. • Los participantes tendrán una estimación sobre las competencias específicas	en un software compatible para cualquier tipo de recurso que se pueda adicionar al objeto de aprendizaje y sea atractivo para el participante del diplomado.	actividades de evaluación en base a la Taxonomía de Marzano lo cual permitirá evaluar en ciertos casos hasta el nivel 4, por ende los alumnos tendrán una evaluación que es permita estimar sus competencias y se verá reflejado en su vida profesional.
Amenazas **Institución** • La evaluación por competencias en un Objeto de Aprendizaje puede ser desarrollada por otras instituciones antes que ésta; lo cual representará prestigio para las otras instituciones y un atraso en la búsqueda de esta institución. • El tiempo establecido para la elaboración del objeto de aprendizaje sea limitado para concluirlo. **Docencia** • Los asesores encargados del seguimiento virtual al Módulo I no implementen de forma adecuada el objeto de aprendizaje; o que no le den la importancia necesaria al objeto de aprendizaje. **Alumnos** • Limitaciones por parte de los participantes en cuanto a sentirse competentes para la seguridad informática. • Debido a la situación económica los alumnos no se inscriban al Diplomado o deserten.	**Estrategias para el logro de objetivos FA** El objeto de aprendizaje dará a conocer al participante al término de cada evaluación el tema que necesita retroalimentación para poder evitar la sensación de incompetencias en algún aspecto de la seguridad informática.	**Estrategias para el logro de objetivos DA** La implementación del objeto de aprendizaje será en base a los lineamientos que debe cumplir dentro de la CEDyTE, lo cual permitirá su creación en el menor tiempo posible, además de que dicho objeto de aprendizaje apoyará a los alumnos con una estimación de las competencias en el Módulo I y evitará la sensación de incompetencia respecto del tema.

Nota: Fuente: Elaboración propia (2014)

A partir de recabar información de las autoridades y alumnos, así como de la elaboración de la Matriz FODA, se identifica la necesidad de contar con un instrumento de evaluación

acorde a los objetivos del diplomado, que en resumen, se encamina a desarrollar competencias informáticas en los alumnos, por lo que el objeto de aprendizaje se visualiza de forma integrada al proceso de aprendizaje y acorde a los temas abordados. El objeto de aprendizaje apoyará el proceso de evaluación en el diplomado una vez que sea aprobado debido a que permitirá a los docentes y participantes estimar sus competencias informáticas; alcanzadas; retroalimentando el tema evaluado de acuerdo al nivel logrado.

I.3 Planteamiento del problema

En el mundo laboral donde se ponen a prueba todos los conocimientos, aptitudes y actitudes de los alumnos, se manifiesta la realidad de estos como es la inexperiencia e incompetencia en aquellas habilidades que no supieron que tenían flaquezas o bien que por desinterés no intentaron el desarrollo de estas competencias al máximo.

En un Diplomado tan práctico como lo es Seguridad Informática es de suma importancia que los egresados muestren su competitividad para generar sistemas de información o sistemas informativos inmunes a cualquier ataque y puedan preservar la integridad de dichos sistemas.

El problema identificado se encuentra en la impartición del Diplomado virtual en Seguridad Informática ya que el modelo de evaluación actual no corresponde a una evaluación por competencias en un entorno virtual; por tal motivo se expone la propuesta de desarrollo de un objeto de aprendizaje para evaluar las competencias del Módulo I del Diplomado en Seguridad Informática; debido a la carencia que existe de materiales educativos que apoyen a la evaluación por competencias profesionales.

Para entender un poco mejor la descripción del problema es necesario hacer una pausa, para poder definir una competencia, Tobón *et al.* (2010) define la competencia como las

> "…actuaciones integrales ante actividades y problemas del contexto, con idoneidad y compromiso ético, integrando el saber ser, el saber hacer y el saber conocer en una perspectiva de mejora continua" (p.11).

En el siguiente Diagrama 1 se muestra un árbol de problemas para poder entender la problemática a resolver:

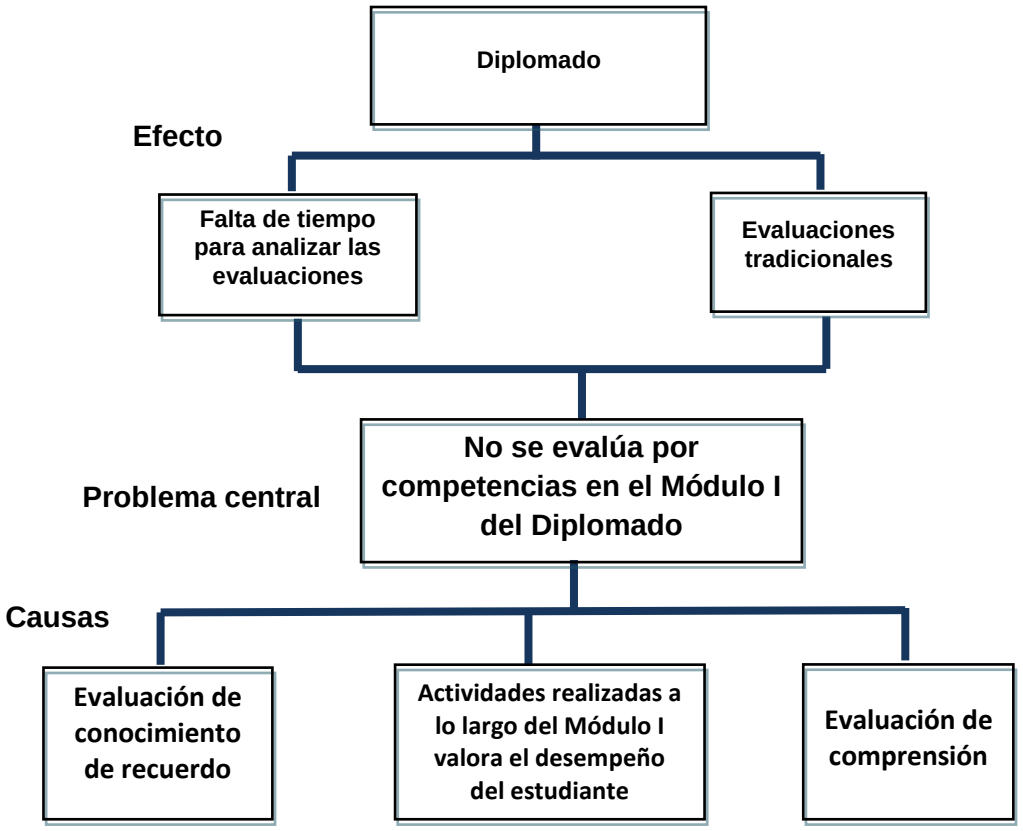


Diagrama 1: Árbol de problemas.
Fuente: Elaboración propia (2014)

El problema central y grave del diplomado es la carencia de una evaluación por competencias del Módulo I del Diplomado en Seguridad Informática; la consecuencia de la falta de análisis en las evaluaciones de un Diplomado y realizar evaluaciones tradicionales, provocan únicamente una estimación cuantitativa de conocimientos y no de competencias lo cual impide al participante conocer una valoración concreta sobre las competencias que adquieren en el Módulo I del Diplomado en Seguridad Informática.

I.4 Antecedentes

Características generales de la CEDyTE

La CEDyTE se encuentra en las Instalaciones de la Universidad Politécnica de Pachuca con domicilio en Carretera Pachuca – Cd. Sahagún, km. 20, Ex – Hacienda de Santa Bárbara Municipio de Zempoala, Estado de Hidalgo.

La CEDyTE fue creada para cubrir de manera virtual las necesidades laborales o profesionales de cualquier individuo; a continuación se explica su:

Misión

> "La Coordinación de Educación a Distancia y Tecnología Educativa tiene como misión el diseño de proyectos de investigación, servicios y materiales educativos, enfocados a las necesidades, expectativas y demandas de la sociedad en general, y en particular, de la comunidad Universitaria de la Universidad Politécnica de Pachuca." (Intranet UPP, 2013)

Visión

> "Ser una Coordinación de Educación a Distancia y Tecnología Educativa líder en el diseño de proyectos de investigación, servicios y materiales educativos, con fundamento teórico y tecnológico de vanguardia, bajo un esquema de pertinencia, congruencia y calidad para ser competente con instituciones de su tipo de corte local, estatal, nacional e internacional." (Intranet UPP, 2013)

Objetivo

> "Desarrollar servicios de formación y capacitación en las modalidades de educación presencial, semi-presencial y virtual, basados en prácticas de vanguardia pedagógica y tecnológica, acorde a las exigencias del mundo globalizado, así como proyectos de investigación en el área de Tecnología Educativa." (Intranet UPP, 2013)

Funciones

> "Introducir a los participantes en las actividades de capacitación, entrenamiento y especialización orientados a la modalidad a distancia.

> Gestionar, organizar y administrar eventos y servicios de capacitación, entrenamiento y especialización en tecnología educativa. Desarrollar proyectos de investigación en tecnología educativa.” (Intranet UPP, 2013)

Cabe mencionar que actualmente no se ha ofertado ningún diplomado virtual en lo que llevamos del año debido a que se están haciendo modificaciones y actualizaciones a la información que contiene en cada uno de los diplomados; se pretende tener todo listo a partir del tercer cuatrimestre del 2014 para poder empezar a abrir las inscripciones.

Antecedentes del Diplomado de Seguridad en Informática

La CEDyTE cuenta con una oferta educativa en modalidad virtual, de diversos cursos de capacitación para personal que se encuentra laborando en diferentes aéreas laborales; el cual podemos encontrar el Diplomado de Seguridad en Informática.

El propósito de Diplomado de Seguridad en Informática es:

> “Proveer una visión de cómo las TIC pueden ser herramientas del cambio hacia la innovación de la función pública y apoyar el desarrollo de la sociedad de la información; conjuntamente propiciar una reflexión sobre la importancia de la Seguridad Informática en el sector público” (Intranet UPP, 2013).

Los alumnos que participan en el Diplomado, realizan evaluaciones dentro del proceso, pero únicamente es la estimación de sus conocimientos, pero la parte más interesante es que no cuentan con las competencias ni objetivos esperados por estas, únicamente muestran el contenido a evaluar y piden trabajos muy sencillos, del nivel de conocimiento de recuerdo, si es que nos basamos en la taxonomía de Marzano. Esta situación no garantiza en que los alumnos cuenten con las competencias para desarrollarse en el campo laboral ni profesional.

Por esta razón, se considera en este diplomado la necesidad de mejorar el proceso de evaluación del Diplomado en Seguridad Informática, en específico del Módulo I, para poder integrar los diferentes niveles de la Taxonomía de Marzano el cual apoyará de manera significativa la adquisición y el desarrollo de las competencias profesionales de los

participantes en cada uno de las unidades que integran el Módulo. Esto conlleva a que el estudiante tenga que buscar nuevas técnicas de estudio e impulso de competencias, para que puedan demostrarlas en su vida diaria.

El OA a desarrollar estará promoviendo una evaluación por competencias de modo que a los informáticos les es familiar el uso de dicho instrumento de evaluación, conjuntamente se aplicará la integración de pedagogía con tecnología, esta evaluación será para los alumnos una oportunidad de demostrar que han alcanzado las competencias específicas del Módulo I del Diplomado.

I.5 Justificación

La CEDyTE de la UPP requiere aplicar una metodología de evaluación coherente con la metodología de enseñanza y las competencias a desarrollar por los alumnos participantes del Módulo I, del Diplomado en Seguridad Informática ofertado por tercera ocasión.

La evaluación tradicional que se realiza en el Diplomado en Seguridad Informática es valorar las actividades de las unidades de cada módulo y la apreciación que únicamente arrojan dichas actividades con base en la Taxonomía de Marzano es a nivel 1 que implica conocimiento de recuerdo y la comprensión correspondiente al nivel 2.

Por tal motivo no se están obteniendo resultados certeros donde se asegure la competitividad laboral lograda en cada Módulo por el estudiante, por tal motivo se busca mejorar el proceso de evaluación del Diplomado con ayuda del diseño de un OA que autoevalúe en el nivel de **análisis** y/o **utilización** es decir niveles 3 y 4.

Las estrategias que se seguirán para el diseño e implementación del proyecto son:

1. Diseñar e implementar el objeto de aprendizaje a partir de sustentarlo en el uso de la tecnología para la evaluación de competencias específicas del Módulo I.
2. El diseño del objeto de aprendizaje será realizado bajo las metodologías para diseño y creación de objetos de aprendizaje.
3. La evaluación de las competencias tendrá como fundamento teorías y prácticas relevantes de instituciones prestigiadas y de investigaciones realizadas.

4. La autora de este proyecto es la experta en el tema y además la persona que desarrollará el objeto de aprendizaje, esto es una ventaja porque se podrá aminorar los riesgos que se presenten para evadir los tiempos reducidos que existen para la elaboración del proyecto.

El evaluar las competencias de los participantes del Diplomado, apoyarán en las siguientes características a cada uno de ellos, tal como lo menciona Yániz *et al.* (2006, p.3):

- Requiere que los alumnos actúen de manera eficaz ante cualquier situación que se les enfrente en base al conocimiento adquirido.
- Supone para el alumnado la realización de un amplio rango de tareas importantes para el desarrollo de competencias.
- Las tareas propuestas suponen retos estructurados y funciones que ayudan a los alumnos a ensayar para la realidad compleja de la vida adulta y profesional.

De acuerdo con los autores Yániz *et al.* (2006):

> Para lograr este tipo de juicios sobre la competencia se deben seguir tres principios:
>
> - Usar los métodos de evaluación más adecuados para evaluar la competencia de manera integrada. La competencia incluye habilidades, actitudes y conocimientos.
>
> Los métodos integrados evalúan una cantidad de elementos de competencia con sus criterios de desempeño.
>
> - Seleccionar los métodos que sean más directos y relevantes para aquello que está siendo evaluado. A veces se requiere la utilización de varios métodos.
> - Usar una amplia base de evidencias para inferir la competencia.
>
> El enfoque de evaluación basado en competencias enfatiza el desempeño, exige una mayor variedad de evidencia que los enfoques tradicionales y busca

> métodos de evaluación directa, asumiendo los principios y pautas de lo que debe ser una evaluación (p.3).

En el Diplomado en Seguridad Informática se requiere efectuar una evaluación por competencias para tener un sentido formativo e integral en el Módulo I, la alternativa es la elaboración de un OA el cual comprende diferentes características las cuales beneficiarán a la evaluación entre ellas podemos mencionar es una pieza digital, independiente, reutilizable además de ser aplicable en sistemas de gestión del conocimiento con el propósito de ser reutilizado en diferentes contextos y plataformas para el intercambio de contenidos, es decir será reusado en el resto de los Módulos del diplomado de acuerdo a las competencias específicas que coincidan en cada Módulo.

Por lo tanto la CEDyTE de la UPP se apoyará en el diseño de un objeto aprendizaje que regule el aprendizaje de los estudiantes y demuestre con evidencias que puede realizar las tareas de la competencia exigidas:

Al completar el Módulo I, el alumno será capaz de:

- **Aplicar** el concepto de Seguridad Informática para identificar la eficiencia de modelos, tipos de control de acceso, autentificación de datos, ataques a sistemas informáticos, para garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

La intención es demostrar las competencias profesionales adquiridas por los alumnos en el Módulo I. El autor García (2008), menciona que se evaluarán los conocimientos, las actitudes, habilidades y los desempeños involucrados en el dominio de una competencia, es decir para este proyecto será durante el proceso de aprendizaje del Módulo I del Diplomado. Específicamente es la estimación de los 4 pilares de la educación (UNESCO) aprender a conocer, aprender a hacer, aprender a vivir juntos y aprender a ser; en el siguiente apartado se explica la forma de evaluación.

Además de evaluar los procesos mentales de los estudiantes en base al Sistema de Cognición que propone la Taxonomía de Marzano, se pretende alcanzar el nivel de **análisis** en donde se relaciona, clasifica, analiza, generaliza o identifica el conocimiento o el de

utilización en donde se aplica en conocimiento para la toma de decisiones, resolución de problemas, investigación experimental o investigación.

Con la conjunción de los elementos anteriormente mencionados se evaluarán las competencias y el nivel del proceso mental del estudiante, demostrando y evidenciando que el estudiante ha cumplido con las competencias y capacidades necesarias para poder acreditar el Módulo I del Diplomado en Seguridad Informática, para dar parte a la formación de ciudadanos libres de pensamiento, de acción y gestores de su propia educación.

El impacto que se logrará con la aplicación del instrumento de evaluación para el estudiante es:

- Conocer el nivel de aprendizaje alcanzado.
- Motivar y estimular al estudiante.
- Realizar un trabajo continuo y no un ejercicio aislado.
- Promover el análisis de los aprendizajes.
- Adaptar sus propias estrategias didácticas para mejorar el proceso de aprendizaje y aumentar sus logros.
- Actitud reflexiva.
- Desarrolla el pensamiento creativo y productivo.
- Experto del Módulo I Introducción a la Seguridad Informática y al Aseguramiento de Información.
- Por parte del facilitador podrá valorar el grado de las competencias que ha desarrollado el participante.

El instrumento de evaluación por competencias es una herramienta que apoyará al CEDyTE de la UPP en el Módulo I del Diplomado en Seguridad en Informática; permitirá valorar el grado de competencias que ha adquirido el participante.

El proyecto que se persigue es el desarrollo de un OA que permita evaluar las competencias de los participantes del Diplomado en Seguridad Informática que estén cursando el Módulo I; ya que no se cuenta con una evaluación que estime las competencias específicas del Diplomado.

La propuesta está dirigida para alumnos inscritos en el Diplomado en Seguridad Informática, aunque cabe destacar que al ser un OA y una de sus características es la reusabilidad, también estará disponible para alumnos de la Ingeniería en Software y Telemática que cursen la materia de Seguridad Informática.

I.6 Objetivos

I.6.1 Objetivo general

Diseñar un objeto de aprendizaje para evaluar las competencias adquiridas del Módulo I del Diplomado en Seguridad Informática modalidad virtual.

I.6.2 Objetivos específicos

- Identificar las necesidades de evaluación por competencias en el Módulo I del Diplomado en Seguridad Informática.
- Determinar los contenidos del objetivo de aprendizaje para la evaluación de competencias en el Módulo I del Diplomado en Seguridad Informática, así como las secuencias, actividades y productos que evidencien el nivel de competencia logrado.
- Evaluar si el objeto de aprendizaje permite la evaluación efectiva de las competencias y arroja resultados confiables.
- Expresar la forma de desarrollar el instrumento de evaluación por competencias en modalidad virtual del Módulo I.

- Proponer un objeto de aprendizaje para validar las habilidades de los participantes del Módulo I Introducción a la Seguridad Informática y al Aseguramiento de Información del Diplomado en Seguridad Informática.

I.7 Metas

Diseñar un OA para la evaluación de competencias adquiridas en las 5 unidades que conforman el Módulo I del Diplomado en Seguridad Informática modalidad virtual, para abril de 2015 y tener un avance del 40% para enero de 2015.

CAPÍTULO II. FUNDAMENTO TEÓRICO

En este capítulo se construye una visión del marco teórico que sustenta la investigación. Se presentan algunas reflexiones en torno a los temas tratados en el proyecto, aportes teóricos y conceptuales, experiencias formales sobre los objetos de aprendizaje, competencias y su evaluación.

II.1 Conceptos Básicos

Competencia Informática

La definición del término competencia informática es un concepto difícil de explicar, es "familiarizarse con el ordenador" (Bork, 1986), "aprender sobre los ordenadores" (Gros, 1987) y así podemos encontrar infinidad de conceptos sobre la competencia, conforme avanzo la tecnología se complementa el concepto, mencionando que es la interacción que tiene un sujeto con la PC para poder cubrir sus objetivos personales con algún software específico como lo afirma Tello (2003) de la Universidad de Murcia (2011).

Es decir, son un conjunto de habilidades, conocimientos y actitudes que adquiere un individuo para conocer las aplicaciones de las TIC y lograr los objetivos específicos de cada individuo, como lo argumenta CRUE-TIC y REBIUN (2009) (Universidad de Murcia, 2011).

Seguridad Informática

La seguridad informática ha tenido un gran auge en los últimos tiempos debido a las cambiantes y nuevas tecnologías de información y comunicación (TIC). Es por eso que el término de Seguridad Informática tiene sus inicios en la década de los 80 por Robert Morris debido a que escribió un programa capaz de infectar todo lo que estuviera a su paso, es decir el primer gusano de la historia Worm; en el 2005, un hacker logro obtener un listado de más de 40 millones de tarjetas de crédito, lo cual repercutía en tener con seguridad toda la información. (Marco 2008), *Hermoso et al. (2011).*

Por esta razón nace la necesidad de resguardar la información, Hermoso *et al.* (2011) define como seguridad la acción de proteger los recursos inestimables de los posibles peligros y ataques cometidos por agentes no autorizados. La seguridad Informática tiene como propósito proteger los recursos de un sistema informático como lo es la información, servicios y arquitecturas.

Alonso (2002) define seguridad informática del Diccionario de la Real Academia Española (DRAE), 22 edición (2001), como Seguridad como la cualidad de seguro es decir asegura un buen funcionamiento, e Información como la adquisición de conocimiento que permita ampliar o precisar sobre una materia determinada y por ultimo Protección es resguardar alguna cosa, persona o información de un peligro o perjuicio.

Ramió (2006) en su libro denominado *Electrónico de Seguridad Informática y Criptografía* define a la Seguridad Informática como un conjunto de herramientas y métodos destinados para la protección y salvaguardia de la información ante cualquier amenaza.

Después de revisar diversos autores se concluye que la Seguridad Informática invariablemente tendrá un gran auge debido a los cambios constantes que existen en la tecnología ya que continuamente se tiene la necesidad de resguardar la información y su buen funcionamiento para la seguridad ante cualquier tipo de amenaza física o lógica del sistema de información o informático.

II.2. Competencias

La definición de “competencia” es muy extenso y complejo que diversos autores han tratado de expresar de la manera más sencilla; entre ellos tenemos a Moreno (2012) que define “competencia” como un concepto polisémico y difícil de entender, las competencias se asimilan y se construyen en el tiempo, no son algo dado, innato y estable.

El proyecto Definition and Selection of Competencies (DESECO) (2000 y 2005), el cual menciona en su publicación Moreno (2012), concluye que:

> “Una competencia es más que el dominio de conocimientos y habilidades. Ésta incluye la capacidad para satisfacer demandas complejas, poniendo y movilizando recursos psicosociales; por ejemplo, la capacidad para comunicarse efectivamente es una competencia que podría extraer del individuo un conocimiento del lenguaje, habilidades prácticas de informática y actitudes hacia aquellos con los que se comunica” (p. 6).

La autora Frade (2009) en su obra Planeación por competencias, define a las competencias como la:

> “Capacidad adaptativa, cognitiva y conductual para responder adecuadamente a las demandas que se presentan en el entorno. Es un saber pensar para poder hacer frente a lo que se necesita” (p.26).

Por otra parte Tobón *et al.* (2010) define la competencia como las acciones integrales ante cualquier actividad o problema en diversos contextos, con idoneidad y compromiso ético, integrando el saber ser, el saber hacer y el saber conocer en un enfoque de mejora continua.

En resumen, definimos una competencia como la capacidad cognitiva, adaptativa y conductal, es decir el dominio de conocimientos y habilidades; para solventar las exigencias de problemas o situaciones en diversos contextos.

¿Cuáles son las bases de una competencia? Una competencia se basa en los conocimientos adquiridos previamente, Moreno, (2012) así lo menciona en su documento “*La evaluación de competencias en educación*”.

De acuerdo al cuestionamiento anterior, surgen más cuestionamientos como; ¿Por qué los conocimientos son parte esencial de la competencia?, encaminemos este cuestionamiento a un ejemplo real, concretando que si un individuo no conoce los saberes sobre algún tema en particular, por ende no tendrá la capacidad de usarlos y se concluye que es un individuo incompetente en el tema o situación en particular.

Ahora veremos el otro lado, sí el individuo posee los saberes, tiene la capacidad para utilizarlos, es decir, “aprende a hacer”, además se percata del por qué y hacia donde llegará

que significa que “aprende a conocer”. A partir de aprender hacer y aprender a conocer a identificar sus alcances y limitaciones se deduce que el individuo es competente, “aprender a ser”.

El término de competente lo consolida Morales (2013) en su publicación *Desarrollo de competencias a través de objetos de aprendizaje*; citando a Monereo (2007) cuando:

> “considera que ser competente no es sólo ser hábil en la ejecución de tareas y actividades concretas…., sino más allá de ello, ser capaz de afrontar, a partir de las habilidades adquiridas, nuevas tareas o retos que supongan ir más allá de lo ya aprendido”. (p.3)

Por otra parte el concepto de competente yuxtapone el mejoramiento de diversas capacidades, ingenios, habilidades y destrezas específicas como lo son las actitudinales, sociales, cognitivas, motoras, etc.

De acuerdo a los autores anteriores se concluye que una competencia cuenta con los elementos que se muestran en la Tabla 2.

Tabla 2

Elementos de la competencia

COMPETENCIAS		
Aprendizajes esperados	Estrategias formativas	Criterios de evaluación
• Cognitivos • Procedimentales • Actitudinales	• Métodos	Evidencias de: • Conocimientos • Desempeño • Producto

Nota: Fuente: Elaboración propia (2014)

II.2.1 Estructura de una competencia

Las competencias se usan para rastrear información acerca del conocimiento, habilidades y destrezas que las personas adquieren en el desempeño de una actividad o en la participación de eventos de formación o capacitación. La determinación de si se ha alcanzado la competencia implica evaluar los resultados para establecer si la persona ha adquirido los conocimientos, habilidades o destrezas que se supone una experiencia de aprendizaje debería de proporcionar.

Partiendo del hecho de que la evaluación de una competencia no necesariamente arroja resultados cuantitativos medibles ya que pueden ser la mayor parte del tiempo aspectos subjetivos no susceptibles de medición, la evaluación puede ser a través de la observación, como cuando se miden las habilidades para operar una máquina excavadora, la habilidad para resolver problemas laborales en una organización, el uso del formato American Psychological Association (APA) en la redacción de documentos académicos, aplicación de ciertos niveles de seguridad informática en los procedimientos de almacenamiento de información al interior de una organización.

Cada institución u organismo si se piensa en un nivel macro, y hasta en un ambiente micro como el aula en donde un profesor evalúa ensayos de sus alumnos, tienen un modo distinto para evaluar las competencias adquiridas. En este OA se parte de la noción de que si una competencia se construye para medir objetivos de aprendizaje, estos se van alcanzando a través de la realización de actividades individuales asociadas al objetivo que permiten ir alcanzando uno a uno de esos objetivos para luego integrarlos en una competencia. Es decir, una competencia no se alcanza directamente de manera completa sino a través del logro de objetivos que finalmente la integran (Frade, 2013).

La estructura de una competencia, para tener posibilidades de evaluarse, puede estructurarse como la Universidad de Montana en Estados Unidos, propone en esta institución el desarrollo de un ambiente de aprendizaje al que ha nombrado “Desire to Learn” (D2L), en el que analiza las estructuras de competencias como sigue:

En primer lugar, establece que para crear la estructura completa, se deben crear los elementos que conforman la estructura y la asociación entre estos elementos. De acuerdo a

esta institución, la relación es padre-hijo, en donde el objetivo de aprendizaje es el padre y las actividades son el hijo; la propuesta la muestra la Tabla 3.

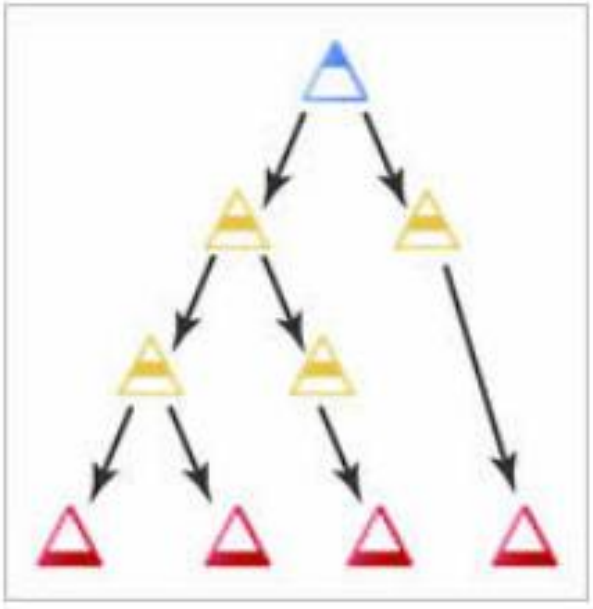
Tabla 3
Relación entre objetivos de aprendizaje y actividades.

Elemento	Padres	Hijos
Competencia	Objetivos de aprendizaje	Actividades de aprendizaje
Objetivos de aprendizaje	Competencias	Actividades
Actividades	Objetivos de aprendizaje	Actividades

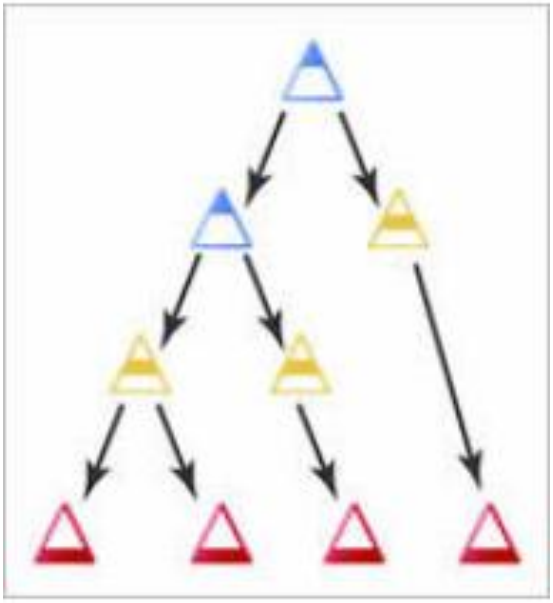
Nota: Fuente: Montana State University (2014)

En esta propuesta, se distingue como la competencia se estructura con varios componentes que se planean por separado pero pensando en su integralidad. En la siguiente figura, proponen la estructura que llaman “estructura anidada” en la se anidan las competencias y los objetivos de aprendizaje agregando la asociación padre-hijo entre las competencias o entre los objetivos de aprendizaje. La idea general es que si se tiene un objetivo de aprendizaje muy amplio en su alcance, se divida en varios objetivos más simples y se les anide, lo que permite al usuario lograr el objetivo amplio a través de completar los más pequeños, como se muestra la Tabla 4.

Tabla 4
Objetivo general y su división



En esta figura puede apreciarse cómo el objetivo general se dividió en varios más pequeños y alcanzables y se anidaron ligando la competencia y las actividades.



En esta otra figura, los autores de la propuesta (MSU) que esta estructura se pueden usar para distinguir niveles múltiples de desempeño en donde un usuario puede completar un nivel básico de competencia logrando dos objetivos de aprendizaje, luego, completa un nivel intermedio completando dos objetivos de aprendizaje más.

Nota: Fuente: Montana State University (2014)

La construcción de los objetivos de aprendizaje para lograr las competencias como se mencionó anteriormente, los autores de la MSU la constituyen de la siguiente manera:

1. Seleccionar un Nombre y una descripción.
   Nota: El nombre que se seleccione debe identificar claramente el objetivo de aprendizaje.

2. A demás de puede utilizar un identificador adicional para el objetivo de aprendizaje, se utiliza este campo para referir a un estándar profesional o académico relacionado con el objetivo que aprendizaje.

La estructura fundamental entre los elementos de una competencia, debe contener por lo menos una competencia, un objetivo de aprendizaje y una actividad, como lo indica la Figura 1.

Competencia existente, Objetivo de aprendizaje, o Actividades.

Figura 1: Estructura fundamental de una competencia.
Fuente: Montana State University (2014)

Continuando con la propuesta de MSU, nos menciona que las actividades son los únicos elementos de la estructura de las competencias que pueden ser determinados; se pueden asociar los objetivos de aprendizaje a múltiples actividades o las actividades a un objetivo de aprendizaje

Las actividades que se utilizan actualmente para evaluar el Módulo I del Diplomado en Seguridad Informática no evalúan competencias además que no permiten validar las competencias que el alumno ha adquirido. A continuación se muestran las actividades actuales en el diplomado con la ponderación que tiene dentro del Módulo I:

Actividad	**Ponderación**
Cuestionario de la guía	40%
Mapa conceptual	30%
Cuadro comparativo	30%
	100%

Las actividades carecen de algunos de los saberes: procedimental, saber o el ser, además de que las actividades mencionadas anteriormente no tiene ninguna rubrica en la cual permita ubicar el nivel de competencia del participante.

Se pueden instalar las estructuras flexibles de la capacidad y asociar objetivos que aprenden múltiples a una actividad, o asocie las actividades múltiples a un objetivo que aprende.

Las asociaciones de las actividades con los objetivos de aprendizaje se expresan a continuación:

Asociación solamente (ninguna estimación): Son las actividades que forman parte del objetivo de aprendizaje, pero no requiere de ninguna estimación formal. Esta asociación no tiene ningún impacto en la estructura de la competencia y no afecta en la competencia o evaluaciones objetivas de aprendizaje.

Nota: Si la asociación de la actividad con un objetivo de aprendizaje sin estimación como en este caso, provee a los usuarios de las evaluaciones claras y específicas que generarán las expectativas de objetivos de aprendizaje.

Asociación con rúbrica de estimación: Este tipo de asociaciones de actividades son sí se desea evaluar a los usuarios, se asignan actividades con rúbricas de estimación, esto es útil si se están creando estimaciones de diagnóstico o formativos.

Asociación con rúbrica de estimación y criterio del umbral: Se pueden realizar estas asociaciones de actividades si se desea evaluar a los usuarios y elaborar los requerimientos de evaluación del cumplimiento de la competencia. El umbral es el nivel requerido mínimo de la rúbrica o porcentaje que debe alcanzar en estimación para concluir el objetivo de aprendizaje asociado.

En base a la propuesta de MSU, a continuación se enlistan y describen algunos tipos de actividad que contendrá el objeto de aprendizaje para evaluar el dominio de competencias adquiridas.

Tipos de la actividad

1. **Actividad de quizz:** Las actividades son determinadas por la estimación, el resultado de las preguntas o rúbricas.
2. **Actividad de estudio de situación:** Las actividades del examen son determinadas por una rúbrica. No se pueden asociar actividades anónimas del examen a objetivos que aprenden.
3. **Actividad de buzón:** Las actividades del buzón son determinadas por una rúbrica.
4. **Actividad de la discusión** Las actividades de la discusión son determinadas por una rúbrica.
5. **Actividad de grado:** Las actividades de grado son determinadas por una estimación numérica o una rúbrica.
6. **Actividad de contenido:** Se pueden asociar los módulos y temas de contenido con el objetivo de aprendizaje, pero no se puede valorarlas numéricamente o con rúbrica.
7. **Actividad de estimación manual:** Son actividades que pueden ser como una presentación, un recital de música, horas de servicio comunitario o actividades extracurriculares. Las actividades de estimación manual son determinadas por una rúbrica.

II.3 Evaluación

La evaluación es un punto crucial en el proceso de aprendizaje, los autores Yániz *et al.* (2006), en su publicación *Planificar desde competencias para promover el aprendizaje*, hacen referencia a los autores Cabaní y Carretero (2003) donde "consideran que la evaluación tiene una función reguladora del aprendizaje".

El autor Tobón (2011) en su obra *Evaluación de las competencias en la Educación Básica*, define a la evaluación por objetivos, como la comparación de los aprendizajes de los estudiantes como las metas muy precisas en la enseñanza; es decir es una comparación continua de los resultados en el aprendizaje con los objetivos previamente establecidos de la enseñanza, los cuales son definidos por el docente (p.25)

Zabala *et al.* (2007) define a la evaluación como la dirección de todo el proceso de enseñanza y de aprendizaje, no sólo en los resultados que ha conseguido el alumno, sino a cualquiera de las 3 variables fundamentales que intervienen en el proceso de enseñanza y aprendizaje, es decir, las actividades que promueve el profesorado, las experiencias que realiza el alumno y los contenidos de aprendizaje, ya que las tres son determinantes para el análisis y comprensión de todo lo que sucede en cualquier acción formativa.

Existen diferentes enfoques en la evaluación Yániz *et al.* (2006); cita a Herrington y Herrington (1998) los cuales proponen una evaluación auténtica o alternativa, donde se evalúan los objetivos formativos a través de diversidad de procedimientos; no es más que una evaluación por competencias.

Yániz *et al.* (2006) cita a Wiggins (1990) quien alude algunas características de este enfoque:

- Los conocimientos adquiridos por los alumnos tienen que ser eficaces.
- Las tareas realizadas por los alumnos tiene un rango de importancia para el desarrollo de la competencia.
- Las tareas son desafíos que apoyan a los alumnos para experimentar con la realidad compleja.

Respecto a la evaluación de las competencias en la publicación *Desarrollo de competencias a través de objetos de aprendizaje*; Morales (2013), enumera:

- Las actividades de evaluación, pueden ser utilizados:
    - Glosarios que ayuden a aclarar las definiciones de los conceptos,
    - Cuestionarios para reforzarlos,
    - Mapas conceptuales,
    - Gráficos,
    - Análisis de lecturas,
    - Elaboración de prácticas, etc. (Ibídem.,p.4)

Segovia (2012), hace referencia a los instrumentos de evaluación por competencias específicas, realizando la siguiente relación que muestra la Figura 2.

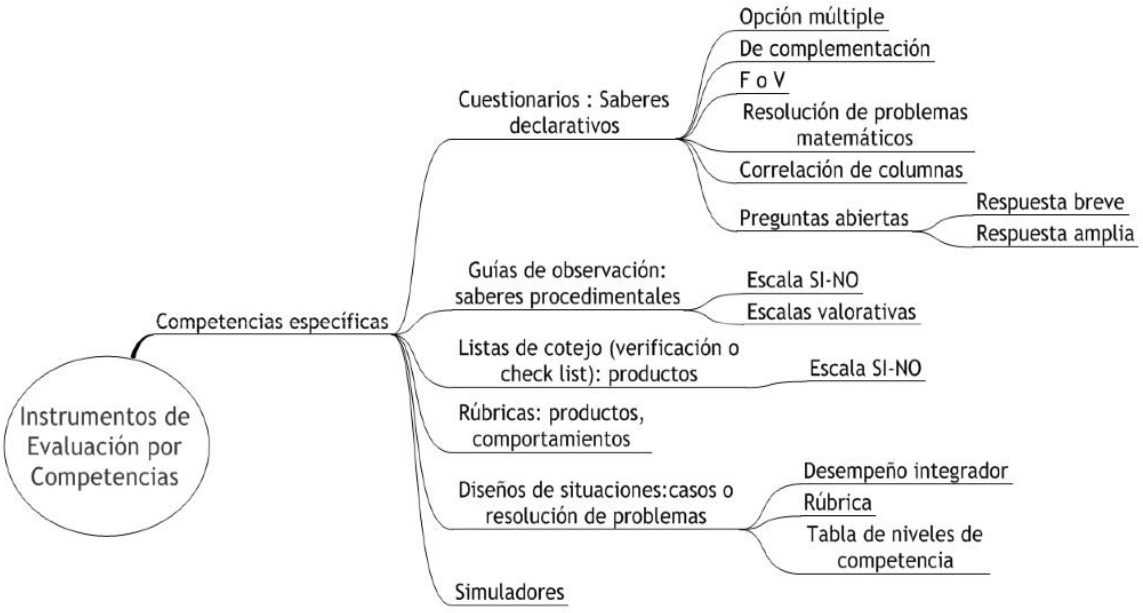


Figura 2: Instrumentos de evaluación por competencias específicas.
Fuente: Segovia (2012)

La propuesta del autor Morales (2013) y Segovia (2012) es congruente con los propósitos de este proyecto, respecto a la evaluación por competencias:

- Competencias específicas,

- Los conocimientos para el desarrollo de las competencias
- Los recursos y actividades que se llevarán a cabo para lograr la competencia
- Las evidencias que permitirán evaluar los desempeños conceptuales, procedimentales y/o actitudinales.

En la figura 3 se muestran las actividades que se desarrollarán en el OA para la estimación de competencias adquiridas por el participante del Módulo I.

Figura 3: Actividades para la evaluación de competencias.
Fuente: Elaboración propia (2014)

II.3.1 Evaluación por competencias en entornos virtuales

Los autores Bazaldua *et al.* (2006), maestros y doctores de diversas Universidades e Institutos en los que podemos mencionar *Instituto de Estudios Superiores de Tamaulipas, Universidad Realística de México, Universidad Simón Bolívar, Universidad de Montemorelos, Instituto Universitario del Estado de México* respectivamente, en su obra *La evaluación de* competencias en la obra *un marco metodológico*; analizan y proponen la siguiente definición:

> La evaluación de competencias es un proceso de recolección de evidencias explícitas sobre el desempeño profesional, laboral o educativo, con el propósito de formarse un juicio a partir de un criterio o referente estandarizado para identificar aquellas áreas

de desempeño que han sido desarrolladas y aquellas que requieren ser fortalecidas (p.3)

Algunas **diferencias** con respecto a la evaluación tradicional de acuerdo con Vargas (2001) son:

- Su base en el juicio “competente” o “aún no competente”.
- Su sustento en evidencias del desempeño real, no en preguntas sobre lo que se sabe.
- Su consideración como un proceso más que un momento (p.4).

Los autores Morales (2013), Yániz *et al.* (2006) y Bazaldua *et al.* (2006) coinciden en el propósito de la evaluación por competencias; es la emisión de un juicio del desempeño que requiere la habilidad de aplicar el conocimiento y a su vez tomar una decisión de utilización del conocimiento; teniendo claro el objetivo de la competencia a evaluar o en su defecto el para qué será se estima, el qué y cómo se realizará.

No existe un método exclusivo para evaluar las competencias, señalan Norman, Watson *et al.* (2002), sino una amplia estrategia de medición que incluye múltiples métodos para asegurar que las personas hayan adquirido el complejo repertorio de conocimientos, habilidades y actitudes que se requieren para demostrar competencias.

Benítez (2006) describe dos de las metodologías más aplicadas para evaluar competencias:

a) **“Las tablas descriptivas**: consisten en párrafos que describen las conductas observables en cada nivel de dominio de la competencia en orden ascendente. Para cada competencia se determina, según el puesto, en qué nivel se debe poseer la competencia y se compara con el nivel en que se ubica al empleado que ocupa dicho puesto.” (p.9)
b) **“Los Indicadores de dominio**: consisten en frases cortas que describen conductas observables y que, en conjunto, permiten evaluar el dominio de la competencia determinando qué nivel tiene la persona en cada uno de todo el conjunto de indicadores. Los niveles son: A (satisface plenamente o supera las exigencias del puesto), B (satisface las exigencias mínimas) o C (requiere entrenamiento formativo

para alcanzar el desempeño requerido). A partir del nivel de cada uno de todos los indicadores de la competencia se asigna una puntuación. Esta se compara con lo esperado y se clasifica la brecha como pequeña, moderada, considerable o critica. La brecha aceptable es menor en competencias importantes para el puesto que en las competencias complementarias." (p.10)

El principio utilizado para la elaboración de los niveles de desempeño e indicadores de dominio tiene como fundamento la propuesta de Benítez (2006) y Segovia (2012) una matriz de doble entrada en la cual se establecen:

- Los niveles de desempeño o indicadores de dominio mínimo indispensable para evaluar si se ha logrado el aprendizaje esperado, deben ser claros y precisos (Segovia 2012), así como establecer para que se va a evaluar y qué se va a evaluar (Bazaldua *et al.,* 2006)
- Segovia (2012) lo define como la escala valorativa con niveles de desempeño; y Bazaldua *et al.* (2006) como los indicadores de dominio donde se describe el nivel en que se encuentra el dominio de la competencia específica.

Tabla 5
Niveles de desempeño o Indicadores de dominio.

A Excelente	Satisface plenamente o supera las exigencias.
B Suficiente	A partir de este nivel se dice que se ha adquirido la competencia. Satisface las exigencias mínimas.
C Insuficiente	Requiere entrenamiento formativo para alcanzar el desempeño requerido

Nota: Fuente: Elaboración propia (2014)

II. 4 Objetos de Aprendizaje

II.4.1 Definición

El desarrollo de recursos educativos es una labor obligada y continua de los docentes. La necesidad de realizar este proceso más eficiente y con apoyo de las aplicaciones Web, emerge una herramienta educativa llamada Objeto de Aprendizaje (OA); la intención es propagar el uso y reutilización de dicho material entre diferentes instituciones o docentes.

La concepción del concepto de Objeto de Aprendizaje ha generado diferentes polémicas de acuerdo a su definición; debido a que el concepto se encuentra en constante cambio y adaptación a las nuevas exigencias tecnológicas y educativas.

La primera idea como lo menciona Chiappe (2007), tiene origen en 1969 por Gerard, quien proponía:

> "Las unidades curriculares se pueden hacer más pequeñas y combinarse de manera estandarizada como piezas de MECCANO, en una gran variedad de programas particulares personalizadas para cada estudiante" (p.1)

Después de 20 años, en 1992, el término de Objeto de Aprendizaje es nombrado por primera vez por Wayne Hodgins mientras realizaba un trabajo sobre estrategias de aprendizaje; observó a sus hijos cuando jugaban con unas piezas de LEGO (Jacobsen, 2002), se percató que era necesario tener una estrategia de aprendizaje interoperable, es decir una estrategia que pueda ser utilizada por diferentes sistemas o materias sin restricción o implementación alguna, a lo que denominó *objeto de aprendizaje*.

Más tarde en el 2000 Wiley, define al objeto de aprendizaje como:

> "Trozos pequeños y reusables de medios instruccionales…cualquier recurso digital que puede ser reutilizado para apoyar el aprendizaje." (Wiley, 2000). (p. 3)

En los años siguientes alcanzó una gran evolución el concepto; diferentes autores realizaron diversas modificaciones, adecuaciones e inclusiones de términos como: *reutilizable, metadatos, aprendizaje, movilidad, información, aprendizaje, interoperabilidad, objetivo, pieza digital…*

La construcción del concepto de objeto de aprendizaje es extenso debido a las particularidades que han incluido diversos autores; Chiappe (2007), reúne diversas definiciones, entre las que se encuentran las siguientes:

> "… consta de una colección de recursos digitales de diversos medios que presenta información" (Dodds, 2001). (p. 3)

> “Un objeto de aprendizaje se define como una “entidad, digital o no digital que puede ser utilizada, reutilizada o referenciada durante el aprendizaje apoyado en tecnología” (IEEE, 2002, p.3)

> “una pieza digital de material de aprendizaje que direcciona a un tema claramente identificable o salida de aprendizaje y que tiene el potencial de ser reutilizado en diferentes contextos” (Mason, Weller, & Pegler, 2003, p.4)

> “una unidad mínima de aprendizaje con sentido pedagógico” (Morales, García, Moreira, Rego, & Berlanga, 2005, p.4)

Con base en los autores mencionados anteriormente, el Objeto de Aprendizaje que se elabora en esta investigación; se define como una “*pieza digital”* así lo menciona Mason *et al*. (2003); el cual apoyará al Diplomado en Seguridad Informática a valorar las competencias del Módulo I. El objeto de aprendizaje tendrá un sentido pedagógico, paralelamente se beneficiará el aprendizaje de los alumnos de la mano con la tecnología.

La Figura 4 representa la definición del objeto de aprendizaje de la investigación:

Figura 4: Concepto de objeto de aprendizaje.
Fuente: Elaboración propia (2014)

II.4.2 Características

Los Objetos de Aprendizaje deberían de cumplir ciertas características o propiedades, como lo menciona Chiappe (2007) en el extracto de los diversos autores que realizó.

Haciendo referencia a esos autores, se establecen las características que puntualizan al Objeto de Aprendizaje que se elaborará en este proyecto, como lo son:

- Movilidad e Interoperabilidad

En 1998, Cisco Systems menciona una característica por la parte tecnológica del desarrollo del OA:

> "realizar avances sobre algunos asuntos relevantes relacionados con los OA (Jacobsen, 2002) sobre todo relacionados con aspectos de tipo tecnológico procurando una refinación del tema en *movilidad*, *interoperabilidad* y automatización." (Cisco Systems, 1998). (p.2)

El Objeto de Aprendizaje a elaborar tendrá la particularidad de ser estable y dinámico para el intercambio entre diferentes instituciones o docentes. A demás de ser un material que podrá ser utilizado en cualquier plataforma educativa y dispositivo de cómputo o móvil.

Reutilizable

Reuso, reusabilidad o reutilización es una capacidad que debe tener un Objeto de Aprendizaje para que pueda ser utilizado en diferentes entornos educativos y temas formativos.

En el 2000 Wiley, afirma que los objetos de aprendizaje son:

> "Trozos pequeños y *reusables* de medios instruccionales…cualquier recurso digital que puede ser reutilizado para apoyar el aprendizaje." (Wiley, 2000). (p. 3)

Al igual la IEEE en el 2002, menciona es una:

> "entidad, digital o no digital que puede ser utilizada, reutilizada o referenciada durante el aprendizaje apoyado en tecnología" (IEEE, 2002). (p. 3)

Mason *et al.,* manifiestan en el 2003 que los objetos de aprendizaje son:

> "una pieza digital de material de aprendizaje que direcciona a un tema claramente identificable o salida de aprendizaje y que tiene el potencial de ser *reutilizado* en diferentes contextos" (Mason, Weller, & Pegler, 2003). (p. 3)

Por último Chiappe en el 2007, señalan que una:

> "entidad digital, autocontenible y *reutilizable*, con un claro propósito educativo, constituido por al menos tres componentes internos editables: contenidos, actividades de aprendizaje y elementos de contextualización. A manera de complemento, los objetos de aprendizaje han de tener una estructura (externa) de información que facilite su identificación, almacenamiento y recuperación: los *metadatos*" (Chiappe 2007). (p. 6)

El OA que se elaborará para el Módulo I del Diplomado en Seguridad Informática modalidad virtual, además tendrá aplicaciones de evaluación en diversas materias, carreras y modalidades.

A continuación se enlistan en la Tabla 6 las asignaturas en las se utilizará el OA para evaluar las competencias y se estará aplicando la propiedad de reuso de dicho objeto.

Tabla 6
Reutilización del objeto de aprendizaje en distintas materias.

Materia	Carrera	Modalidad
Seguridad Informática Redes Análisis de Sistemas Diseño de Sistemas Seguridad y Auditoria Informática	Ingeniería en Software	Presencial
Tópicos selectos de redes Seguridad en Informática Fundamentos de redes Administración de Redes Administración de los Centros de Computo	Ingeniería en Telemática	Presencial

Nota: Fuente: Elaboración propia (2014)

El OA desarrollado dispondrá de la capacidad de ser reutilizado o reusado en cualquier contexto educativo necesario.

- Metadatos

  Otra característica no menos importante es la de metadatos, Hodgins en el 2000, indica que:

  > "una colección de objetos de información ensamblada usando ***metadatos*** para corresponder a las necesidades y personalidad de un aprendiz en particular. Múltiples objetos de aprendizaje pueden ser agrupados en conjuntos más grandes y ***anidados*** entre sí para formar una infinita variedad y tamaños" (Hodgins, 2000). (p. 7)

  Para entender el concepto de metadatos, el Instituto de Ciencias de la Educación de la Universidad Politécnica de Valencia (2007) lo define como:

  > *"una serie de características identificativas o atributos (metadatos) que permitan distinguir el objeto de otros. Puede almacenarse en bases de datos con interacciones entre ellas, por lo que tendrá una información descriptiva que le permitirá ser buscado y encontrado fácilmente*." (Instituto de Ciencias de la Educación, 2007)

Es la información que contienen los Objetos de Aprendizaje, para poder tener una accesibilidad y localización eficiente en el repositorio de Objetos de Aprendizaje donde se encuentre. Es decir una etiqueta que contiene la descripción del objeto.

El OA que se desarrollará tendrá posibilidad de ser *interoperable y movible* para cualquier plataforma o artefacto tecnológico y de esta forma agilizar su intercambio; *la capacidad de ser reutilizable en cualquier otra materia de diversos diplomados o de licenciatura* y *se describirá por medio de metadatos; otras de las características que podemos encontrar en el objeto es su manejo simple, eficaz y comprensible.*

A continuación se muestran las características del OA a desarrollar:

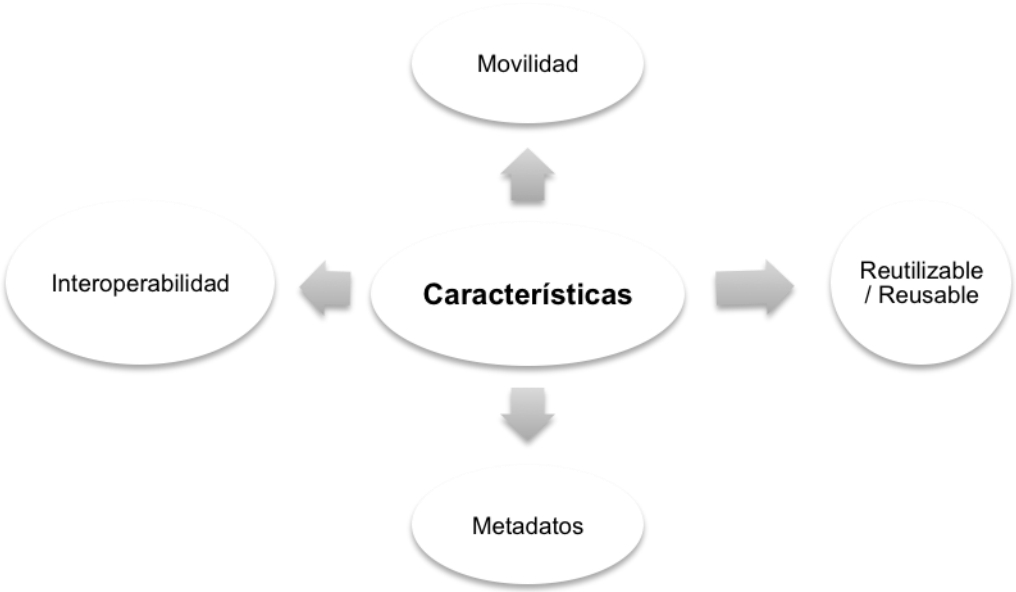


Figura 5: Características del objeto de aprendizaje.
Fuente: Elaboración propia (2014)

II.4.3 Elementos

Los factores que construyen el OA son diversos, entre los cuales podemos encontrar a Cisco (1999) argumenta que deben tener: una *descripción, un resumen y una evaluación*.

Otros autores como Chiappe (2007) sugiere que deben incluir los Objetos de Aprendizaje los siguientes elementos: *contenidos, actividades de aprendizaje y elementos de contextualización*

Recapitulando lo anterior, el OA desarrollado para el Módulo I del Diplomado en Seguridad Informática contendrá los siguientes elementos:

- Objetivos
- Contenidos
- Actividades y evaluaciones.

A continuación se muestran los elementos que incluirá el OA.

Figura 6: Elementos del objeto de aprendizaje.
Fuente: Elaboración propia (2014)

II.4.4 Construcción

En este proyecto se propone el desarrollo de un OA dirigido a determinar el nivel de competencias logradas en el Módulo I del Diplomado en Seguridad Informática.

El Instituto de Ciencias de la Educación de la Universidad Politécnica de Valencia (2007) sugiere para la construcción de un OA, se sigan los pasos siguientes:

- Formular el objetivo general y los específicos
- Determinar los saberes a alcanzar por los estudiantes
- Seleccionar los contenidos
- Desarrollar el objeto de aprendizaje
- Describir los metadatos del objeto
- Diseñar la evaluación

Esta propuesta de construcción de un OA resulta conveniente para su desarrollo, debido a que permitirá generarlo paso a paso desde el desarrollo de los objetivos hasta la elaboración de evaluaciones, incluyendo todos los elementos mencionados con anterioridad.

Se busca aplicar diversas tareas por alumno; las cuales valoraran el nivel de logro de cada una de las competencias a medir; esto como resultado de establecer parámetros de valoración de cada actividad.

A continuación se muestran los pasos para el desarrollo del OA del Módulo I del Diplomado en Seguridad Informática; con fundamento a la propuesta del Instituto de Ciencias de la Educación de la Universidad Politécnica de Valencia (2007):

Tabla 7

Pasos para la construcción de un objeto.

PASOS PARA LA CONSTRUCCIÓN DE UN OBJETO DE APRENDIZAJE			
OBJETIVOS:	CONCEPTUALES **saber qué**	PROCEDIMENTALES **saber cómo**	ACTITUDINALES **saber acerca de**
Determinar qué tipo de objetivo se pretende alcanzar con el OA. Optando por (conceptual, procedimental y/o actitudinal)	Describir, explicar, recordar, analizar, interpretar, resumir, reconocer, comprender y/o aplicar datos y conceptos.	Verificar, configurar, ejecutar, aplicar, diseñar, manejar, utilizar, elaborar, demostrar, planificar, componer… una habilidad a aprender por el alumno.	Superar el desinterés, comprometerse, predisponer a, modificar las actitudes negativas del alumno en diferentes ámbitos.
CONTENIDOS	La selección de contenidos se realizará en función del objetivo anterior, es decir si se ha optado por objetivos conceptuales, los contenidos a desarrollar serán también conceptuales.		
INTRODUCCIÓN	La introducción puede contemplar: • Utilidad del contenido. Provecho, importancia y relaciones. • Guía del proceso de aprendizaje. • Motivar al alumno para su estudio, despertando su interés por el tema a tratar. • Detalles que convengan para suscitar controversias, curiosidad, asombro, etc. • Relación con otros conocimientos: previos y posteriores. • Ayudas externas que se precisarán para su aprendizaje. • Estructura del contenido.		
DESARROLLO	CONCEPTUALES	PROCEDIMENTALES	ACTITUDINALES
	Descripción del contenido: • Utilizar un lenguaje claro e introducir progresivamente la nueva terminología. • Realizar una estructura ordenada: división y subdivisión de los distintos párrafos. • Obviar párrafos y frases excesivamente largos. • Intercalar interrogaciones que ayuden a mantener la atención del alumno. • Integrar refuerzos motivadores a lo largo del texto. • Incluir referencias a objetos, situaciones o descripciones reales, utilizando los ejemplos y contraejemplos.	Pasos y componentes del desempeño: • Demostración secuenciada de cada uno de los pasos. • Componentes asociados a los pasos (materiales, diagramas, conceptos…) • Pautas a tener en cuenta. • Ámbitos de aplicación.	Demostración: • Presentación de la situación. • Análisis de los componentes que involucra una actitud: cognitivos, afectivos y conductuales. • Análisis de las circunstancias que afectan a la actitud. • Análisis de las circunstancias en las que se manifiesta la actitud.
CIERRE	Puede contener las ideas principales, mapa conceptual con los contenidos vistos, etc.		

METADATOS	General: Título, Idioma, Descripción, Palabras clave, Otros autores Uso educativo: Tipo de recurso educativo, Nivel de interactividad, Densidad semántica, Destinatario, Contexto, Dificultad, Tiempo típico, Descripción acerca del uso, Idioma del destinatario
EVALUACIÓN	Del aprendizaje obtenido por el alumno en base a evaluaciones, caso de uso, problemas y prácticas. Una evaluación fraccionada e integral por conceptos, procesos y actitudes.

Nota: Fuente: Instituto de Ciencias de la Educación de la Universidad Politécnica de Valencia (2007).

CAPÍTULO III. PROCESO METODOLÓGICO

El Capítulo III está constituido de manera inicial por un diseño instruccional Análisis, Diseño, Desarrollo, Implementación y Evaluación (ADDIE) el cual es utilizado para el desarrollo del objeto de aprendizaje; la investigación se basa en un enfoque cualitativo con un diseño de investigación de estudio de caso además de que se pretende construir conocimiento aplicando la Teoría Fundamentada.

III.1 Procedimientos

III.1.1 Metodología para el desarrollo del proyecto

El trabajo de investigación realizado en este documento es el desarrollo de un OA, para la evaluación de competencias del Módulo I del Diplomado en Seguridad Informática.

El OA se va a diseñar con base al modelo instruccional ADDIE es el acrónimo del modelo, integrado por las fases que se muestran en el Diagrama 2.

Diagrama 2: Modelo instruccional ADDIE
Fuente: Belloch (2006)

La selección de este modelo instruccional se realiza tomando como base el hecho de que cada una de sus fases se adapta a las necesidades del OA a desarrollar, cabe mencionar que la evaluación del Módulo I será por competencias, descritas en el apartado de Fundamentación

Descripción de las fases:

Fase 1: Análisis

En esta fase, se determinará la estructura del OA, se analizarán los objetivos y la taxonomía a alcanzar en cuanto a la evaluación de las competencias específicas además de determinar la forma de aplicarlas en el Objeto de Aprendizaje.

Fase 2: Diseño

Esta etapa establecerá la forma en que se integrarán las competencias a evaluar, una a una, para que la evaluación resulte apropiada y congruente con la competencia a lograr por parte del alumno.

Fase 3: Desarrollo

Al desarrollar el OA, se tendrá especial cuidado la realización de las actividades diseñadas para evaluar las competencias asimismo que sean lo suficientemente sólidas, y que comprendan todas las subcompetencias necesarias; para que la evaluación de habilidades se logre de manera efectiva.

Fase 4: Implementación

Se determinará una atención minuciosa en que el diseño, estructura y funcionamiento del OA sea adecuado.

Fase 5: Evaluación

Por último en esta fase, se comprobará si el OA evalúa las competencias de manera efectiva y los resultados arrojados serán positivos.

Cuando se imparta el curso, se realizará un análisis cualitativo de los resultados del curso, se codificarán los datos obtenidos de la evaluación y se integrarán las categorías y los datos mediante la comparación constante de los resultados obtenidos por cada alumno para conocer la pertinencia y efectividad del OA.

El proyecto gira en una disciplina humanística como lo es la Educación; se busca analizar al sujeto de estudio para descubrir sus carencias y debilidades, de esta manera atender sus necesidades.

En resumen después de analizar a Hernández *et al.* (2010) y Bernal (2010), se menciona que la metodología cualitativa es un enfoque inductivo que implica una inmersión inicial en campo, interpretación contextual, flexibilidad, preguntas y recolección de datos.

El desarrollo de este proyecto se enfoca en el diseño e implementación de un OA para evaluar competencias en alumnos del Diplomado en Seguridad Informática modalidad virtual; se realizará dicho diseño para poder evaluar las competencias adquiridas en el Módulo I de dicho diplomado; los resultados derivados de este proyecto darán pauta para la implementación del OA a nivel institución, una vez comprobada su efectividad.

III.1.2 Alcance de investigación

El desarrollo del OA únicamente comprenderá la evaluación del Módulo I del Diplomado en Seguridad Informática; se pretende construir conocimiento aplicando la Teoría Fundamentada.

Strauss & Corbin (2002) la denominan Teoría Fundamentada ya que se deriva de datos recopilados de manera sistemática y analizados por medio del proceso de investigación. En este método, la recolección de datos, el análisis y la teoría que surgirá de ellos tienen una estrecha relación entre sí.

Permitirá analizar los datos y construir una mirada teórica sobre el tema de evaluación de competencias a través de un OA a elaborar del Módulo I correspondiente al Diplomado en Seguridad en Informática.

La Teoría Fundamentada permite la generación de teoría a partir de:

- Recolección de los datos de cada alumno
- Del análisis de los datos obtenidos una vez implementado el OA, serán procesados los datos, se obtendrán las categorías y subcategorías que permitirán determinar si el Objeto de Aprendizaje sirve o no.

- Creación de teoría, entonces si es evidente que el uso del OA, permite realmente evaluar las competencias, se puede generar y difundir el conocimiento alcanzado sobre su diseño, elaboración, aplicación y evaluación.

Es preciso mencionar que la teoría generada es derivada de los datos que se parecen más a la "realidad"; es decir en experiencias o especulaciones del cómo se piensa que debería funcionar, así lo mencionan Strauss & Corbin (2002).

III.1.3 Diseño de la evaluación

Las competencias consideradas en este estudio se explican en la Tabla 8

Tabla 8

Competencias a evaluar.

COMPETENCIAS	SUBCOMPETENCIAS	OBJETIVOS A EVALUAR
Aplicar el concepto de Seguridad Informática para identificar la eficiencia de modelos, tipos de control de acceso, autentificación de datos, ataques a sistemas informáticos, para garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.	Distinguir entre sistema de información y sistema informático	Recordar la información de sistemas de información y sistema informático. Identificar los detalles importantes de los sistemas de información y sistema informático. Utilizar lo que ha aprendido de sistemas de información y sistema informático para crear nuevos conocimientos y aplicarlo en situaciones diversas.
	Comprender qué significa seguridad en el amplio concepto de sistema de información y en el concreto de sistema informático. Conocer cuáles son las propiedades de un sistema seguro.	Definir el concepto de seguridad de sistema de información y de sistema informático. Identificar los conceptos se seguridad en un sistema de información y sistema informático. Describir las propiedades de un sistema seguro. Identificar las propiedades de un sistema seguro.
	Comprender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto.	Recordar el concepto de análisis de riesgo y lo que conlleva en seguridad informática. Explicar los riesgos a los que se enfrenta los sistemas de información.

	Entender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto.	Recordar los servicios de seguridad, para un control de riesgos Entender lo que son servicios, mecanismos y herramientas de seguridad.
	Tener la base necesaria para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos.	Recordar las herramientas de análisis y gestión de riesgos. Identificar la importancia de las herramientas de análisis y gestión de riesgos en una empresa Utilizar las herramientas de análisis y gestión de riesgos para una empresa. Tener la base necesaria para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos

Nota: Fuente: Elaboración propia (2014)

III.1.4 Proceso para analizar resultados del curso

El diseño que se utilizará para la recolección de resultados será estudio de caso, es una modalidad nacida desde el siglo XXI, con extraordinarios resultados en las ciencias sociales y para efectos de estudio para la educación, entre otras. Uno de los pioneros en la aplicación del estudio de caso fue el autor Robert Stake en 1978, señala que debe contener 5 requerimientos básicos para la comprensión del caso:

- Selección del tema/área/caso, son las personas o instituciones involucradas en el estudio, para dicha investigación serán los participantes del Diplomado de Seguridad informática y la evaluación de las competencias del Módulo I de dicho diplomado.
- Contexto en el área geográfica que se realizará la investigación es la Universidad Politécnica de Pachuca, a alumnos que participaron en el Diplomado.
- Actividades, se realizará un cuestionario a los alumnos y uno más a la coordinadora del Diplomado.

Bernal (2010) menciona que el objetivo es estudiar a detalle una unidad de un universo poblacional; el proceso de desarrollo parte de la definición de un tema donde se analiza la unidad, se recolectan los datos, se analizan y validan; al término se redactará el caso.

III.2 Sujetos

III.2.1 Delimitación de la población

La población considerará en el aplicación de los instrumentos de diagnóstico consiste en alumnos de la carrera de Ingeniería en Telemática e Ingeniería en Software, la primera característica que tienen en común estos alumnos es que en su momento les fue impartida la materia de Seguridad en Informática y se pretende que después de que concluyan su carrera realicen el Diplomado virtual.

Esta población seleccionada ha estudiado bajo el modelo Educación Basada en Competencias durante toda su carrera por tal motivo conocen la evaluación por competencias además otras de las características importantes para seleccionar a esta población es debido a que son alumnos próximos a egresar de las ingenierías mencionadas anteriormente; por lo que estamos hablando de una población de 30 alumnos en total.

Las personas a las que se aplicará los cuestionarios son 6 alumnos pertenecientes a la Universidad Politécnica de Pachuca de los cuales 4 son varones y 2 mujeres la edad promedio de los encuestados es de 20.5 años, con un perfil profesional como Técnico en Informática además de ser estudiantes del noveno cuatrimestre de Ingeniería en Software y haber cursado la materia de Seguridad Informática.

III.3 Instrumentos

Los instrumentos que se utilizaron para la recolección de datos, son cuestionarios con preguntas abiertas las cuales se aplicaron a 6 alumnos y a la coordinadora del CEDyTE y se busca encontrar la importancia que tiene para los alumnos una evaluación por competencias, si alguna vez les han aplicado una evaluación por competencias y por consiguiente el nivel que creen tener de competencias específicas de Seguridad en Informática. Además de la importancia que tiene esta evaluación para el Diplomado en forma general. (Véase. Anexo 1).

Por otro lado, el propio OA es un instrumento de evaluación por competencias que se describe en el apartado de Producto.

CAPÍTULO IV. PRODUCTO

En este apartado, se describe el producto elaborado para darle solución a la problemática del proyecto, el OA está constituido por 18 actividades que evaluarán cada una de las 5 unidades que integran el Módulo I, diseñando los objetivos y estrategias pedagógicas de cada unidad y el desarrollo de los contenidos serán parte del OA.

IV.1 Propuesta concreta de alternativa de solución

El OA tiene como función principal evaluar las competencias del Diplomado en Seguridad Informática (modalidad virtual), específicamente del Módulo I se encuentra distribuido en:

- 3 apartados principales el objetivo o metadatos del OA,
- los contenidos de cada uno de las 5 unidades en los que se constituye la Módulo I
- las actividades correspondientes para poder lograr los objetivos de aprendizaje descritos en cada uno de las unidades

Se pretende que el alumno lo realice en un lapso de dos semanas la valoración sobre el Módulo I, en la que se evidenciará el dominio de las competencias con cada una de las actividades de evaluación correspondientes a cada unidad.

La elaboración digital del objeto virtual será desarrollado en el software de aplicación Dreamweaver en un formato *html* este formato es compatible para visualizarse en casi todos los navegadores web, es muy versátil, desarrollar entornos profesionales y de fácil uso.

El OA se elaborará con el modelo de diseño instruccional ADDIE, a continuación se explica una breve descripción de las etapas en que consiste el modelo (2006) como se muestra en la Tabla 9.

Tabla 9

Desarrollo del diseño instruccional ADDIE

Análisis	Es analizar el alumnado, el contenido y el entorno cuyo resultado es la descripción de su situación y sus necesidades formativas.
Diseño	Se desarrolla el programa del curso desde un aspecto pedagógico, secuencial y del cómo organizar el contenido.
Desarrollo	Es la creación de los contenidos, materiales y recursos necesarios de aprendizaje basados en la fase de diseño.
Implementación	Es la ejecución y puesta a la práctica de la acción formativa de los alumnos.
Evaluación	La realización de evaluaciones formativas en primera instancia de cada una de las fases del proceso de ADDIE, para proseguir con una evaluación sumativa a través de pruebas específicas para analizar los resultados

Nota: Fuente: Elaboración propia (2014)

La interacción entre cada una de las fases es cíclica, como se muestra en el Diagrama 3.

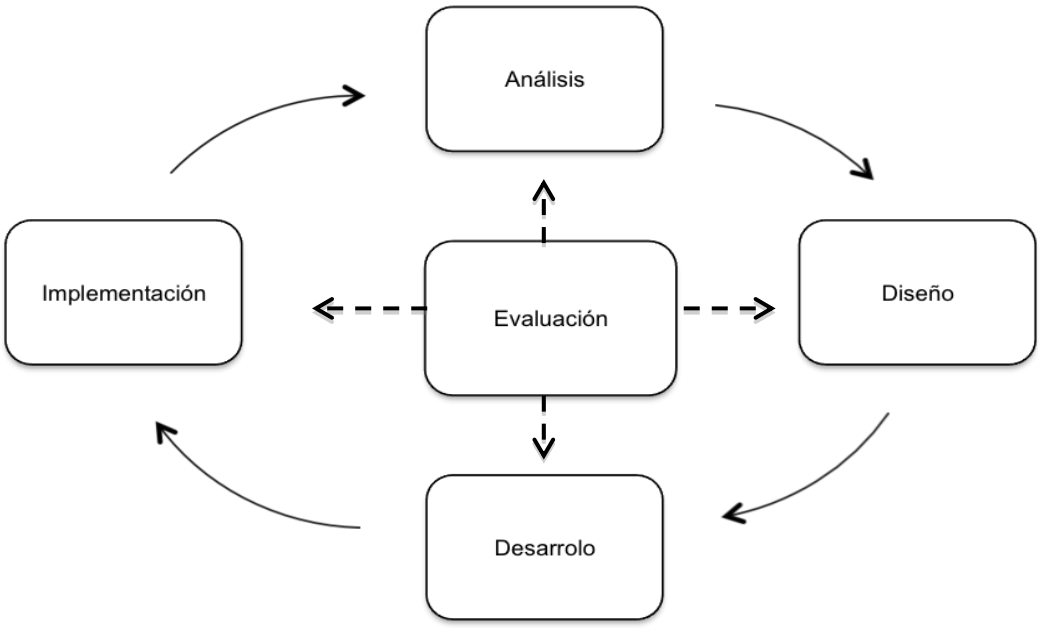


Diagrama 3: Interacción Modelo ADDIE.

Fuente: Belloch (2006)

Con fundamento en lo anterior en la Tabla 10 se establecen las etapas del objeto conforme el modelo de instruccional ADDIE.

Tabla 10

Etapas del modelo instruccional ADDIE.

Modelo ADDIE	Tareas	Resultados	Recursos	Tiempo de desarrollo
Análisis	Evaluación de necesidades. Identificación del problema. Análisis de tareas.	Perfil de estudiantes. Descripción de obstáculos. Necesidades, definición de problemas.	Humanos: Experto pedagógico y técnico	1 semana
Diseño	Escribir objetos. Desarrollar las unidades a evaluar. Planear la instrucción. Identificar los recursos.	Objetivos medibles. Estrategia Instruccional. Especificaciones del prototipo.	Tecnológicos: Hardware y software Humanos: Experto pedagógico y técnico.	
Desarrollo	Trabajar con productores. Desarrollo del libro de trabajo, organigrama y programa.	Storyboard. Instrucción basada en la computadora. Instrumentos de retroalimentación Instrumentos de medición. Instrucción mediada por computadora.	Tecnológicos: Hardware y software Humanos: Experto técnico.	1 semana
Implementación	Entrenamiento docente. Entrenamiento Piloto.	Comentarios del estudiante. Datos de evaluación.	Tecnológicos: Hardware y software Humanos: Experto técnico	1 semana
Evaluación	Datos de registro del tiempo Interpretación de los resultados de la evaluación Encuestas a graduados Revisión de actividades	Recomendaciones. Informe de evaluación. Revisión de los materiales. Revisión del prototipo.	Tecnológicos: Hardware y software Humanos: Experto técnico	1 semana

Nota: Fuente: Elaboración propia (2014)

A continuación de desglosan cada una de las etapas que se utilizaron para el desarrollo del objeto, mediante el modelo instruccional anteriormente explicado.

Fase 1. Análisis

La fase de Análisis es la etapa principal para determinar el perfil de los participantes, la metodología de aprendizaje, el contenido del OA y los requerimientos de hardware y software mínimos con los que debe contar el participante.

Tabla 11
Análisis del Módulo I

Diplomado	Seguridad en Informática
Módulo I	Introducción a la Seguridad Informática y al Aseguramiento de Información

Pre requisitos

Ser egresado de alguna carrera técnico profesional o profesional del área de sistemas computacionales, informática o a fin. Dominar el uso de herramientas de Internet así como el manejo de herramientas ofimáticas y nociones básicas de software en general.

Introducción al Objeto de Aprendizaje

El propósito de esta guía es facilitar el aprendizaje del alumno, encausando actividades y juicios que propician situaciones en las que se desarrollaran competencias. El docente facilitará el proceso de aprendizaje poniendo sumo cuidado en el encuadre de las actividades y las competencias que se desarrollarán en cada una de las actividades.

El desarrollo de las competencias significa que el alumno genere su propio aprendizaje en base a experiencias, además de que adquieran la capacidad de resolver problemas en diversos contextos o situaciones; e involucrar las dimensiones cognitivas, afectivas y psicomotoras del alumno; por lo que el Módulo I está conformada por actividades, prácticas, caso de uso y actividades del mundo real para que puedan poner en práctica sus competencias logradas.

El alcance es involucrar la comprensión, transferencia y aplicación de conocimientos a situaciones de la vida cotidiana; esto exige recuerdo, identificación, utilización y aplicación de los saberes o conocimientos para resolver problemas o para la toma de decisiones. El alumno tiene que aprender el cómo se hace y la aplicación de sus conocimientos en la vida cotidiana y profesional.

Estructura temática

Unidad	Nombre de la Unidad
1	Sistemas de información y sistemas informáticos.
2	Seguridad
3	Análisis de riegos
4	Control de riesgos
5	Herramientas de análisis y gestión de riesgos

Calendario del curso

Duración de la Unidad		**2 semanas**
Unidad	**Nombre de la Unidad**	**Duración**
1	Sistemas de información y sistemas informáticos.	3 días
2	Seguridad	3 días
3	Análisis de riegos	2 días
4	Control de riesgos	2 días
5	Herramientas de análisis y gestión de riesgos	4 días

Requerimientos técnicos:

Hardware mínimo:	**Software mínimo:**
Procesador Pentium III	Resolución de pantalla 1024 x 768 píxeles.
1 Gb en RAM	Mozilla Firefox o Internet Explorer
60 GB en disco duro	Adobe Reader 6 o superior
Tarjeta de audio	Java Runtime Environment
	Macromedia Flash Player 6 o superior
	RealPlayer 10 o superior

Nota: Fuente: Elaboración propia (2014)

Fase 2. Diseño

La fase de diseño se encarga especialmente en el desarrollo de objetivos y las estrategias pedagógicas para la evaluación por competencias.

Tabla 12
Diseño del Módulo I

Objetivo
Aplicar el concepto de Seguridad Informática para identificar la eficiencia de modelos, tipos de control de acceso, autentificación de datos, ataques a sistemas informáticos, para garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
Objetivos específicos

Unidad	Nombre de la unidad
1	**Sistemas de información y sistemas informáticos**. Distinguir entre sistema de información y sistema informático.
2	**Seguridad** Comprender qué significa seguridad en el amplio concepto de sistema de información y en el concreto de sistema informático. Conocer cuáles son las propiedades de un sistema seguro.
3	**Análisis de riegos** Entender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto.
4	**Control de riesgos** Entender lo que son servicios, mecanismos y herramientas de seguridad.
5	**Herramientas de análisis y gestión de riesgos** Tener la base necesaria para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos.

Estrategia de aprendizaje

1. **Aprendizaje Basado en Problemas**
   Consiste en la presentación de situaciones reales o simuladas que requieren la aplicación del conocimiento, en las cuales el alumno debe analizar la situación y elegir o construir una o varias alternativas para su solución (Díaz Barriga, 2003) Es importante aplicar esta estrategia ya que las competencias se evalúan en el proceso de solución de problemas y en este sentido; el alumno aplicará soluciones a los problemas que enfrenta en su vida cotidiana y estas evidencias serán evaluables.

2. **Evaluación de manejo de información documental**
   Consiste en llevar a los alumnos a la discusión y al análisis de situaciones o información, con base en preguntas planteadas y formuladas por el docente o por los mismos alumnos, con el fin de explorar las capacidades del pensamiento al activar sus procesos cognitivos; se recomienda integrar esta técnica de manera sistemática y continua a las anteriormente descritas y al abordar cualquier tema del programa de estudio.

Metodología de Evaluación

La rúbrica permite establecer los criterios e indicadores que se deben considerar para evaluar el logro de la competencia. Los criterios que se han establecidos son:

	A Excelente	B Suficiente	C Insuficiente

	Satisface plenamente o supera las exigencias.	A partir de este nivel en el que podemos decir que se ha adquirido la competencia. Satisface las exigencias mínimas	Requiere entrenamiento formativo para alcanzar el desempeño requerido
Cumple con los estándares o requisitos para el logro del producto o desempeño	✓	✓	✗
Demuestra iniciativa y creatividad	✓	✓	✗
Va más allá de lo que se solicita como mínimo.	✓	✗	✗

Nota: Fuente: Elaboración propia (2014)

Fase 3. Desarrollo

Desarrollo de contenidos

En la etapa de desarrollo se elaboran las 5 unidades que integran el Módulo I el desarrollo de la estructura completa de cada unidad se encuentra en anexos (Véase Anexo 3), cada unidad está estructurada con los siguientes elementos:

Tabla 13
Desarrollo de contenidos.

Elemento	Descripción
Nombre	Indica el título de la unidad.
Tiempo	Son los días que dura la unidad.
Competencia específica	Se detalla la competencia a alcanzar en la unidad.
Contenido	Descripción de los conceptos que se proporcionarán en la unidad.
Actividades de evaluación	Incluye el número y el nombre de la actividad a evaluar.
Descripción de la evaluación	Se especifica la actividad que servirá para evaluar la unidad además del número y tipo de preguntas que lo integran.

Objetivos de aprendizaje o competencia a evaluar (Propuesta de MSU)	Explica de forma clara el objetivo que se pretende cumplir al concluir la evaluación, cabe mencionar que se basan en la taxonomía de Marzano.

Nota: Fuente: Elaboración propia (2014)

Las unidades que componen el Módulo I se enuncian a continuación:

Unidad	Nombre de la unidad
1	**Sistemas de información y sistemas informáticos**.
2	**Seguridad**
3	**Análisis de riegos**
4	**Control de riesgos**
5	**Herramientas de análisis y gestión de riesgos**

El desarrollo de los contenidos de las unidades mencionadas anteriormente son extraídos del libro de *Seguridad Informática* del autor Aguilera (2010), la cual se utilizó para fines didácticos, estos contenidos son estructurados con elementos visuales como lo son imágenes relacionadas al tema, esquemas que apoyan al entendimiento de términos además de texto que es imprescindible para los contenidos; el desarrollo completo de contenidos se encuentra en anexos (Véase Anexo 4).

Instrumentos de evaluación

El proceso de evaluación que integra el OA será de forma continua y secuencialmente, esto nos permitirá recolectar los datos necesarios para verificar si el alumno ha cumplido con los objetivos esperados y las competencias establecidas al inicio de la unidad. El OA está comprendido por 18 actividades de evaluación (Véase Anexo 5) a lo largo de las 5 unidades que integran el Módulo I, elaborando cada actividad de evaluación para estimar la competencia correspondiente a la unidad evaluada.

La ponderación asignada para cada una de las 18 actividades de encuentra el sistema completo de evaluación en el Anexo 6, a continuación se mencionan los elementos que estructuran dicha ponderación.

Tabla 14
Elementos que estructuran la ponderación

Elemento	Descripción
Unidad	Es el número de la unidad que evalúa.
Nombre de la Unidad	Se establece el nombre de la unidad correspondiente al número de la unidad a evaluar.
Porcentaje	Se establece de forma global el cual corresponde a toda la unidad y de forma parcial el cual indica la ponderación para cada una de las actividades evaluativas que integran la unidad.
Actividad	Indica el número y el nombre de la actividad a evaluar en la unidad.

Nota: Fuente: Elaboración propia (2014)

La creación de la siguiente rúbrica apoya en la evaluación de cada una de las actividades a evaluar, bajo en la cual se indica la forma de evaluar cualitativamente y los descriptores que debe cumplir:

Tabla 15
Rúbrica de evaluación

	A **Excelente**	**B** **Suficiente**	**C** **Insuficiente**
	Satisface plenamente o supera las exigencias.	A partir de este nivel en el que podemos decir que se ha adquirido la competencia. Satisface las exigencias mínimas	Requiere entrenamiento formativo para alcanzar el desempeño requerido
Cumple con los estándares o requisitos para el logro del producto o desempeño	✓	✓	✗
Demuestra iniciativa y creatividad	✓	✓	✗
Va más allá de lo que se solicita como mínimo.	✓	✗	✗

Nota: Fuente: Elaboración propia (2014)

Y específicamente de cada una de las actividades se realizará una rúbrica concreta por actividad.

Criterios de evaluación Actividad 1.1 Caso Práctico inicial

Tabla 16
Criterios de evaluación de la actividad 1

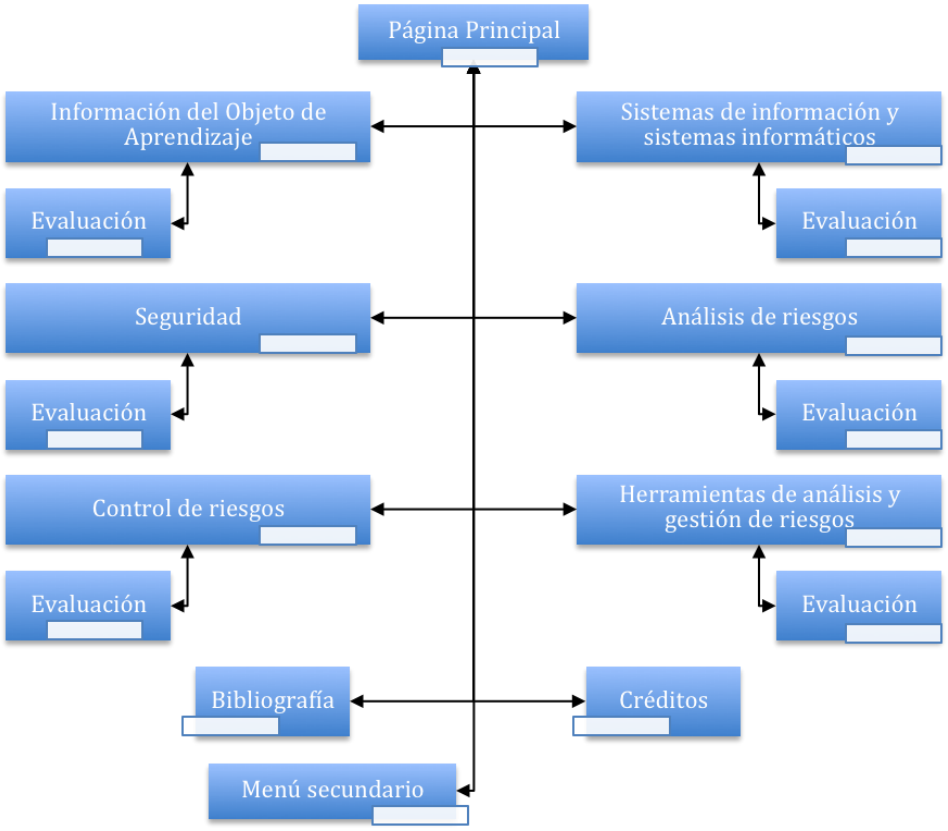
	A Excelente	**B Suficiente**	**C Insuficiente**
Cumple con los estándares o requisitos para el logro del producto o desempeño	Responde correctamente las 6 preguntas	Responde correctamente de 4 a 6 preguntas	Responde correctamente menos de 2 preguntas
Demuestra iniciativa y creatividad	Envía el cuestionario al concluir el tema 1 de la unidad 1.	Envía el cuestionario al concluir la unidad 1.	Envía el cuestionario al concluir el Módulo I.
Presentación y ortografía	Buena presentación, usa imágenes para ejemplificar el caso, explica muy bien sus ideas y no tiene errores gramaticales ni ortográficos.	Presentación adecuada, trata de explicar sus ideas y tiene algunos errores gramaticales ni ortográficos de 5 a 8.	Presentación mínima, no explica sus ideas y tiene errores gramaticales ni ortográficos más de 8.

Nota: Fuente: Elaboración propia (2014).

Interactividad

A continuación se muestra el diagrama de navegación el OA cuyo propósito es mostrar un esquema que incluye los elementos que integran el OA y la navegación entre cada uno de los elementos

Diagrama 4: Navegación del Objeto de Aprendizaje.
Fuente: Elaboración propia (2014)



Interfaz de usuario: la elaboración de las pantallas de navegación del OA serán sencillas y amigables con el usuario final, colocando colores, tamaños y posiciones adecuadas para la vista del usuario. (Véase Anexo 7).

Los contenidos tendrán imágenes adecuadas al tema que se esté abordando; en cada una de las actividades se mencionará las competencias específicas, los objetivos de aprendizaje y las rúbricas con las que se evaluarán las competencias.

Instrumentos de retroalimentación

Al realizar cada una de las actividades de evaluación, al finalizar el alumno recibirá una retroalimentación en cada una de las evaluaciones que desarrolle el participante, haciendo mayor énfasis en las respuestas incorrectas.

Cada una de las actividades contendrá una retroalimentación automática después de finalizarla, excepto aquellas actividades que requieran de mayor elaboración y tengan que ser enviados por otro medio como correo electrónico, la retroalimentación será realizada personalmente por el experto de la unidad.

Los niveles de dominio logrados en cada una de las evaluaciones, van de la mano con las competencias específicas que se van adquirir en cada una de las unidades (véase Anexo 3.)

Fase 4. Implementación

Después de elaborar el OA mediante la metodología ADDIE y desarrollar las primeras 3 etapas con éxito (Análisis, Diseño y Desarrollo) se integran todos los recursos previamente ha sido revisado su funcionamiento de estos, el OA está listo para ser subido a un dominio.

El desarrollo del OA se realizó en un lenguaje de programación para páginas web *html* (hyperText Markup Language) debido a su compatibilidad, versatilidad de uso y de programación, para la implementación parcial del proyecto se ha requerido de ser alojado el OA en un host Español, cuyo dominio es gratuito cuya dirección es http://seguridadinformatica.2trweb.com.

En la dirección antes mencionada se encuentra el OA concluido y en funcionamiento, se aprecia la información general del objeto, el menú principal de los contenidos temáticos a abordar y los instrumentos de evaluación de cada unidad respectiva al Módulo I.

Fase 5. Evaluación

La CEDyTE cuenta con 3 criterios de evaluación y cada uno con diversos lineamientos de evaluación para poder aprobar un OA y poder implementarlo en sus Diplomados, a

continuación se muestra el instrumento de evaluación que tendrá que cubrir el OA para evaluar competencias del Módulo I del Diplomado en Seguridad Informática (Véase Anexo 8.).

Formato 1

Instrumento de evaluación del Módulo I en Seguridad Informática

Título: Seguridad Informática

Descripción: Objeto de aprendizaje para evaluar competencias específicas del Módulo I del Diplomado en Seguridad Informática impartido por la Universidad Politécnica de Pachuca

Autor: I. S. C. Rubí Yuriana Bautista García

Fecha de evaluación: 19 de noviembre de 2014

Criterios		Si	No	Observaciones
Competencias	Las competencias específicas constituyen la competencia general del Módulo I.			
	Los contenidos de cada una de las unidades son suficientes para poder adquirir cada una de las competencias específicas establecidas.			
Actividades de evaluación	Los cuestionarios evalúan las de competencias del Módulo I del Diplomado en Seguridad Informática.			
	Las 18 actividades propuestas, son idóneas para la evaluación de competencias en Seguridad Informática.			
	Considera que las 18 evaluaciones tiene una extensión adecuada,			
	Los 3 casos prácticos que se presentan al final de las evaluaciones, apoyan a la adquisición de la competencia general del Módulo I.			
	Incluiría alguna actividad más.			
	Eliminaría alguna actividad.			
	Existen actividades que no proporcionen información relevante para la adquisición de			

	competencias.			
	Las evaluaciones están expresadas de forma comprensible.			
	Es correcta la ordenación y distribución de las actividades.			

Ítems de cada evaluación	Los ítems de cada evaluación estiman las competencias específicas de cada unidad.			
	Incluiría algún ítem más			
	Eliminaría algún ítem			
	Existen ítems que no proporcionen información relevante para la adquisición de competencias.			
	Los ítems están expresados de forma comprensible.			
	Es correcta la ordenación y distribución de los ítems.			
	Considera que a través de estos ítems se pueden estimar las competencias adquiridas en el Módulo I del Diplomado en Seguridad Informática.			

Nota: Fuente: Elaboración propia (2014)

Evaluadores:

CONCLUSIONES

Existen dos términos difíciles de conceptualizar y de estudiar, por la gran gama de características y definiciones, como lo es el termino de competencias y OA. Después de analizar los autores concluyo que las competencias es una capacidad cognitiva, adaptativa y conductual, es decir el dominio de conocimientos y habilidades para responder adecuadamente a las demandas que se presentan en el entorno; las competencias se asimilan y se construyen en el tiempo, no son algo dado, innato y estable.

El objeto de aprendizaje se define como una pieza digital con sentido pedagógico que consta de una colección de recursos digitales, además de ser reutilizables en diferentes contextos.

Durante el desarrollo de este proyecto se analizaron diferentes autores y puntos de vista que ayudaron a nutrir las bases de la fundamentación que se requería para sustentar la problemática encontrada; y elaborar un Objeto de Aprendizaje que apoyará el Diplomado en Seguridad Informática a valorar las competencias del Módulo I. El objeto de aprendizaje tendrá un sentido pedagógico, paralelamente se beneficiará el aprendizaje de los alumnos de la mano con la tecnología.

El OA que se elaborará para el Módulo I del Diplomado en Seguridad Informática modalidad virtual, además tendrá aplicaciones de evaluación en diversas materias, carreras y modalidades.

Se logró identificar que aún en estos tiempos existe un desconocimiento por parte del sector educativo acerca de la evaluación por competencias, debido a que aún no existe una definición formal para los maestros y estudiantes. Los estudiantes no cuentan con dicha conceptualización sobre la evaluación por competencias; pero los hallazgos para este proyecto que coexiste en valorar competencias para la vida laboral y profesional.

Al realizar el proceso de construcción del OA sirvió para identificar que la evaluación de competencias debe abarcar no solo el examen escrito, adquisición de competencias y el producto final así mismo de las carencias que existen en cuanto a la evaluación de competencias que hasta ahora se evalúan a través de exámenes y productos

En el proceso, surgieron dudas sobre la mejor opción para proponer las actividades evaluativas por competencias, en base a la investigación que realiza la Universidad de Monatana se seleccionaron: solución de problemas, estudio de situaciones, y quizz; las cuales permiten evaluar las competencias de acuerdo a la reflexión, análisis, procedimiento y pensamiento crítico de cada alumno.

Aunado a esto se realizó el análisis para determinar los requerimientos de la evaluación; el umbral o nivel mínimo requerido que se utilizó; de cada uno de los objetivos de aprendizaje. Así mismo como lo hace mención Frade (2013) “una competencia no se alcanza directamente de manera completa sino a través del logro de objetivos que finalmente la integran”, al igual hace referencia a esto la Universidad de Monatana la cual indica que una actividad debe ir acompañada de un objetivo de aprendizaje (como MSU lo denomina), que cumpla y satisfaga una competencia.

La evaluación generalmente se realiza a través de la demostración de lo que se sabe a través de exámenes (Frade, 2011). El resultado de estos exámenes generalmente evalúa la memorización y se trata de pregunta y respuesta. En cambio cuando se plantean problemas a resolver o de estudios de caso, se le pide al alumno que ejerza habilidades del pensamiento para el análisis del caso y buscar alternativas de solución. En este caso el alumno demostrará lo que sabe, lo que sabe hacer y su actitud para abordar un problema complejo, que a su vez le exige un producto de aprendizaje más complejo que tiene que ver con el saber hacer, saber ser y saber convivir, que son los elementos de las competencias. Un profesor sabrá cuando está trabajando por competencias, cuando sus actividades son complejas y pedirá que lo resuelvan los alumnos.

En la elaboración de dicho proyecto se enfrentaron diversas dificultades como lo es el poco tiempo que dedicaba la CEDyTE para apoyar en el proceso de investigación, falta de desarrollo de competencias en el Diplomado, incoherencia entre los objetivos, unidades y actividades de cada unidad del Diplomado, y adversidades como la recopilación de información sobre evaluación de competencias en la virtualidad, que es escasa como se mencionó con anterioridad. Por lo que se tuvo que aprender desde las competencias específicas que se requieren para el Módulo I, así como la elaboración de materiales, evaluaciones y rúbricas apegadas a la Seguridad Informática.

Después de un arduo trabajo de investigación, diseño y desarrollo del OA para la evaluación de competencias específicas del Módulo I del Diplomado en Seguridad Informática se culminó la elaboración y se espera sea eficiente y viable.

ANEXOS

ANEXOS

Anexo 1 Instrumento de recolección de información de Diagnóstico de los alumnos

“Evaluación por competencias”

El siguiente cuestionario se realiza para recabar información para la elaboración de un objeto de aprendizaje para la evaluación por competencias.

Esperando contar con su apreciable colaboración con este proyecto, cabe resaltar que sus contribuciones serán anónimas y se le darán posteriormente los resultados de la misma.

Solicito a usted conteste el siguiente cuestionario.

Nombre: _____ Fecha: _____

1. ¿Ha realizado una evaluación por competencias? ¿Cómo fue?
   _____
   _____
   _____
   _____

2. De la siguiente tabla, señala cuales son las competencias que crees tener en Seguridad Informática.

Competencia	Si	Más o menos	No
Distinguir entre sistema de información y sistema informático			
Comprendes que significa seguridad en el amplio concepto de sistema de información y conoces cuales son las propiedades de un sistema seguro.			
Puedes entender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto			
Entiendes lo que son servicios, mecanismos y herramientas de seguridad			
Tienes las bases necesarias para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos.			

3. ¿Por qué crees que es importante tener estas competencias y habilidades en Seguridad Informática?

   _____
   _____
   _____
   _____

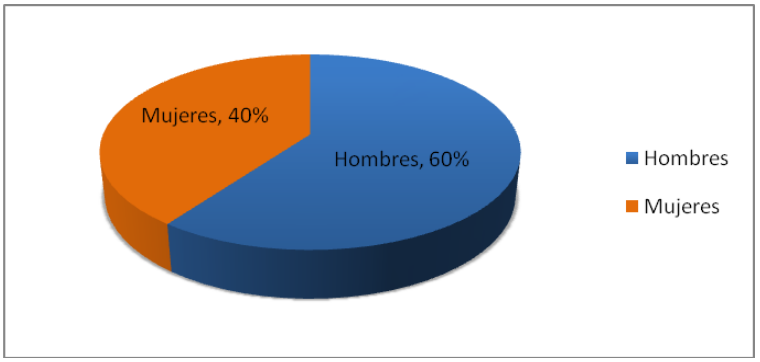
4. ¿Qué piensas sobre la importancia de realizar una evaluación por competencias en el Diplomado de Seguridad Informática?

   _____
   _____
   _____
   _____

   Agradezco su participación en esta recopilación de información, sus contribuciones serán anónimas y únicamente serán utilizadas para esta investigación.

Anexo 1 Tabla. 1 Resultados del cuestionario número 1

	Alumnos
Masculino	4
Femenino	2
No han realizado evaluación por competencias	4
Creen tener competencias específicas en Seguridad Informática	3
Afirman la importancia de desarrollar competencias	6



Anexo 1

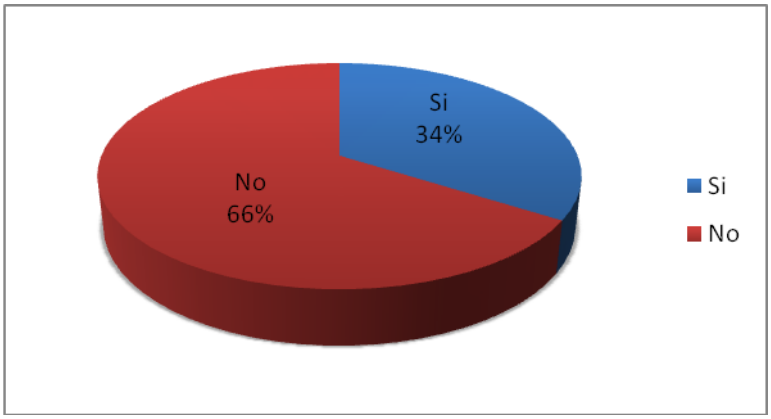


Figura. 2: Alumnos que han realizado una evaluación por competencias

Anexo 1

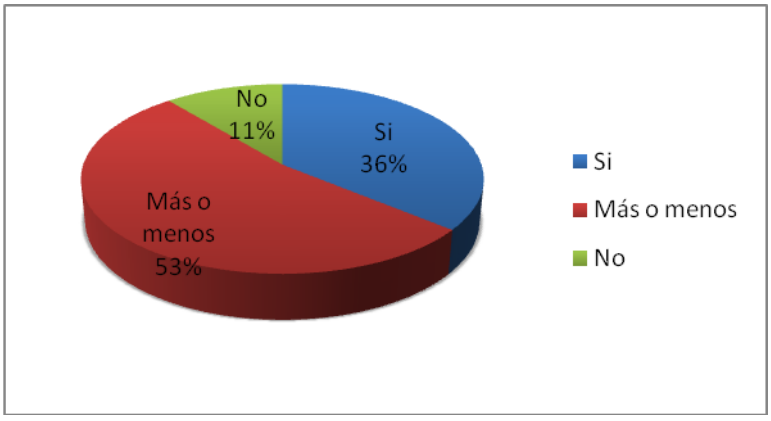


Figura. 3. Alumnos que creen tener competencias específicas en Seguridad Informática

Anexo 2 Instrumento de recolección de información de Diagnóstico para la coordinadora de la CEDyTE

"Evaluación por competencias"

El siguiente cuestionario se realiza para recabar información acerca de las necesidades que tiene la CEDyTE (Coordinación de Educación a Distancia y Tecnología) sobre el Diplomado en Seguridad Informática.

Esperando contar con su apreciable colaboración con este proyecto, cabe resaltar que sus contribuciones serán anónimas y se le darán posteriormente los resultados de la misma.

Solicito a usted conteste el siguiente cuestionario.

Nombre: _____ Fecha: _____

1. ¿Ha identificado alguna problemática relacionada con la evaluación de las competencias en el Diplomado virtual en Seguridad Informática en el ámbito de evaluaciones?
   _____
   _____
   _____
   _____
2. ¿Por qué es importante realizar una evaluación por competencias en dicho Diplomado?
   _____
   _____
   _____
   _____
3. ¿Qué técnicas considera que serían efectivas para la evaluación de competencias en este diplomado?
   _____
   _____
   _____
   _____
4. ¿Cómo considera que podrán evidenciar las competencias adquiridas en el Diplomado?
   _____
   _____
   _____
   _____

   Agradezco su participación en esta recopilación de información, sus contribuciones serán anónimas y únicamente serán utilizadas para esta investigación.

ANEXO 3. Estructura de unidades

Nombre de la unidad 1	Sistemas de información y sistemas informáticos	**Tiempo**	3 días
Competencia específica	Distinguir entre sistema de información y sistema informático		
Contenido	Se explican los conceptos y elementos de sistemas de información y sistemas informáticos.		
Actividades de evaluación	**Descripción de la evaluación**	**Objetivos de aprendizaje o competencia a evaluar**	
Actividad 1.1 Cuestionario de conceptos fundamentales.	Realizar un quizz de 5 cuestionamientos de opción múltiple.	Recordar la información de sistemas de información y sistema informático. **Saberes** ✓ **Conceptual** **Procedimental** **Actitudinal**	
Actividad 1.2 Descripción de los sistemas de información y sistemas informáticos.	Conocer la importancia de tener claro los conceptos de seguridad informática y sistemas de información, además de saber las diferencias entre cada una de ellas, para esto debe contestar de manera reflexiva y critica dos preguntas abiertas.	Identificar los detalles importantes de los sistemas de información y sistema informático. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**	
Actividad 1.3 Analizar los elementos de un sistema información y sistema de informático.	Analizar los conceptos, elementos y diferencias de los sistemas informáticos y de información, para poder resolver un caso práctico de una biblioteca donde pueda identificar los elementos sobre los sistemas.	Utilizar lo que ha aprendido de sistemas de información y sistema informático para crear nuevos conocimientos y aplicarlo en situaciones diversas. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**	

Nombre de la unidad 2	Seguridad	**Tiempo**	3 días
Competencia específica	Comprender qué significa seguridad en el amplio concepto de sistema de información y en el concreto de sistema informático. Conocer cuáles son las propiedades de un sistema seguro.		
Contenido	Se determina la definición de seguridad informática y los conceptos adicionales que se deben saber para establecer un sistema seguro. Es importante tener en cuenta cuales son los tipos de seguridad y las propiedades de un sistema seguro		
Actividades de evaluación	**Descripción de la evaluación**	**Objetivos de aprendizaje o competencia a evaluar** (Propuesta de MSU)	
<u>Actividad 2.1</u> Cuestionario de conceptos de seguridad.	Después de realizar una lectura crítica y reflexiva del contenido de la unidad 2, el alumno podrá elaborar sus propios puntos de vista sobre los conceptos básicos de seguridad, en las 5 preguntas de tipo abierto que abarca esta actividad.	Definir el concepto de seguridad de sistema de información y de sistema informático. **Saberes** ✓ **Conceptual** ✓ **Procedimental** **Actitudinal**	
<u>Actividad 2.2</u> Identificación de concepto de seguridad en un sistema de información y un sistema informático.	Retomando el caso práctico de la Biblioteca de la unidad 2, contestar las 6 cuestiones de tipo abierto sobre la seguridad y las propiedades que deben existir para un sistema seguro.	Identificar los conceptos se seguridad en un sistema de información y sistema informático. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**	
<u>Actividad 2.3</u> Cuestionario de propiedades de un sistema de información seguro.	Relación de columnas de 8 preguntas sobre las propiedades principales de un sistema de información seguro.	Describir las propiedades de un sistema seguro. **Saberes** ✓ **Conceptual** **Procedimental** **Actitudinal**	
<u>Actividad 2.4</u> Identificación de concepto de seguridad y propiedades de un sistema seguro.	Después de identificar los conceptos de seguridad y propiedades de un sistema seguro podrá contestar de forma explícita las 4	Identificar las propiedades de un sistema seguro. **Saberes** ✓ **Conceptual**	

	respuestas que se proponen. Ingresar al siguiente link http://navegacionsegura.es para a través de un juego reafirme los conocimientos, procedimientos y actitudes adquiridas en la unidad 2.	✓ **Procedimental** ✓ **Actitudinal**

Nombre de la unidad 3	Análisis de Riesgos	**Tiempo**	2 días
Competencia específica	Comprender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto		
Contenido	Se muestran los riesgos a los que se afronta un sistema como lo son las amenazas, riegos, vulnerabilidades, ataques e impactos.		
Actividades de evaluación	**Descripción de la evaluación**	**Objetivos de aprendizaje o competencia a evaluar** (Propuesta de MSU)	
<u>Actividad 3.1</u> Cuestionario de conceptos de seguridad.	Son 8 cuestionamientos de tipo abierto sobre las amenazas, riegos e impactos que puede sufrir un sistema de información.	Recordar el concepto de análisis de riesgo y lo que conlleva en seguridad informática. **Saberes** ✓ **Conceptual** ✓ **Procedimental** **Actitudinal**	
<u>Actividad 3.2</u> Identificación de concepto de seguridad en un sistema de información y un sistema informático.	Es el desarrollo de una problemática en un centro de cómputo, donde se tienen que identificar en 4 preguntas abiertas de las amenazas a las que se encuentra vulnerable.	Explicar los riesgos a los que se enfrenta lis sistemas de información. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**	

Nombre de la unidad 4	Control de Riesgos	**Tiempo**	2 días
Competencia específica	Entender lo que son servicios, mecanismos y herramientas de seguridad.		
Contenido	Explicación sobre los servicios de seguridad que se deben de ofrecer para un sistema seguro, a su vez la clasificación de la seguridad en lógica y física.		
Actividades de evaluación	**Descripción de la evaluación**	**Objetivos de aprendizaje o competencia a evaluar** (Propuesta de MSU)	
Actividad 4.1 Cuestionario de control de riesgos.	Una vez analizado el contenido de la unidad 4, se realizan 10 cuestionamientos de opción múltiple en donde se recuerdan los mecanismos de seguridad de un sistema.	Recordar los servicios de seguridad, para un control de riesgos. **Saberes** ✓ **Conceptual** **Procedimental** **Actitudinal**	
Actividad 4.2 Interpretación de control de riesgos.	Está actividad está conformada por 9 preguntas de los cuales son problemas o casos los cuales se tienen que ir contestando de acuerdo a las especificaciones o dificultades que tenga cada caso en particular.	Entender lo que son servicios, mecanismos y herramientas de seguridad. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**	

Nombre de la unidad 5	Herramientas de análisis y gestión de riesgos.	**Tiempo**	4 días
Competencia específica	Aplicación de los conocimientos, herramientas y gestión de riesgos en sistemas informáticos.		
Contenido	El argumento de este tema son las políticas de seguridad que se deben seguir para crear y mantener un sistema seguro.		
Actividades de evaluación	**Descripción de la evaluación**	**Objetivos de aprendizaje o competencia a evaluar** (Propuesta de MSU)	
Actividad 5.1 Cuestionario de herramientas de análisis y gestión de riesgos	Analizar cada uno de los cuestionamientos sobre las herramientas de análisis de riesgos y determinar si las	Recordar las herramientas de análisis y gestión de riesgos.	

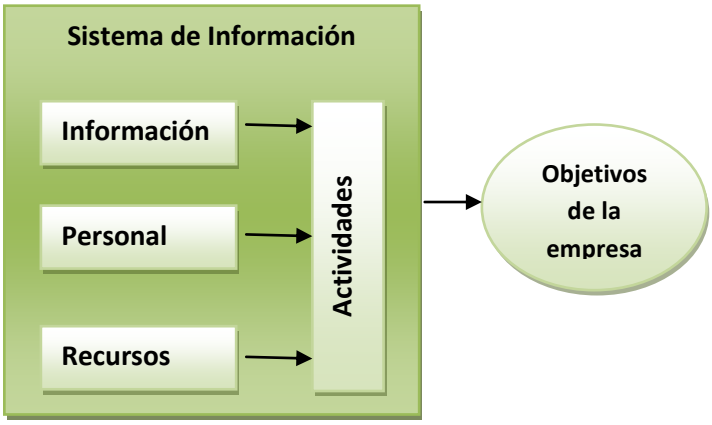
	10 afirmaciones de la actividad son verdaderas o falsas, según corresponda.	**Saberes** ✓ **Conceptual** ✓ **Procedimental** **Actitudinal**
Actividad 5.2 Explicación de las herramientas de análisis y gestión de riesgos informáticos.	Explicar de manera crítica y reflexiva las 4 cuestiones sobre las herramientas de análisis e identificar los riesgos informáticos a los que se enfrenta.	Identificar la importancia de las herramientas de análisis y gestión de riesgos en una empresa. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**
Actividad 5.3 Análisis las herramientas de análisis y gestión de riesgos.	Desarrollar un plan de contingencias de los 3 casos que se manifiestan en esta evaluación.	Utilizar las herramientas de análisis y gestión de riesgos para una empresa. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**
Actividad 5.4 Aplicación de las herramientas de análisis y gestión de riesgos.	Contestar 17 problemáticas referente a problemas de la vida laboral en base a la aplicación de las herramientas de análisis.	Tener la disposición para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**
Actividad 6 Caso práctico inicial Actividad 7 Práctica profesional. Actividad 8 Mundo laboral	Darle solución a las 3 prácticas en base a los conocimientos adquiridos, en el Módulo I. Ingresar al siguiente link http://electronicabarrios.blogspot.mx/2009/10/juego-se-seguridad-informatica.html para que través de un juego reafirme los conocimientos, procedimientos y actitudes adquiridas en el Módulo I.	Proveer una visión del uso de las Tecnologías de la Información y Comunicaciones (TICs) como herramientas fundamentales para el cambio hacia la innovación en la administración de la seguridad informática, dirigidas a proteger su organización y apoyar su desarrollo. **Saberes** ✓ **Conceptual** ✓ **Procedimental** ✓ **Actitudinal**

ANEXO 4. Contenidos de unidades

Contenido 1

Tema 1.1 Sistemas de información y sistemas informáticos

Un **sistema de información** (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus **objetivos.**

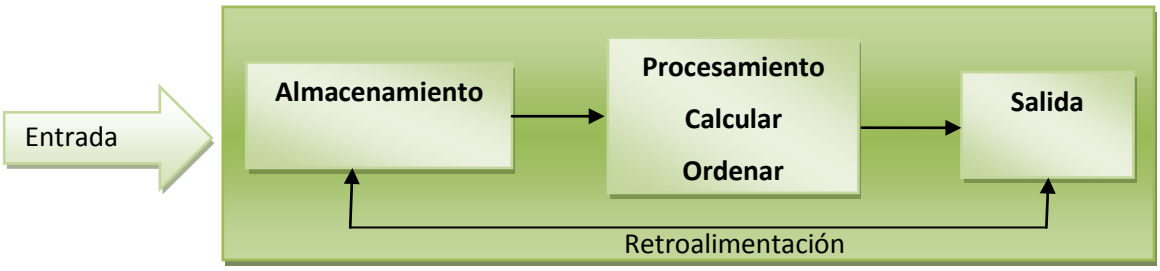


Estos elementos son:

- **Recursos.** Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.
- **Equipo humano.** Compuesto por la organización, relacionadas o no con la informática.
- **Información**. Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.

Actividades que se realizan en la organización, relacionadas o no con la informática.

Un **sistema informático** está constituido por un conjunto de elementos **físicos** (hardware, dispositivos, periféricos y conexiones), **lógicos** (sistemas operativos, aplicaciones, protocolos…) y con frecuencia se incluyen también los elementos **humanos** (personal experto que maneja el software y el hardware).



Un sistema informático puede ser un subconjunto del sistema de información, pero en principio un sistema de información no tiene por qué contener elementos informáticos, aunque en la actualidad es difícil imaginar cualquier actividad humana en la que no se utilice la informática

Contenido 2

Tema 1.2 Aproximación al concepto de seguridad en sistemas de información

Una de las acepciones de la RAE para el término seguro, que es la que aquí nos interesa, es la de estar **libre y exento de todo peligro, daño o riesgo.**

La **seguridad informática** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confía.

Un sistema de información, no obstante las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

- Cuáles son los **elementos** que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos dela organización para la que se hace el estudio de riesgos y mediante apreciación directa.

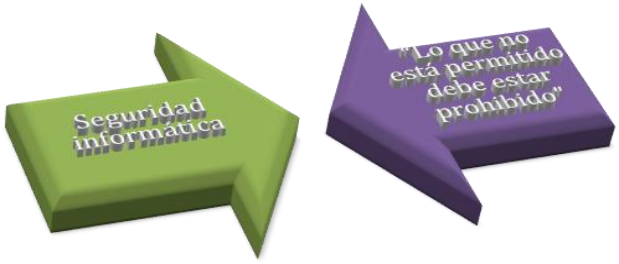
- Cuáles son los **peligros** que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.

- Cuáles son las **medidas** que deberían adoptarse para conocer, prevenir, impedir,

reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico, revisando y actualizando las medidas adoptadas.

Todos los elementos que participan en un sistema de información pueden verse afectados por fallos de seguridad, si bien se suele considerar la información como el factor más vulnerable. El hardware y otros elementos físicos se pueden volver a comprar o restaurar, el software puede ser reinstalado, pero la información dañada no siempre es recuperable, lo que puede ocasionar daños de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es que la mayoría de los fallos de seguridad se deben al factor humano.



Tema 1.2.1 Tipos de Seguridad

Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

Pasiva

Está formada por las medidas que se implantan para, una vez producido el incidente de

seguridad, minimizar su repercusión y facilitar la recuperación del sistema.

Ejemplo: teniendo siempre al día copias de seguridad de los datos.

Tema 1.2.1.1 Propiedades de un sistema de información seguro

Los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización.

Su **origen** puede ser:

- **Fortuito.** Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistema, catástrofes naturales...

- **Fraudulento.** Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

Se considera seguro un sistema que cumple con las propiedades de **integridad, confidencialidad** y **disponibilidad** de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad que se estudiarán más adelante.

Integridad

Este principio *garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita*, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.

Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto.

Confidencialidad

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como «*el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada*».

saber más

Los activos de un sistema de información: datos, software, hardware y sus accesorios, redes, soportes, instalaciones, personal y servicios.

Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

Disponibilidad

La información ha de estar disponible para los usuarios autorizados cuando la necesiten.

El programa MAGERIT define la disponibilidad como «*grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.* Situación que se pro duce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información».

Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido

saber más

MAGERIT

Es una metodología de análisis y gestión de riesgos de los sistemas de información. En ingles *Methodology for Information Systems Risk Analysis and Management.*

Contenido 3

Tema 1.3 Análisis de riesgos

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema.

La persona o el equipo encargado de la seguridad deberán analizar con esmero cada uno de los elementos. A veces el descuido de un elemento considerado débil ha producido importantes fallos de seguridad. Al estar interrelacionados todos los elementos este descuido puede producir errores en cadena con efectos insospechados sobre la organización.

1.3.1 Elementos de estudio

Para comenzar a analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta los siguientes elementos: activos, amenazas, riesgos, vulnerabilidades, ataques e impactos.

Activos

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos. Al hacer un estudio delos activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido a otro.

Podemos clasificarlos en los siguientes tipos:

- **Datos**. Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo. El funcionamiento de una empresa u organización depende de sus datos, que pueden ser de todo tipo: económicos, fiscales, de recursos humanos, clientes o proveedores…

Cada tipo de dato merece un estudio independiente de riesgo por la repercusión que su deterioro o pérdida pueda causar, como por ejemplo los relativos a la intimidad y honor de las personas u otros de índole confidencial.

- **Software**. Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

- **Hardware**. Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información. Incluimos en este grupo los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vía de transmisión de los datos (módem, router, instalación eléctrica o sistemas de alimentación ininterrumpida, destructores de soportes informáticos…).
- **Redes**. Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancia.
- **Soportes**. Los lugares en donde la información queda registrada y almacenada durante largos períodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).
- **Instalaciones**. Son los lugares que albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales o edificios, pero también pueden ser vehículos y otros medios de desplazamiento.
- **Personal**. El conjunto de personas que interactúan con el sistema de información: administradores, programadores, usuarios internos y externos y resto de personal de la empresa. Los estudios calculan que se producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología.
- **Servicios** que se ofrecen a clientes o usuarios: productos, servicios, sitios web, foros, correo electrónico y otros servicios de comunicaciones, información, seguridad, etc.

Amenazas

saber más

Identificar las amenazas y las vulnerabilidades del sistema permitirá conocer los riesgos potenciales que amenazan la seguridad de un sistema.

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que –de tener la oportunidad–atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

En función del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

- **De interrupción**. El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.
- **De interceptación**. Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.
- **De modificación**. Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.
- **De fabricación**. Agregarían información falsa en el conjunto de información del sistema.

Según su origen las amenazas se clasifican en:

- **Accidentales**. Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.
- **Intencionadas**. Son debidas siempre a la acción humana, como la introducción de software malicioso –malware– (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática (con frecuencia se produce previa la introducción de malware en los equipos), robos o hurtos. Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma.

saber más

Algunos tipos de malware:

- Backdoor
- Botnet (Zombies)
- Exploit
- Gusano
- Hoax
- Key logger
- Phishing
- Rogue
- Rootkit
- Spam
- Spyware/Adware
- Troyano

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (por ejemplo, contratando un seguro).

saber más
Analizar los riesgos de un sistema de información requiere un proceso secuencial de análisis de activos, sus vulnerabilidades, amenazas que existen, medidas de seguridad existentes, impacto que causaría un determinado ataque sobre cualquiera de los activos, objetivos de seguridad de la empresa y selección de medidas de protección que cubran los objetivos.

Vulnerabilidades

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Ataques

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza. En función del impacto causado a los activos atacados, los ataques se clasifican en:

- **Activos**. Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.
- **Pasivos**. Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento«víctima» directamente, o a través de recursos o personas intermediarias.

saber más
El ataque cometido por parte de un *hacker* que utiliza ordenadores intermediarios para ocultar la propia identidad (IP) hasta llegar a su objetivo es un ataque indirecto

Impactos

Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

1.3.2. Proceso del análisis de riesgos

Para implantar una política de seguridad en un sistema de información es necesario seguir un esquema lógico.

- Hacer inventario y valoración de los activos.
- Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.
- Identificar y evaluar las medidas de seguridad existentes.
- Identificar y valorar las vulnerabilidades de los activos a las amenazas que les afectan.
- Identificar los objetivos de seguridad de la organización.
- Determinar sistemas de medición de riesgos.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección.

Contenido 4

Tema 1.4 Control de riesgos

Una vez que se ha realizado el análisis de riesgos se tiene que determinar cuáles serán los servicios necesarios para conseguir un sistema de información seguro (epígrafe 2.3). Para poder dar esos servicios será necesario dotar al sistema de los mecanismos correspondientes.

1.4.1 Servicios de seguridad

Integridad

Asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

Confidencialidad

Proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Disponibilidad

Permitirá que la información esté disponible cuando lo requieran las entidades autorizadas.

saber más
Cuando se realiza un análisis de riesgos, hay que detectar qué servicios de seguridad cumple el sistema
de información y cuáles quedan descubiertos o incompletos para poder aplicar los mecanismos necesarios que aseguren la consecución de los objetivos de seguridad de la organización

Autenticación (o identificación)

El sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o que genera una determinada información es quien dice ser. Solo cuando un usuario o entidad ha sido autenticado, podrá tener autorización de acceso. Se puede exigir autenticación en la entidad de origen de la información, en la de destino o en ambas.

No repudio (o irrenunciabilidad)

Proporcionará al sistema una serie de evidencias irrefutables de la autoría de un hecho.

El no repudio consiste en no poder negar haber emitido una información que sí se emitió y en no poder negar su recepción cuando sí ha sido recibida.

De esto se deduce que él no repudio puede darse:

- **En origen**. El emisor no puede negar el envío porque el receptor tiene pruebas certificadas del envío y de la identidad del emisor. Las pruebas son emitidas por el propio emisor.
- **En destino**. En este caso es el destinatario quien no puede negar haber recibido el envío ya que el emisor tiene pruebas

saber más
Hablamos de seguridad física o seguridad lógica según que el mecanismo utilizado para ofrecer seguridad sea físico o lógico.

infalsificables del envío y de la identidad del destinatario. Es el receptor quien crea las pruebas.

saber más
Los mecanismos de seguridad proporcionan servicios de seguridad que reducen tanto las vulnerabilidades del sistema como la intensidad del impacto de posibles ataques a los activos.

Control de acceso

Podrán acceder a los recursos del sistema solamente el personal y usuarios con autorización.

1.4.2 Mecanismos de seguridad

Según la función que desempeñen los mecanismos de seguridad pueden clasificarse en:

- **Preventivos**. Actúan antes de que se produzca un ataque. Su misión es evitarlo.
- **Detectores**. Actúan cuando el ataque se ha producido y antes de que cause daños en el sistema.
- **Correctores**. Actúan después de que haya habido un ataque y se hayan producidos años. Su misión es la de corregir las consecuencias del daño.

Cada mecanismo ofrece al sistema uno o más servicios de los especificados en el epígrafe anterior.

Existen muchos y variados mecanismos de seguridad. En esta sección se mencionan los más habituales, que se detallarán en otras unidades didácticas.

La elección de mecanismos de seguridad depende de cada sistema de información, de su función, de las posibilidades económicas de la organización y de cuáles sean los riesgos a los que esté expuesto el sistema.

saber más
Los mecanismos físicos o lógicos de seguridad tienen como misión prevenir, detectar o corregir ataques al sistema, asegurando que los servicios de seguridad queden cubiertos.

Seguridad lógica

Los mecanismos y herramientas de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa.

- **Control de acceso** mediante nombres de usuario y contraseñas.
- **Cifrado de datos (encriptación).** Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Emisor y receptor son conocedores de la clave y a la llegada del mensaje se produce el descifrado. El cifrado de datos fortalece la confidencialidad.

- **Antivirus**. Detectan e impiden la entrada de virus y otro software malicioso. En el caso de infección tienen la capacidad de eliminarlos y de corregir los daños que ocasionan en el sistema. Preventivo, detector y corrector. Protege la integridad de la información.
- **Cortafuegos (firewall)**. Se trata de uno o más dispositivos de software, de hardware o mixtos que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información.
- **Firma digital**. Se utiliza para la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos (por ejemplo, gestiones en oficinas virtuales). Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o del documento. Protege la integridad y la confidencialidad de la información.
- **Certificados digitales**. Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien dice ser, avalada por la verificación de su clave pública. Protege la integridad y la confidencialidad de la información.

Las redes inalámbricas (WiFi) necesitan precauciones adicionales para su protección:

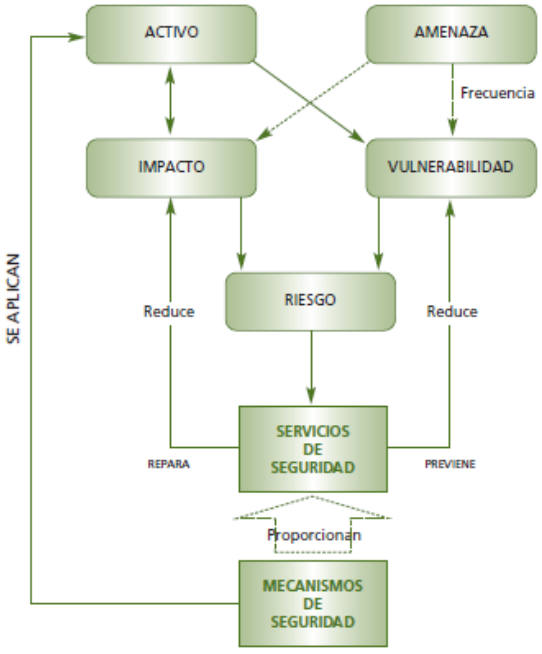
- **Usar un SSID** (Service Set Identifier), es decir, darle un nombre a la red, preferiblemente uno que no llame la atención de terceros que detecten esta red entre las disponibles. Cambiar con cierta frecuencia el SSID.
- **Protección de la red mediante claves encriptadas WEP** (Wired Equivalent Privacy) o WPA (WiFi Protected Access). La clave WEP consume más recursos y es más fácilmente descifrable que la WPA y debería cambiarse con frecuencia. La **WPA** es de encriptación dinámica y mucho más segura al ser más difícil de descifrar. Cambiar periódicamente la contraseña de acceso a la red.
- **Filtrado de direcciones MAC (Media Access Contro**l). Es un mecanismo de acceso al sistema mediante hardware, por el que se admiten solo determinadas direcciones, teniendo en cuenta que cada tarjeta de red tiene una dirección MAC única en el mundo. Puede resultar engorroso de configurar y no es infalible puesto que es posible disfrazar la dirección MAC real.

Seguridad física

Son tareas y mecanismos físicos cuyo objetivo es proteger al sistema (y, por tanto indirectamente a la información) de peligros físicos y lógicos.

- **Respaldo de datos**. Guardar copias de seguridad de la información del sistema en lugar seguro. Disponibilidad.
- **Dispositivos físicos de protección**, como pararrayos, detectores de humo y extintores, cortafuegos por hardware, alarmas contra intrusos, sistemas de alimentación ininterrumpida (para picos y cortes de corriente eléctrica) o mecanismos de protección contra instalaciones. En cuanto a las personas, acceso restringido a las instalaciones; por ejemplo, mediante vigilantes cualquier dispositivos que discrimine la entrada de personal a determinadas zonas.

En este gráfico se puede observar claramente la relación entre mecanismos y servicios de seguridad, y de ambos sobre los activos y los peligros que los acechan.



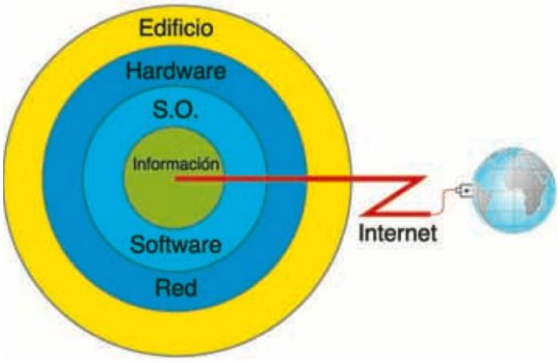
1.4.3 Enfoque global de la seguridad

La información es el núcleo de todo sistema de información. Par a proteger sus propiedades de integridad, disponibilidad y confidencialidad es necesario tener en cuenta a los niveles que la rodean para dotarlos de mecanismos y servicios de seguridad.

Desde el exterior hasta llegar a la información, se pueden definir estos niveles:

- La ubicación física. Edificio, planta o habitaciones, por ser el lugar físico en donde se encuentran ubicados los demás niveles
- El hardware y los componentes de la red que se encuentran en e l interior del entorno físico, porque contienen, soportan y distribuyen la información.
- El sistema operativo y todo el software, porque gestiona la información.
- La conexión a internet, por ser la vía de contacto entre el sistema de información y el exterior.
- La información.

Observa la figura siguiente para comprobar que la conexión a internet atraviesa los distintos niveles hasta llegar a la información: En el edificio habrá antenas, cableado en los muros, etc. Entre el hardware contamos con routers, switches, ordenadores, servidores, periféricos, etc. El sistema operativo y el software gestionan los accesos a internet. La información es el bien preciado que no se debe descuidar, pues desde internet solamente se podrá acceder a una parte de ella y siempre que los usuarios tengan autorización. Una vez más aludimos al personal de la empresa que puede actuaren todos los niveles o en parte de ellos y por lo tanto es un factor a tener en cuenta.



Contenido 5

Tema 1.5 Políticas de seguridad

Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la

dirección.

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización.

No todas las políticas de seguridad son iguales. El contenido depende de la realidad y de las necesidades de la organización para la que se elabora.

Existen algunos estándares de políticas de seguridad por países y por áreas (gobierno, medicina, militar...), pero los más internacionales son los definidos por la ISO (International Organization for Standardization).

Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de información, generalmente englobados en cuatro grupos:

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- Relacionar todas las medidas de seguridad que deben implementarse para afrontar los riesgos de cada activo o grupo de activos.
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización
- Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- Definir un plan de contingencias.

saber más

Los objetivos y normas de seguridad están recogidos en la política de seguridad de la organización. Para la consecución de objetivos, el personal debe estar informado de cuál es la política de seguridad de la empresa.

La auditoría es un análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan. Su finalidad es verificar que se cumplen los objetivos de la **política de seguridad** de la organización. Proporciona una imagen real y actual del estado de seguridad de un sistema de información.

Tema 1.5.1 Auditoría

Tras el análisis e identificación de vulnerabilidades, la persona o equipo encargado de la auditoría emite un **informe** que contiene, como mínimo:

- Descripción y características de los **activos** y **procesos** analizados.
- Análisis de las **relaciones y dependencias** entre activos o en el proceso de la información.
- Relación y evaluación de las **vulnerabilidades** detectadas en cada activo o subconjunto de activos y procesos.
- Verificación del cumplimiento de la **normativa** en el ámbito de la seguridad.
- Propuesta de **medidas** preventivas y de corrección.

Para evaluar la seguridad de un sistema de información se necesitan herramientas de análisis:

- **Manuales.** Observación de los activos, procesos y comportamientos, mediciones, entrevistas, cuestionarios, cálculos, pruebas de funcionamiento.
- **Software específico para auditoría.** Se le reconoce por las siglas CAAT *(**C**omputer **A**ssisted **A**udit **T**echniques)*. Los CAATS son herramientas de gran ayuda para mejorar la eficiencia de una auditoría, pudiendo aplicarse sobre la totalidad o sobre una parte del sistema de información. Proporcionan una imagen en tiempo real del sistema de información, realizan pruebas de con trol y emiten informes en los que señalizan las vulnerabilidades y puntos débiles del sistema, así como las normativas que podrían estar incumpliéndose.

La auditoría puede ser **total,** sobre todo el sistema de información, o **parcial,** sobre determinados activos o procesos. La auditoría de un sistema de información puede realizarse:

- Por personal capacitado perteneciente a la propia empresa.
- Por una empresa externa especializada.

1.5.2 Plan de contingencias

Determinadas amenazas a cualquiera de los activos del sistema de información pueden poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.

El plan de contingencias consta de tres sub planes independientes:

- **Plan de respaldo**. Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en lugar seguro copias de seguridad de la información, instalar pararrayos o hacer simulacros de incendio.
- **Plan de emergencia**. Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse. Por ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.
- **Plan de recuperación**. Indica las medidas que se aplicarán cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento del sistema y de la organización. Por ejemplo, tener un lugar alternativo donde continuar la actividad si el habitual hubiese sido destruido, sustituir el material deteriorado, reinstalar aplicaciones y restaurar copias de seguridad.

La elaboración del plan de contingencias no puede descuidar al personal de la organización, que estará informado del plan y entrenado para actuar en las funciones que le hayan sido encomendadas en caso de producirse una amenaza o un impacto.

1.5.3 Modelos de seguridad

Un modelo de seguridad es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información. Al decir formal queremos expresar

que estará redactado fundamentalmente en términos técnicos y matemáticos.

Clasificación

En relación a las funciones u operaciones sobre las que se ejercen mayor control podemos clasificar los modelos de seguridad en tres grandes grupos:

- **Matriz de acceso.** Este modelo considera tres elementos básicos: sujeto, objeto y tipo de acceso. Un sujeto tiene autorización de acceso total o parcial a uno o más objetos del sistema. Aplicable a cualquier sistema de información, controla tanto la confidencialidad como la integridad de los datos.

- **Acceso basado en funciones de control** (RBAC –Role-Access Base Control–). Puede considerarse una modalidad del de matriz de acceso, pero, en este caso, el acceso no se define en función de quién es el sujeto, sino de qué función tiene. Por ejemplo, un determinado individuo puede ser alumno de una universidad en cuanto que está estudiando una carrera, pero también puede ser profesor de la universidad en otra especialidad distinta de la misma universidad. Tratándose del mismo individuo, en calidad de profesor tendrá un tipo de acceso al sistema y en calidad de alumno tendrá otro. También controla la confidencialidad y la integridad de los datos.

- **Multinivel**. Este modelo se basa en la jerarquización de los datos (todos los datos son importantes pero unos son más privados que otros. Por ejemplo, el nivel de protección de datos personales ha de ser superior que los nombres de los artículos con los que comercia una empresa). Los usuarios tendrán acceso a un nivel u otro de la jerarquía en función de las autorizaciones que les hayan sido dadas. Este nivel controla el flujo de datos entre los niveles de la jerarquía. Ejemplos de este grupo son el modelo Bell-La Padula (controla la confidencialidad) y el modelo Biba (controla la integridad).

ANEXO 5. Actividades de evaluación

Actividad 1.1 Cuestionario de conceptos fundamentales.

Instrucciones: Contesta las siguientes interrogantes, con el inciso apropiado.

1. Un SI es:
    a. Sistema Informático
    b. Sistema de Información
    c. Sistema Integral

2. Un sistema de información es un:
    a. Es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de conseguir los objetivos de la empresa.
    b. Es un conjunto de elementos organizados, físicos, lógicos y con frecuencia se incluyen los elementos humanos.
    c. Conjunto de actividades de entrada, almacenamiento, procesamiento, salida y retroalimentación.

3. Los elementos en un sistema de información son:
    a. Elementos, físicos, lógicos y con frecuencia se incluyen los elementos humanos.
    b. Conjunto de actividades de entrada, almacenamiento, procesamiento, salida y retroalimentación.
    c. Recursos, equipo humano, información y actividades.

4. Los sistemas informáticos está constituido por:
    a. Un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de conseguir los objetivos de la empresa.
    b. Un conjunto de elementos organizados, físicos, lógicos y con frecuencia se incluyen los elementos humanos.
    c. Conjunto de actividades de entrada, almacenamiento, procesamiento, salida y retroalimentación.

5. Las actividades en un sistema informático son:
    a. Entrada, almacenamiento, procesamiento y salida.
    b. Entrada, procesamiento, salida y retroalimentación.
    c. Entrada, almacenamiento, procesamiento, salida y retroalimentación.

Actividad 1.2 Discusión de sistemas de información y sistemas informáticos.

Instrucciones: Responde el siguiente cuestionamiento en base a los conocimientos adquiridos.

Expresa, ¿por qué es importante en Seguridad informática, tener claro los conceptos de *Sistema de información* y *Sistema informático?*

Manifiesta cuáles son las principales diferencias entre *Sistema de información* y *Sistema informático.*

En cooperación con las personas que laboras en tu área, formula la importancia de estos términos, para tu área laboral. *(Interés en acompañar a las otras personas en la resolución de sus problemas. Valor Solidaridad.)*

Actividad 1.3 Análisis de los elementos de un sistema información y sistema de informático.

Instrucciones: Indica a continuación de cada elemento con un **sí**, si forma parte de un sistema informático y con un **no** si no forma parte de él.

1. La biblioteca pública de una ciudad tiene mobiliario, libros, revistas, microfilms, varios ordenadores para los usuarios en donde pueden consultar libros electrónicos, y un ordenador en el que la bibliotecaria consulta títulos, códigos, referencias y ubicación del material bibliográfico.

a) Libros y revistas colocados en las estanterías.

b) Mobiliario.

c) Microfilms.

d) Libros electrónicos.

e) Ordenadores de los usuarios.

f) Ordenador de la bibliotecaria.

g) Datos almacenados en el ordenador de la bibliotecaria.

h) Bibliotecaria.

2. De los elementos relacionados en la pregunta anterior, ¿cuáles pertenecen al sistema de información de la biblioteca?

3. Incorpora los conceptos de Sistema Informático y Sistema de Información en el área donde laboras, y realiza un listado de los elementos que forman parte de un Sistema Informático y otro listado de los cuales pertenecen al sistema de información. *(Actitud a nuevos conocimientos. Valor Amor por el saber.)*

4. ¿Cuáles son los retos en los que te enfrentaste al realizar el análisis anterior?

5. ¿Cómo superarías estos retos?

Actividad 2.1 Cuestionario de conceptos de seguridad

Instrucciones: Lee con atención los siguientes enunciados e identifica sí son verdaderos o falsos.

1. RAE es estar libre y exento de todo peligro, daño o riesgo.
2. Seguridad informática es una disciplina que se ocupa de diseñar normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y malicioso.
3. Para afrontar el establecimiento de un sistema seguro es necesario conocer: el personal que labora en el organismo, las debilidades y éxitos con los que cuenta el sistema de información.
4. Los elementos que componen el sistema, son útiles para el hacer estudio de riesgos.

5. La información dañada no siempre es recuperable, lo que puede ocasionar ciertas ventajas de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas.

Actividad 2.2 Identificación de concepto de seguridad y propiedades de un sistema seguro

Instrucciones: Contesta los siguientes cuestionamientos, de acuerdo al caso de la actividad 1.3

1. Un incendio fortuito destruye completamente todos los recursos de la biblioteca. ¿En qué grado crees que se verían comprometidas la integridad, la confidencialidad y la disponibilidad de la información? (Actitud Disposición a compartir lo que se tiene. Valor Solidaridad)
2. El informático que trabaja para la biblioteca, ¿forma parte del sistema informático de la misma?
3. El ordenador de la biblioteca tiene un antivirus instalado, ¿esto lo hace invulnerable?
4. ¿A qué se deben la mayoría de los fallos de seguridad? Razona tu respuesta.
5. ¿Podrías leer un mensaje encriptado que no va dirigido a ti? Busca en internet algunos programas que encriptan mensajes.
6. ¿La copia de seguridad es una medida de seguridad pasiva?
7. Busca en internet algunos avances e innovaciones tecnológicas los cuales puedan apoyar en la situación de la Biblioteca en reforzar la integridad, confidencialidad y disponibilidad de la información. (Actitud Actualización permanente en una determinada área. Valor Amor por el saber)

Actividad 2.3 Cuestionario de propiedades de un sistema de información seguro

Instrucciones: Relaciona ambas columnas:

a) Fortuito	( ) Garantiza autenticidad y precisión de la información sin importar el momento en que se solicite.
b) Fraudulento	( ) Metodología de análisis y gestión de riesgos de los sistemas de información.
c) Propiedades de un sistema	( ) Organización para la cooperación y el Desarrollo Económico
d) Integridad	( ) Daños causados por software malicioso, intruso o por la mala voluntad del personal, robo o accidentes provocados.
e) Confidencialidad	( ) Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.
f) OCDE	( ) Integridad, confidencialidad y disponibilidad
g) Disponibilidad	( ) Son errores cometidos accidentalmente por los usuarios, accidentes, cortes eléctricos, averías del sistema, catástrofes naturales.
h) MAGERIT	( ) Los datos o información estén únicamente al alcance del conocimiento de personas, entidades o mecanismos autorizados.

Actividad 2.4 Identificación de concepto de seguridad y propiedades de un sistema seguro

Instrucciones: Contesta los siguientes cuestionamientos, de acuerdo a los conocimientos que lograste de las propiedades de un sistema seguro.

1. ¿Qué propiedades debe cumplir un sistema seguro?
2. ¿Qué garantiza la integridad?

3. ¿Por qué es importante que un sistema cumpla con todas las propiedades de seguridad?
4. En el caso de la biblioteca, ¿Qué acciones realizarías para garantizar las propiedades de un sistema seguro? (Actitud Disposición a compartir lo que se tiene. Valor Solidaridad)
5. En el área donde laboras identifica las fortalezas y debilidades con el que cuentan para tener un sistema seguro, y realiza un plan de acciones necesarias para garantizar la seguridad de su sistema. (Actitud Tener en cuenta las necesidades y dificultades de otras personas. Valor Solidaridad.)

Actividad 3.1 Cuestionario de análisis de riesgos

Instrucciones: Lee con atención y contesta las siguientes cuestiones.

1. ¿Qué se debe tener en cuenta para dotar de seguridad un sistema de información?
2. ¿Qué elementos se deben tomar en cuenta para la seguridad de un sistema de información?
3. Los activos, ¿Cómo se clasifican?
4. ¿Qué son las amenazas?
5. Las amenazas, ¿Cómo se clasifican?
6. ¿Qué son los riesgos?
7. ¿Qué es un impacto?
8. Los impactos, ¿Cómo pueden ser?
9. En base a los conocimientos adquiridos en las preguntas anteriores, realiza un listado de activos que existan en tu área donde laboras, además las amenazas y riesgos a los que se enfrentan su sistema de información.
10. Realiza un escrito con el registro de las dificultades y la superación de estas al realizar el punto anterior (Actitud Motivación hacia el logro).

Actividad 3.2 Explicación de riegos

Instrucciones: Razona las siguientes problemáticas, y contesta.

1. La ventana de un centro de cálculo en donde se encuentran la mayor parte de los ordenadores y el servidor de una organización se quedó mal cerrada. Durante una

noche de tormenta, la ventana abierta ¿constituye un riesgo, una amenaza o una vulnerabilidad? Razona la respuesta.

2. Teniendo en cuenta las propiedades de integridad, disponibilidad y confidencialidad, indica cuáles de estas propiedades se verían afectadas por:
    a) Una amenaza de interrupción.
    b) Una amenaza de interceptación.
    c) Una amenaza de modificación.
    d) Una amenaza de fabricación.

3. Menciona un ejemplo de cómo un sistema de información podría ser seriamente dañado por la presencia de un factor que se considera de poca relevancia y que explique de alguna manera que «La cadena siempre se rompe por el eslabón más débil».

4. ¿Qué elementos se deben estudiar para hacer un análisis de riesgos?

Actividad 4.1 Cuestionario de Control de Riesgos

Instrucciones: Lee con atención y selecciona la respuesta que contesta las siguientes cuestiones.

1. Los servicios de seguridad son:
    a) Integridad, confidencialidad, disponibilidad, autentificación, no repudio y control de acceso.
    b) Preventivos, Detectores y Correctores.
    c) Confidencialidad, detectores, disponibilidad y preventivos.

2. Los mecanismos de seguridad son:
    a) Integridad, confidencialidad, disponibilidad, autentificación, no repudio y control de acceso.
    b) Preventivos, Detectores y Correctores.
    c) Detectores, disponibilidad, preventivos y confidencialidad.

3. Los mecanismos y herramientas de seguridad lógica tienen como objetivo:
   a) Proteger físicamente la información de manera directa.
   b) Proteger física y digitalmente la información de manera directa.
   c) Proteger digitalmente la información de manera directa.

4. Los mecanismos de seguridad lógica son:
   a) Respaldo de datos y dispositivos físicos.
   b) Control de acceso, cifrado de datos, antivirus, cortafuegos, firma digital, certificados digitales, SSID, WEP, MAC.
   c) Respaldo de datos, dispositivos físicos, SSID,WEP, MAC

5. La seguridad física es la encargada de:
   a) Proteger al sistema de peligros físicos y lógicos.
   b) Respaldo de datos y dispositivos físicos.
   c) Proteger digitalmente la información de manera directa.

6. Los mecanismos de seguridad física son:
   a) Respaldo de datos y dispositivos físicos.
   b) Control de acceso, cifrado de datos, antivirus, cortafuegos, firma digital, certificados digitales, SSID, WEP, MAC.
   c) Respaldo de datos, dispositivos físicos, SSID, WEP, MAC

7. La seguridad de la información implica a todos los niveles que la rodean:
   a) Edificio y habitaciones, Hardware.
   b) Edificio y habitaciones, Hardware y red interna, Sistema operativo y software, Conexión a Internet.
   c) Edificio y habitaciones, Hardware y SSID, Sistema operativo y software y Control de accesos.

8. La ubicación física es:
   a) Es el software que gestiona la información
   b) El lugar físico en donde se encuentran ubicados los demás niveles.
   c) Es el contacto entre el sistema de información y el exterior.

9. El sistema operativo es:
    a) Es el software que gestiona la información
    b) El lugar físico en donde se encuentran ubicados los demás niveles.
    c) Es el contacto entre el sistema de información y el exterior.

10. La conexión a internet es:
    a) Es el software que gestiona la información
    b) El lugar físico en donde se encuentran ubicados los demás niveles.
    c) Es el contacto entre el sistema de información y el exterior.

Actividad 4.2 Interpretación de Control de Riesgos

Instrucciones: Razona las siguientes problemáticas, y contesta.

1. Investiga el término *wardriving,* que también puede expresarse como *wardriving*o *warxing*. ¿Crees que el *wardriving* constituye un riesgo contra la confidencialidad?

2. ¿Qué relación hay entre servicios de seguridad y mecanismos de seguridad?

3. ¿Qué es el SSID de una red WiFi?

4. ¿Podrías explicar qué significa encriptar un mensaje? Inventa un sencillo sistema de encriptación (codificación).Imagina que envías a otra persona unas palabras codificadas según tu sistema inventado. ¿Qué necesita tener o saber la persona que recibe tu mensaje para poder descifrarlo?

5. De los siguientes dispositivos indica cuáles son preventivos, detectores o correctores:
    a) Cortafuegos *(firewall).*
    b) Antivirus.
    c) Extintor de fuegos.
    d) Detector de humos.
    e) Firma digital.

6. Imagina esta situación: Quieres presentar a tu jefe una brillante idea que puede interesar a la competencia, pero te encuentras de fin de semana en un pueblecito donde los teléfonos móviles no funcionan, por suerte te has llevado tu portátil y el hotel rural donde te encuentras alojado dispone de servicio de internet. Así que decides enviarle un correo electrónico pero sin encriptar. Explica los peligros de este procedimiento.

7. Investiga qué es la estenografía.

8. ¿Cómo escogerías una clave segura de acceso al ordenador de una empresa donde se guardan datos confidenciales de clientes?

9. Trabajas como técnico de informática y te llega una llamada de una oficina. Un empleado hacía cada semana una copia de seguridad de la carpeta Documentos Importantes. La copia la guardaba en otra partición del mismo disco duro. Una tormenta eléctrica ha dañado el disco y un experto en informática no ha hallado modo de restablecer su funcionamiento. Te piden que te acerques a la oficina para ver si existe la posibilidad de recuperar al menos los datos. a) ¿Podrás recuperar los datos originales? b) En su defecto, ¿podrán recuperarse los que hay en la copia de seguridad? c) A tu juicio, ¿el empleado ha cometido alguna imprudencia con la copia de seguridad?

Actividad 5.1 Cuestionario de herramientas de análisis y gestión de riesgos

Instrucciones: Lee con atención los siguientes enunciados e identifica sí son Verdaderos o falsos.

1. Todas las políticas de seguridad son iguales.

2. Las políticas de seguridad internacionales son definidas por la ISO.

3. Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de ventas.

4. La auditoría es un análisis general de un sistema de información que permite identificar las vulnerabilidades en los procesos que se realizan.

5. El plan de contingencias es un instrumento de gestión que contiene las medidas que garanticen la continuidad del negocio; protegiendo el sistema de información de los peligros que lo amenazan.

6. El plan de contingencias consta de tres subplanes dependientes.

7. Un modelo de seguridad es la expresión de una política y se utiliza como directriz para evaluar la infraestructura de la empresa.

8. La clasificación de los modelos de seguridad son matriz de acceso, RBCA, y multinivel.

9. La matriz de acceso considera tres elementos básicos: sujeto, objeto y tipo de acceso.

10. El multinivel se basa en la jerarquización de las conexiones de red y sistemas operativos.

Actividad 5.2 Explicación de las herramientas de análisis y gestión de riesgos informáticos.

Instrucciones: Razona y contesta los siguientes cuestionamientos.

Manifiesta porqué es transcendental disponer de políticas de seguridad en cualquier empresa.

Explica el motivo por el cual la auditoría permite descubrir, identificar y corregir vulnerabilidades en los activos.

Menciona que aspectos deberías tomar en cuenta para realizar un plan de contingencias, en el área que laboras

Las políticas de seguridad tienen el mismo funcionamiento si se omite su modelo de seguridad.

Después de dar respuesta a las preguntas anteriores, ¿qué consideras que es lo más valioso que aprendiste?

Actividad 5.3 Análisis de las herramientas de análisis y gestión de riesgos informáticos.

Instrucciones: Responde el siguiente cuestionamiento en base a los conocimientos adquiridos**.**

1. De acuerdo al ejemplo de la biblioteca pública, ¿qué políticas de seguridad establecerías de acuerdo a los estándares internacionales definidos por la ISO?

2. Para evaluar la seguridad del sistema de información de la biblioteca pública ¿qué herramienta de auditoría utilizarías, manuales o Software específico para auditoría?

3. La biblioteca pública (caso actividad 1.1) requiere de un plan de contingencias, elabora las medidas preventivas, paliativas de recuperación de desastres que requiere de acuerdo a sus necesidades.

Actividad 5.4 Aplicación de las herramientas de análisis y gestión de riesgos.

Instrucciones: Razona las siguientes problemáticas, y contesta.

1. Investiga qué es un test de intrusión.

2. Tu jefe te dice que ha detectado que el rendimiento de los trabajadores ha bajado considerablemente desde que la empresa tiene acceso a internet. Te pide que le propongas una solución.

3. En tu empresa acaban de crear unas claves de seguridad para los empleados. Dichas claves se envían por correo electrónico. ¿Esto es desconocimiento de las prácticas de seguridad?

4. El hecho de preparar un plan de contingencias, ¿implica un reconocimiento de la ineficiencia en la gestión de la empresa?

5. ¿Cuál es la orientación principal de un plan de contingencia?

6. Investiga: diferencias entre redes cableadas y redes inalámbricas WIFI.

7. ¿En qué se basa la recuperación de la información?

8. Tu jefe te pide que le hagas una buena política de copias de seguridad para que sea seguida por todos los trabajadores de la empresa. ¿Qué deberá contemplar?

9. Trabajas en una empresa donde además de la oficina central, hay una red de oficinas por varias ciudades. Se elabora un plan de contingencias exclusivamente para la oficina central, ¿es esto correcto?

10. En tu empresa se desarrolla un plan de contingencias que entre otras muchas situaciones, cubre las siguientes: un corte en la corriente eléctrica, el sol pasando a través de un cristal en pleno agosto, derramar una bebida en el teclado o sobre el monitor, olvidarse el portátil en un taxi, el robo del ordenador.

11. ¿Crees que cubrir estos puntos es acertado?

12. ¿Una misma política de seguridad puede servir a todo tipo de empresas?

13. ¿De qué modo debe ser redactada la política de seguridad de una organización?

14. Define con tus propias palabras qué es un plan de contingencias.

15. Investiga en internet sobre empresas especializadas en auditorías de sistemas de información (sugerencias: Hipasec, Audisis). Escoge una de estas empresas y contesta las siguientes preguntas:

    a) ¿En qué fases realiza la auditoría?

b) ¿Qué tipos de auditoría realiza?

c) ¿Ofrece revisiones periódicas del sistema?

16. Investiga en internet para encontrar el software de auditoría: CaseWare, WizSoft, Ecora, ACL, AUDAP u otros. Escoge uno o varios y haz una lista de las operaciones que realiza para llevar a cabo la auditoría.

17. Averigua qué información tiene wikipedia sobre el modelo de seguridad Bell-LaPadula. Escribe la definición que hace del modelo.

Actividad 6 Caso práctico inicial

Instrucciones: leer con atención el siguiente caso y contesta las preguntas que se presentan en la parte final.

Una clínica dental se dirige a una empresa de servicios informáticos solicitando un estudio de sus equipos e instalaciones para determinar el grado de seguridad informática y los ajustes que se consideren necesarios. Un trabajador de la empresa informática se dirige a la clínica y mantiene una entrevista con el titular de la misma, quien le informa delos siguientes aspectos:

El personal de la clínica está formado por: el titular, médico especialista en odontología. Como contratados: otro odontólogo, dos auxiliares de clínica y un auxiliar administrativo, que también ejerce como recepcionista, y una persona para la limpieza.

La clínica cuenta con dos consultas, cada una de ellas con un especialista en odontología. En cada consulta hay un ordenador desde el que pueden consultar la base de datos de pacientes tanto el especialista como el auxiliar de clínica que trabaja en esa consulta. En recepción hay otro ordenador con un programa de tipo agenda para consultar las horas libres y anotar las citas. En un despacho aparte están los archivos en soporte papel y donde se encuentra el servidor.

Todos los ordenadores tienen sistema operativo Windows, excepto el servidor que es Linux.

El objetivo de la clínica es proteger la información, especialmente la relativa a los historiales médicos de sus pacientes.

1. Elabora un listado de los activos de la clínica.

- ¿Cuáles son los activos?

2. Observa qué sistemas de seguridad física y lógica están protegiendo actualmente el sistema. Si están revisados y actualizados.

- ¿Qué es seguridad física y lógica?

3. Comprueba cuáles son las vulnerabilidades del sistema informático, tanto en el software, como en el hardware, el personal y las instalaciones.

- ¿Qué propiedades debe tener el sistema de información para ser seguro?
- ¿Qué amenazas y riesgos existen?
- ¿Qué vulnerabilidades tiene el sistema?

4. Elabora una lista de servicios y mecanismos que incrementarían la seguridad de la información.

- ¿Qué servicios de seguridad se necesitan y qué mecanismos son necesarios para asegurar esos servicios?

5. Investiga si la clínica dispone de una política de seguridad de un plan de contingencias.

- ¿Está informado todo el personal de la política de seguridad?
- ¿Se realizan ensayos y simulacros según el plan de contingencias?

6. Determina si la clínica requiere una auditoría informática.

- ¿En qué consistirá la auditoría?
- ¿Se realizará con algún software específico para auditoría informática?

Actividad 7 Práctica profesional

ESTUDIO DE LA SEGURIDAD DE UNA EMPRESA

Empresa: asesoría laboral y fiscal.

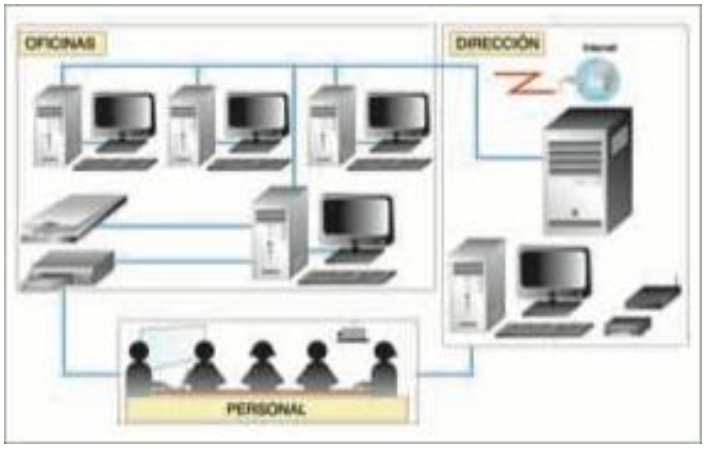
Instalaciones: una oficina, una sala de reuniones y el despacho de dirección. Protección contra incendios y alarma contra intrusos.

Oficina: cuatro ordenadores en la oficina. Uno de ellos tiene conectados dos periféricos: una impresora y un escáner. Todos los ordenadores van conectados mediante cable a un servidor.

Dirección: un ordenador con conexión inalámbrica a la red. Un servidor conectado a internet. Además, en dirección se encuentra el archivo de todas las copias de seguridad de los datos, que se generan una vez al día.

Sala de reuniones: mesa y sillas para reuniones, un portátil, pantalla y proyector.

Recursos humanos: cinco personas, de ellas cuatro trabajan en la oficina; la directora de la asesoría, en su despacho.



Software: sistemas operativos, aplicaciones específicas para gestorías y asesorías, antivirus.

Situación: la asesoría tiene definida su política de seguridad, conocida por todo el personal. Recientemente le ha sido realizada una auditoría informática, y el estado de seguridad ha sido calificado como óptimo. Sin embargo, el ordenador de la dirección, debido a un pico de corriente ha sufrido daños en la placa base y el disco duro. Ambos elementos deben ser reemplazados. La información contenida en el disco duro había sido previamente copiada y se encuentra archivada.

Resuelve

Con los conocimientos que posees tras haber estudiado esta unidad:

1. Enumera los activos del sistema de información de la asesoría.
2. ¿Se ha producido algún ataque? En caso afirmativo, responde cuál ha sido.
3. ¿Crees que ha sido importante para la empresa el impacto por los daños en la placa base y el disco duro? Comenta tu impresión.
4. Investiga si existe algún medio para evitar que los picos de corriente puedan dañar equipos o dispositivos físicos de un sistema informático.
5. El disco duro inutilizado contenía información personal y fiscal de clientes de la asesoría. Se ha decidido tirar- lo a la basura, pero una empleada dice que ese método no es seguro. Haz tus investigaciones y comenta si has averiguado que la empleada está o no en lo cierto.

Actividad 8 Mundo Laboral

LAS PERSONAS SON EL ESLABÓN DÉBIL EN LA CIBERSEGURIDAD

La popularidad de Facebook y otros sitios muy visita- dos de redes sociales ha dado a los nuevas vías para robar dinero e información, dijo la compañía de seguridad Sophos en un reporte publicado el miércoles.

Cerca de la mitad de las compañías bloquea parcial o completamente el acceso a las redes sociales debido a la preocupación por ciber-incursiones a través de esos sitios, de acuerdo al estudio.

«Los resultados de las investigaciones también revela- ron que un 63 por ciento de los administradores de sistemas están preocupados porque sus empleados comparten demasiada información personal a través de los sitios de redes sociales, lo que pone su infraestructura corporativa –y los datos sensibles almacenados en ella– en riesgo», dijo el reporte de Sophos.

Esto ocurre a pesar de años de exhortaciones a los usuarios de computadoras respecto a que deberían mantener su información personal en privado y abstenerse de abrir archivos adjuntos de correos electrónicos provenientes de fuentes no conocidas.

Uno de los resultados es que una cuarta parte de los negocios ha sido afectada por tácticas como el o los ataques de software malicioso a través de Twitter u otras redes sociales, dijo Sophos.

El envío de correos electrónicos a través de los cuales los estafadores tratan de convencer a sus potenciales víctimas para que revelen información personal como contraseñas o cuentas bancarias.

Sophos también descubrió que la cantidad de páginas web con software malicioso se cuadruplicó desde principios del 2008, y un 39,6 por ciento de ellas tiene sede en Estados Unidos, que alberga más que cualquier otro país. China es el segundo, con 14,7 por ciento.

Sophos, que tiene sedes en Gran Bretaña y Estados Unidos, es el mayor fabricante de software de capital privado.

Reuters

Reporte de Diane Bartz; editado en español por Hernán García

http://lta.reuters.com/article/internetNews/ idLTASIE56L08920090722

Washington, miércoles 22 de julio de 2009.

Actividades

Lee el artículo y en vista de su contenido responde a las siguientes cuestiones:

1. ¿Qué propiedades de seguridad del sistema de información podrían verse vulneradas por negligencias cometidas por empleados de la empresa al publicar sus datos personales en redes sociales?

2. Indica alguna manera de que los administradores de un sistema de información puedan impedir que el personal de la empresa acceda a sitios que podrían poner en peligro las propiedades de seguridad del sistema.

3. ¿Qué proporción de negocios se ven afectados por o software malicioso debido al uso indebido de re- des sociales por parte de los empleados?

4. En tu opinión, ¿consideras cierta la afirmación de que se producen más fallos de seguridad por la intervención humana que por errores en la tecnología?

ANEXO 6. Porcentaje de actividades

Módulo I Introducción a la Seguridad Informática y al Aseguramiento de Información

Actividades y Porcentaje

Unidad	Nombre de la unidad	Porcentaje
1	**Sistemas de información y sistemas informáticos**	**15%**
	Actividad 1.1 Cuestionario de conceptos fundamentales.	**5%**
	Actividad 1.2 Descripción de los sistemas de información y sistemas informáticos.	**5%**
	Actividad 1.3 Analizar los elementos de un sistema información y sistema de informático.	**5%**
2	**Seguridad**	**20%**
	Actividad 2.1 Cuestionario de conceptos de seguridad	**5%**
	Actividad 2.2 Identificación de concepto de seguridad en un sistema de información y un sistema informático	**5%**
	Actividad 2.3 Cuestionario de propiedad de un sistema de información seguro.	**5%**
	Actividad 2.4 Identificación de concepto de seguridad y propiedades de un sistema seguro.	**5%**
3	**Análisis de riegos**	**10%**
	Actividad 3.1 Cuestionario de análisis de riesgos.	**5%**
	Actividad 3.2 Explicación de riegos.	**5%**
4	**Control de riesgos**	**10%**

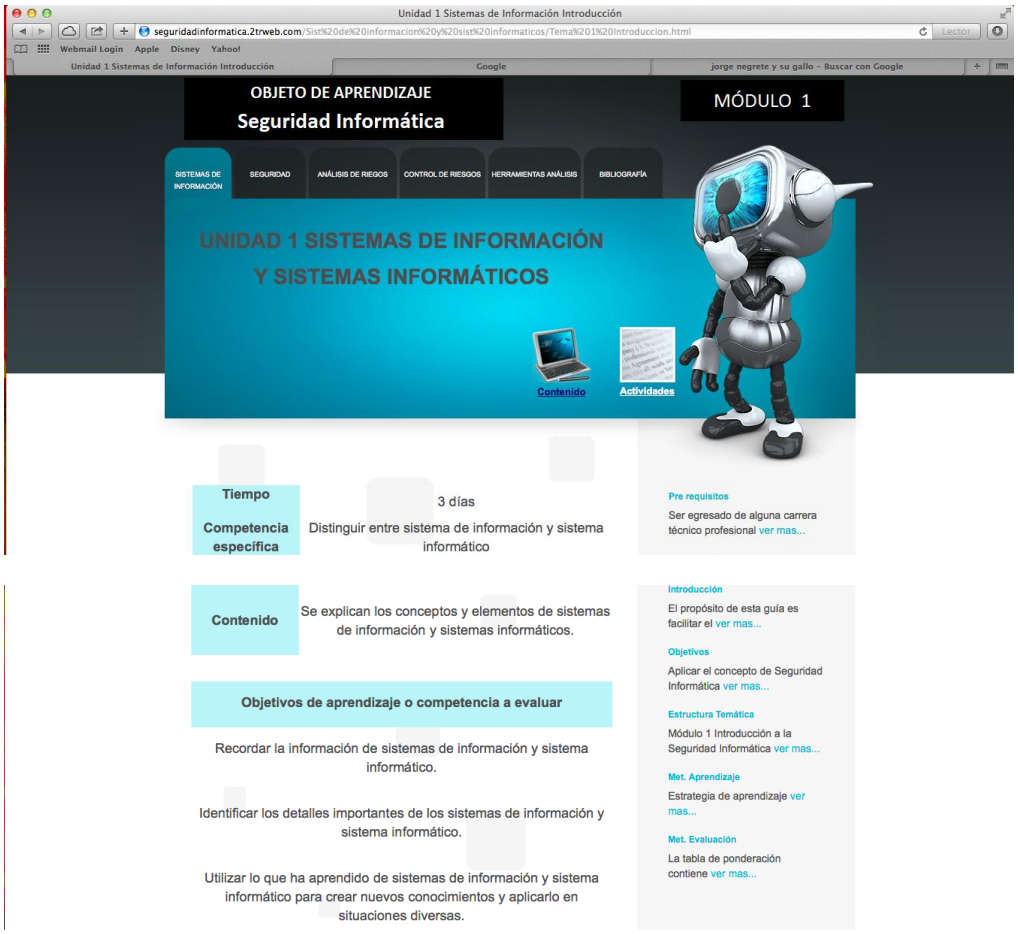
	Actividad 4.1 Cuestionario de control de riesgos.		**5%**
	Actividad 4.2 Interpretación de control de riesgos		**5%**
5	**Herramientas de análisis y gestión de riesgos**	**20%**	
	Actividad 5.1 Cuestionario de herramientas de análisis y gestión de riesgos.		**5%**
	Actividad 5.2 Explicación de las herramientas de análisis y gestión de riesgos informáticos.		**5%**
	Actividad 5.3 Análisis las herramientas de análisis y gestión de riesgos.		**5%**
	Actividad 5.4 Aplicación de las herramientas de análisis y gestión de riesgos		**5%**
	Practicas finales	**20%**	
	Actividad 6 Caso práctico inicial		**5%**
	Actividad 7 Práctica profesional.		**5%**
	Actividad 8 Mundo laboral		**10%**

ANEXO 7. Interfaz de usuario

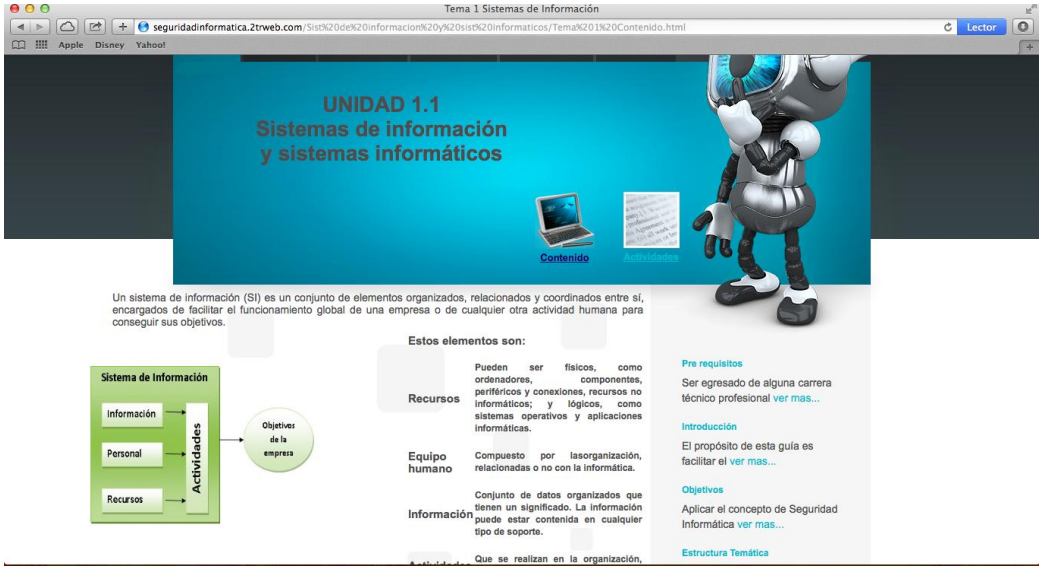
Imagen, Pantalla Principal del Objeto de aprendizaje. Fuente: Elaboración propia (2014)

Imagen, Menú sobre el objeto de aprendizaje. Fuente: Elaboración propia (2014).

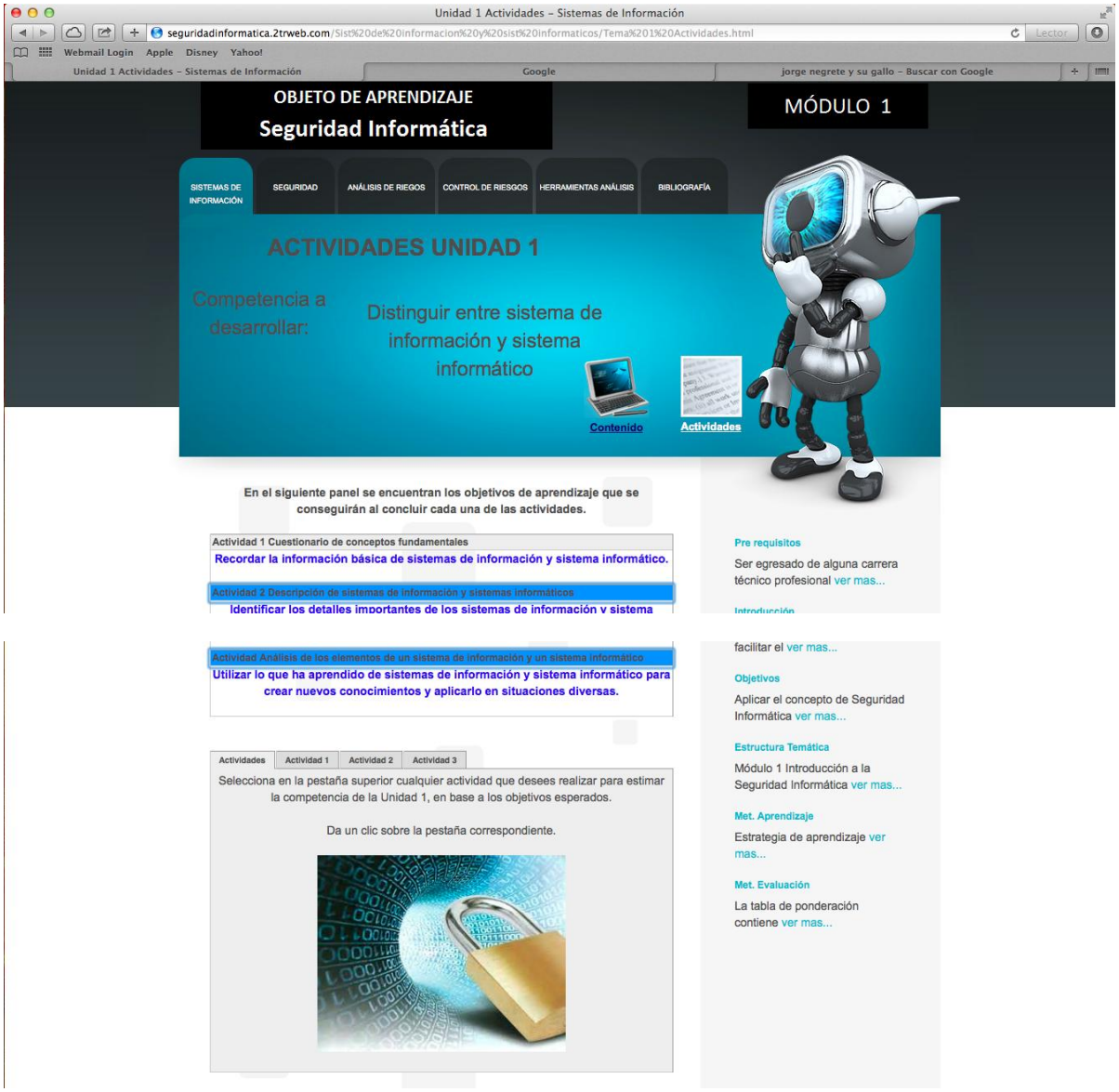
Imagen, Unidad 1 del objeto de aprendizaje. Fuente: Elaboración propia (2014).



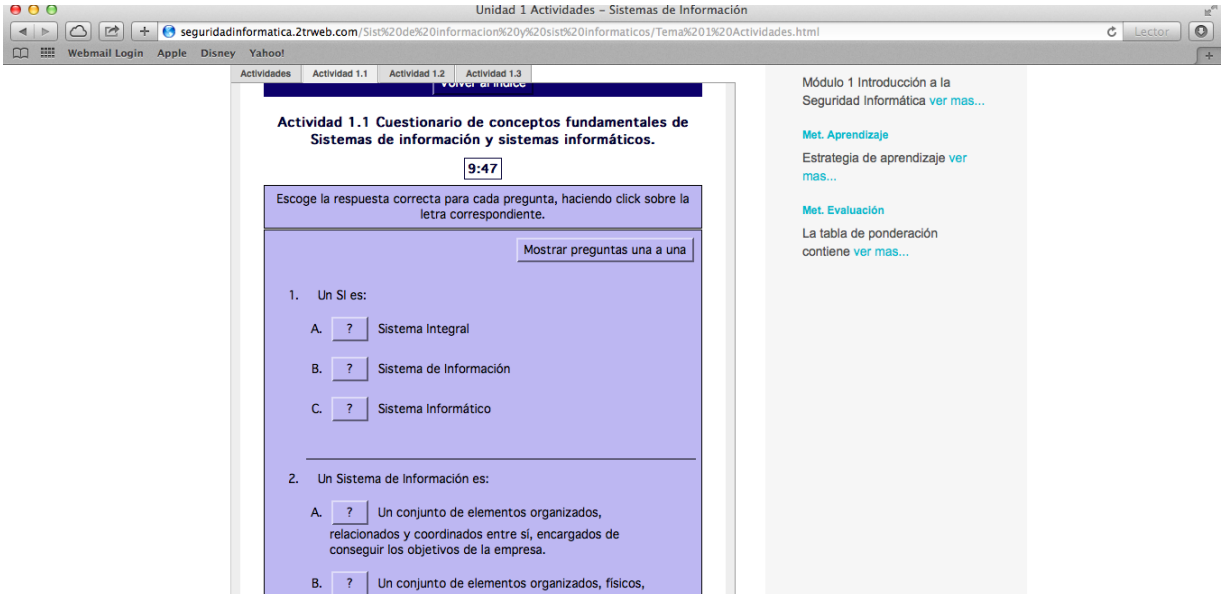
Imagen, Unidad 1 contenido del objeto de aprendizaje. Fuente: Elaboración propia (2014).



Imagen, Unidad 1 evaluaciones del objeto de aprendizaje. Fuente: Elaboración propia (2014).



Imagen, Unidad 1 evaluaciones del objeto de aprendizaje. Fuente: Elaboración propia (2014).



ANEXO 8. Evaluación de expertos

Instrumento de evaluación del Módulo I en Seguridad Informática

Título: Seguridad Informática

Descripción: Objeto de aprendizaje para evaluar competencias específicas del Módulo I del Diplomado en Seguridad Informática impartido por la Universidad Politécnica de Pachuca

Autor: I. S. C. Rubí Yuriana Bautista García

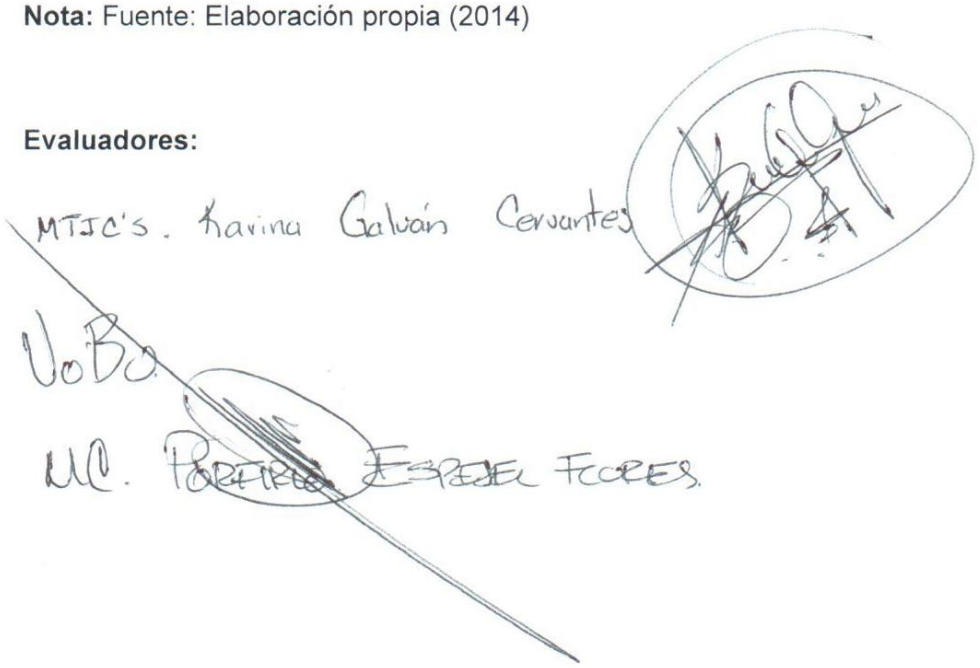
Fecha de evaluación: 26 de noviembre de 2014

Criterios		Si	No	Observaciones
Competencias	Las competencias específicas constituyen la competencia general del Módulo I.	X		
	Los contenidos de cada una de las unidades son suficientes para poder adquirir cada una de las competencias específicas establecidas.	X		
Actividades de evaluación	Los cuestionarios evalúan las competencias del Módulo I del Diplomado en Seguridad Informática.	X		
	Las 18 actividades propuestas, son idóneas para la evaluación de competencias en Seguridad Informática.	X		
	Considera que las 18 evaluaciones tiene una extensión adecuada,	X		
	Los 3 casos prácticos que se presentan al final del las evaluaciones, apoyan a la adquisición de la competencia general del Módulo I.	X		
	Incluiría alguna actividad más.			
	Eliminaría alguna actividad.			
	Existen actividades que no proporcionen información relevante para la adquisición de competencias.	X		
	Las evaluaciones están expresadas de forma comprensible.	X		
	Es correcta la ordenación y distribución de las actividades.	X		

Criterios		Si	No	Observaciones
Ítems de cada evaluación	Los ítems de cada evaluación estiman las competencias específicas de cada unidad.	X		
	Incluiría algún ítem más	X		
	Eliminaría algún ítem	X		
	Existen ítems que no proporcionen información relevante para la adquisición de competencias.	X		
	Los ítems están expresados de forma comprensible.	X		
	Es correcta la ordenación y distribución de los ítems.	X		
	Considera que a través de estos ítems se pueden estimar las competencias adquiridas en el Módulo I del Diplomado en Seguridad Informática.	X		

Nota: Fuente: Elaboración propia (2014)

Evaluadores:



GLOSARIO

Ambiente de aprendizaje: es el conjunto de entornos de interacción, sincrónica y asincrónica, donde, con base en un programa curricular, se lleva a cabo el proceso enseñanza-aprendizaje, a través de un sistema de administración de aprendizaje.

Aprendizaje: (Travers) puede ser considerado – en su sentido más amplio – como un proceso de adaptación; el hombre adquiere nuevos modos de comportamiento o ejecución, con el objeto de hacer mejores ajustes a las demandas de la vida.

Características de un objeto de aprendizaje: (Martínez, N. Susana 2009), formato digital, propósito pedagógico, contenido interactivo, indivisible e independiente, reutilizable.

Competencia: Una competencia es una capacidad para movilizar diversos recursos cognitivos para hacer frente a un tipo de situaciones (Perrenoud, 2000). Se refiere a una combinación de destrezas, conocimientos, aptitudes y actitudes, y a la inclusión de la disposición para aprender además del saber común. (COMISIÓN EUROPEA).

Educación a distancia: (García Aretio, 1994: 1006) lo define como: Un sistema tecnológico de comunicación bidireccional, que puede ser masivo y que sustituye la interacción personal en el aula de profesor y alumno como medio preferente de enseñanza, por la acción sistemática y conjunta de diversos recursos didácticos y el apoyo de una organización y tutoría, que propician el aprendizaje independiente y flexible de los estudiantes.

Evaluación: “Proceso sistemático, diseñado intencional y técnicamente, de recogida de información, que ha de ser valorada mediante la aplicación de criterios y referencias como base para la posterior toma de decisiones de mejora, tanto del personal como del propio programa”. (Pérez Juste, 1995).

Evaluación por competencias: “Se orienta a evaluar las competencias en los estudiantes teniendo como referencia el desempeño de estos ante las actividades y problemas del contexto profesional, social, disciplinar e investigativo (producto integrador).” (Bravo *et. al* 2013, p.5)

Evaluador: persona designada por un organismo de acreditación para ejecutar, sola o como parte de un equipo evaluador.

Facilitador: “es una persona que tiene habilidades para crear espacios para la confianza, participación y relaciones interpersonales; que orienta el proceso grupal reuniendo esfuerzos para descubrir y desarrollar las potencialidades de sus miembros” (Anónimo. Julio, 2004).

Instrumento de evaluación: “proyectos, resolución de problemas, estudio de casos, ensayos, reportes de investigación, presentaciones orales, portafolio de evidencias, rúbricas, exámenes, entre otros, así como diversas modalidades de evaluación: autoevaluación, coevaluación y heteroevaluación.” (Moreno, 2012).

Objeto de aprendizaje: Chan, María E. (2001), menciona “son solamente una herramienta educativa que puede insertarse en propuestas curriculares y metodologías de enseñanza y aprendizaje de muy diversa índole.”

Taxonomías de Marzano: Robert Marzano propone una taxonomía conformada por:

a) El Sistema de Conciencia del Ser que determina el grado de motivación al nuevo aprendizaje,

b) el Sistema de Metacognición que elabora el plan de acción,

c) el Sistema de Cognición que procesa la información y

d) el Dominio del Conocimiento que provee el contenido necesario.

Tipos de competencia: Competencias básicas, laborales, ciudadanas, generales y especificas.

Tipos de evaluación: evaluación automática, evaluación enciclopédica, colaborativa, interactiva.

Tipos de objetos de aprendizaje: Según los contenidos pedagógicos: conceptuales, procedimentales y latitudinales. Según el formato: Imagen, texto, sonido y multimedia. (Moreno, 2012).

REFERENCIAS

Aguilera, P. (2010). *Seguridad Informática*. Editorial Editex

Alonso, L (2002). *Seguridad Informática*. Universidad de Salamanca. Recuperado desde http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

Anónimo. (Julio, 2004). *Guía para el facilitador*. Programa Institucional de Calidad. Universidad de Guanajuato. Recuperado el 13 de noviembre desde http://www.calidad.ugto.mx/ACTUALIZACION%20SEPTIEMBRE%202008/Introduccion%20a%20la%20Calidad-%20Guia%20del%20Facilitador.pdf

Bazaldua, J. A., Conde, R., Rivera, M. E., Rodríguez, J. & Rovira, M. (2006). *La evaluación de competencias: un marco metodológico*. Recuperado el 7 de noviembre de 2013 desde http://es.scribd.com/doc/211779149/Competencias

Belloch, C. (2006). *Diseño Instruccional*. Universidad de Valencia. Recuperado desde http://www.uv.es/bellochc/pedagogia/EVA4.wiki

Bernal, C. A. (2010). *Metodología de la investigación administración, economía, humanidades y ciencias sociales*., Colombia, Prentice Hall.

Bravo, M., Hipólito & E., Torres, A., (Enero - Junio 2013) Seguimiento y evaluación de competencias *profesionales de las estudiantes de la licenciatura en educación preescolar*. Revista Iberoamericana para la Investigación y el Desarrollo Educativo. ISSN 2007-2619. Publicación # 10.

Cantoni, N. M. (2009). *Técnicas de muestreo y determinación del tamaño de la muestra en investigación cuantitativa, 7* (2). ISSN 1669-1555. Recuperado de http://www.sai.com.ar/metodologia/rahycs/rahycs_v7_n2_06.htm

Chiappe, A. (2007). *Evolución conceptual de los objetos de aprendizaje: antes de comenzar… un poco de historia*. Objetos de aprendizaje: conceptualización y producción. Recuperado el 7 de noviembre de 2013 desde http://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCgQFjAA&url=http%3A%2F%2Fwww.cudi.edu.mx%2FdiplomadoOA%2Fmateriales%2Fmodulo_01%2Fevolucion-conceptual-

OA.doc&ei=sq1EU4KDIKuK2AWIqICQCQ&usg=AFQjCNH3DG6y5rTb9hRigTY4DKvAg-w3Pg&bvm=bv.64507335,d.b2I

Durán, M. (Enero- Junio 2012). El estudio de caso en la investigación cualitativa. Revista Nacional de Administración. Universidad Estatal a Distancia, Costa Rica. Recuperado desde http://estatico.uned.ac.cr/rna/documents/Revistaadministracion09.pdf

Frade, L. (2013). *La evaluación por competencias. Tomando en cuenta los últimos planes y programas y las modificaciones realizadas en la evaluación*. México. Ed. Inteligencia educativa.

Frade, L. (2009) *Planeación por competencias*. México. Ed. Inteligencia educativa.

Chan, María E. (2001). *OBJETOS DE APRENDIZAJE: una herramienta para la innovación educativa.* Innova, U de G. Recuperado el 13 de noviembre desde http://cvonline.uaeh.edu.mx/Cursos/ObjetosAprendizaje/PDF/STModulo01/lec_oa_htainnovacion.pdf

García, J. (Abril, 2008). *La evaluación por competencias*. *Módulo 6. Saber evaluar el aprendizaje de los alumnos*. Curso-Taller Educando para una Formación Integral. Tecnológico de Monterey, México. Recuperado el 7 de noviembre de 2013, desde http://www.cca.org.mx/apoyos/cu095/l_m6.pdf

Hermoso, R, Ortiz, R. & Vasirani, M. (2011) *Seguridad Informática*. Universidad Rey Juan Carlos Recuperado desde http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2011/introduccion.pdf

Hernández, S. R., Fernández, C. C. & Baptista, L. P. (2010) *Metodología de la Investigación.*, México, D.F. McGraw-Hill. Recuperado desde https://www.u-cursos.cl/fau/2013/2/DGH-406/1/foro/r/Metodologia_de_la_investigacion,_5ta_Edicion_-_Sampieri.pdf

Instituto de Ciencias de la Educación. (2007). *Los objetos de aprendizaje como recurso para la docencia universitaria: criterios para su elaboración*. Plan de acciones para la convergencia europea (PACE). Recuperado el 7 de noviembre de 2013, desde http://www.aqu.cat/doc/doc_22391979_1.pdf

Marco, P. (2008). *Seguridad Informática. Una visión global.* Universidad Politécnica de Madrid. Recuperado desde http://www.dma.eui.upm.es/conferencias/contenido/seguridad_infor

Martínez, N. Susana. (2009). *Los objetos de aprendizaje como recurso de calidad para la docencia: criterios de validación de objetos en la Universidad Politécnica de Valencia*. Instituto de

Ciencias de la Educación. Camino de Vera s/n. 46022 – Valencia. España. Recuperado el 7 de noviembre de 2013, desde http://spdece07.ehu.es/actas/Naharro.pdf

Marzano, R. J. (2001). *Taxonomía de Marzano*. Recuperado el 7 de noviembre de 2013, desde http://mat.uv.cl/profesores/apuntes/archivos_publicos/6885798721_taxonomia%20Marzano.pdf

Montana State University (2014). *Desire to Learn Learning Environment. Creating activities.* Recuperado de http://eu.montana.edu/d2l/help/instructor_help/assessment_tools/competencies/creating_activities.htm

Montana State University (2014). *Desire to Learn Learning Environment. Creating learning objectives.* Recuperado de http://eu.montana.edu/d2l/help/instructor_help/assessment_tools/competencies/creating_learning_objectives.htm

Montana State University (2014). *Desire to Learn Learning Environment. Understanding competency structures*. Recuperado de http://eu.montana.edu/d2l/help/instructor_help/assessment_tools/competencies/understanding_competency_structures.htm

Morales, E. M., (2013). *Desarrollo de competencias a través de objetos de aprendizaje*. Revista de Educación a Distancia. *Volumen* (36), 19. Recuperado el 7 de noviembre de 2013 desde http://www.um.es/ead/red/36/morales.pdf

Moreno, O. Tiburcio. (julio-diciembre, 2012). *La evaluación de competencias en educación*. Sinética, 39. Recuperado el 7 de noviembre de 2013, desde http://www.sinectica.iteso.mx/assets/files/articulos/39_la_evaluacion_de_competencias_en_educacion.pdf

Ramió, J. (2006) Electrónico de Seguridad Informática y Criptografía.

Strauss, A. & Corbin, Juliet. (2002). *Bases de la investigación cualitativa. Técnica y procedimientos para desarrollar la teoría fundamentada*. Colombia, Editorial Universidad de Antioquia. Recuperado de http://www.iiicab.org.bo/Docs/doctorado/dip3version/Modulo-I/DOC001.PDF

Segovia, J. (2012) Diseño de Instrumentos de Evaluación de Competencias conforme a Secuencias. Global Educación. Recuperado desde http://0305.nccdn.net/4_2/000/000/07b/00b/Dise-o-de-IE-por-Competencias-conforme-a-SD--120229-.pdf

Tobón, S., Pimienta, J. & García, J. (2010). Secuencias didácticas: Aprendizaje y Evaluación de Competencias. México. Ed. Pearson – Prentice Hall.

Universidad de Murcia (2011). *Proyecto de acreditación de competencias TIC del alumnado de la UM.* Vicerrectorado de Estudios Unidad de Innovación. Recuperado desde http://www.um.es/innovacion/wp-content/uploads/2011/03/PROYECTOCompTIC_UM.pdf

Yániz, C. & Villardón, L. (2006). Planificar desde competencias para promover el aprendizaje. El reto de la sociedad del conocimiento para el profesorado universitario. Bilbao: ICE de la UD. Cuadernos monográficos del ICE, núm. 12.

Zabala, A & Arnau, L. (2007). 11 ideas clave cómo aprender y enseñar competencias. México. Ed. GRAÓ