Universidad de Guantánamo

CENTRO DE ESTUDIOS DE LA EDUCACIÓN

Tesis presentada en opción al título académico de Máster en Ciencias de la Educación
Mención Tecnología Educativa

SITIO WEB PARA LA EDUCACIÓN EN SEGURIDAD INFORMÁTICA DE LOS TÉCNICOS DE LABORATORIO EN LA UNIVERSIDAD DE GUANTÁNAMO

Autor: Lic. Héctor Guibert Bosch. (PI)

Guantánamo, 2016

CENTRO DE ESTUDIOS DE LA EDUCACIÓN

Tesis presentada en opción al título académico de Máster en Ciencias de la Educación

Mención Tecnología Educativa

SITIO WEB PARA LA EDUCACIÓN EN SEGURIDAD INFORMÁTICA DE LOS TÉCNICOS DE LABORATORIO EN LA UNIVERSIDAD DE GUANTÁNAMO

Autor: Lic. Héctor Guibert Bosch. (PI)

Tutor: Dr.C. Luis Ángel Kerton Manneres (PT)

Guantánamo, 2016

DEDICATORIA

A mi madre: por la educación ofrecida, por su ternura y dedicación familiar, sostén inigualable en cualquier circunstancia de mi vida.

A mi padre: por confiar y brindarme su hombro íntegro en todo momento.

A mi familia: por su optimismo y apoyo incondicional.

A mis resistentes hermanos y sobrinos.

A mí amada Sucel: por su dedicación, esmero y colaboración incondicional.

AGRADECIMIENTOS

A mi tutor Dr. C. Luis Angel Kerton Manneres y al consultante Dr.C Rolando Durand Rill por su elevada profesionalidad y calidad humana.

A Ms.C Juan Carlos Begué Reyna por su asesoría en la parte tecnológica de la propuesta.

A la Dra.C Liuvis Del Toro Bergondo y a su esposo por su sencillez y modestia, así como por apoyo sustantivo.

A mis amigos Ernesto Navarro Ramos, Orlando Olivares Acosta, Esteban Wilson Agüero, y Antonio Estévez Matos, por apoyarme incondicionalmente en estos momentos difíciles, en lo profesional y en lo personal y por haberme demostrado el valor de la solidaridad.

A los profesores del Centro de Estudio de Educación y de la Escuela de Formación Doctoral quienes unidos me han apoyado en esta ardua tarea.

A los profesores que participaron en esta formación académica y siempre depositaron en nosotros la confianza de poder cumplir este sueño profesional.

A todos mi gratitud.

Muchas gracias

ÉXORDIO

"La tecnología informática no es dañina, pero sí existen formas dañinas de usarla"

Rodríguez, Cuervo, A. M. 2009

SÍNTESIS

El dominio de las nuevas tecnologías de la información y las comunicaciones es una prioridad de la política estatal cubana, pero además una exigencia para asegurar el proceso docente educativo en las facultades y Centros Universitarios Municipales. Por ello, el estudio de la Seguridad Informática en el contexto de la Universidad de Guantánamo, exige educación permanente a los técnicos y otro personal en temas fundamentales para mantener la vitalidad en los servicios informáticos, de manera que contribuyan a la protección y manejo efectivo de la información científica con el uso de las TIC.

Los técnicos de laboratorio de computación muestran insuficiencias en la Seguridad Informática durante su desempeño como resultado de la deficiente preparación teórica, metodológica y comportamental en esta temática. Precisamente, para solucionar esta problemática se diseñó un sitio web que favorece a la educación del personal técnico para que contribuyan a la elevación sostenida en la calidad de los servicios informáticos en los diversos procesos sustantivos.

Se corrobora la factibilidad de la propuesta mediante del método de criterio de especialistas sobre el uso del sitio web sobre Seguridad Informática, el que responde a las necesidades recientes de la gestión educacional en la Universidad de Guantánamo.

INTRODUCCIÓN

El empleo adecuado de las tecnologías de la información y las comunicaciones está transformando la sociedad cubana, caracterizada por gestionar la información y el conocimiento en complejos escenarios mediáticos, con la consiguiente generación de cambios paradigmáticos en las relaciones entre los ámbitos docente, social, económico y cultural y, por consecuencia, transformaciones en las formas de pensar y actuar de sus individuos.

Las tendencias actuales indican que las tecnologías de la información y las comunicaciones (TIC) están íntimamente ligadas al progreso de los pueblos. Su desarrollo ha proporcionado a la sociedad herramientas cada vez más potentes, lo que se evidencia en los avances logrados por las redes de comunicación, las redes sociales con sus aplicaciones y servicios asociados, así como en la incorporación de nuevos dispositivos tecnológicos.

A su vez, llama la atención que su uso ha traído implicaciones notables en el comportamiento de las personas desde el punto de vista ético, los valores morales y políticos e ideológicos, aspectos sobre los que han de incidir la sociedad y la educación al enfrentar la urgente tarea de preparar a los sujetos para absorber, examinar críticamente, reflexionar y proponer líneas de acción en ese sentido.

Las instituciones del Ministerio de Educación (MINED) reconocen la extraordinaria importancia de la información académica, administrativa y científica que gestionan con el uso de las tecnologías de la información y las comunicaciones, como un recurso indispensable para satisfacer los objetivos propuestos por la sociedad.

Como parte de este proceso estratégico cada año se acomete - junto a las instituciones autorizadas -un sistema de acciones a fin de priorizar el empleo de herramientas de las TIC en la gestión de la ciencia con salida en la eficiencia de los procesos educativos.

De esta manera, la fiabilidad y seguridad de las tecnologías con las que se trabaja, se convierten en un soporte trascendental para el desarrollo sostenible de la sociedad

actual. Es por ello que la seguridad y protección de los recursos informáticos surge entonces como un nuevo reto desde las ciencias pedagógicas. Precisamente con el incremento del uso de las tecnologías de la información y las comunicaciones en Cuba, se acrecientan los ataques y amenazas a los medios informáticos; por tanto, asegurar su integridad es vital, sobre todo en la actual coyuntura nacional e internacional.

Se reconocen, en el ámbito internacional y nacional, indagaciones que potencian el uso de las TIC en la sociedad: Entre los autores de se encuentran: J. Cabero (2001), S. Lima (2005), P. Torres (2005), E. J. Ibáñez (2006), UNESCO (2008), J. Vasco (2010) y P. Marqués (2010). De igual manera se destacan los trabajos de Cabrera (2006); Batista, (2007), quienes abordan la temática desde el enfoque de que la información es un recurso metodológico para el desarrollo científico de cualquier nación, al convertirse en conocimientos como ente activo que proporciona ventajas competitivas.

Estos investigadores aportan aspectos significativos, a partir de una visión más integral, y denotan una tendencia a la sobresaturación informativa, por lo que buscar y recuperar información confiable y actualizada, así como el logro de un filtrado y una selección efectivos se ha convertido en un reto para satisfacer las necesidades de los usuarios durante su proceso de almacenamiento o transmisión con la utilización de las tecnologías de la información y las comunicaciones.

Según P. Marqués (2010), la actual sociedad de la información, caracterizada por el uso generalizado de las tecnologías informáticas en todas las actividades humanas y por una fuerte tendencia a la mundialización económica y cultural, conduce a una nueva cultura que supone otras formas de ver y entender el mundo actual, el uso de nuevas máquinas e instrumentos, además de la implantación de valores y normas de comportamiento social novedosas.

Al respecto Borghello (2001), refiere en sus aportaciones que la Seguridad Informática y su educación constituye un problema para la sociedad actual, en tanto el amplio desarrollo de las TIC está ofreciendo un nuevo campo de acción para las conductas antisociales y delictivas, manifestadas en formas antes imposibles de imaginar: se ofrece la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El referente anterior permite identificar que, a nivel internacional se reconoce la importancia de la educación en Seguridad Informática de los recursos humanos, como una vía para enfrentar los nuevos retos planteados en el área de las TIC.

En ese sentido, en diferentes congresos y conferencias internacionales se han producido diversas declaraciones acerca de la importancia de la educación en Seguridad Informática para los usuarios de las TIC. Estos escenarios son: la Cumbre Mundial de la Sociedad de la Información (CMSI, 2003), el XI Congreso de la ONU sobre Crimen y Justicia Penal (COCJP, 2005), la Cumbre Mundial de la Sociedad de la Información (CMSI, 2005) y la XIX Conferencia Iberoamericana de Educación (CIE, 2009),; en ellos se ha destacado la necesidad de una mayor sistematización y profundización teóricas en la educación de los recursos humanos en temas de Seguridad Informática

Actualmente en el mundo existen dos tendencias para abordar el tema de la educación en Seguridad Informática en los usuarios de las TIC. La primera está centrada esencialmente hacia aspectos técnicos y la segunda en elementos administrativos. Estas tendencias realmente expresan serias limitaciones al no considerar como el elemento esencial al usuario común de las TIC. Este fenómeno ha provocado que varios investigadores asocien el analfabetismo digital entendida como la (educación informática) como la principal barrera que impide el crecimiento de la Seguridad Informática en la sociedad.

Lo descrito hasta aquí demuestra que la educación en Seguridad Informática ha encontrado un espacio en la sociedad cubana, que reconoce su rol como una vía para contribuir a la educación de los recursos humanos.

En la revisión bibliográfica realizada se estudiaron distintos artículos y tesis de investigación realizadas por investigadores cubanos y foráneos desde distintas aristas de la Seguridad Informática, como fenómeno complejo que abarca múltiples y muy diversas áreas relacionadas con los sistemas informáticos.

P. M. Curbelo (2003), W. Baluja (2006), R. Montesino (2009), J. Bidot (2009), G. Parets (2009), M. Rodríguez (2009) y la Oficina de Seguridad para las Redes Informáticas de

Cuba (OSRI, 2010) abordan aspectos de la educación de los recursos humanos en Seguridad Informática, destacando que la educación y concientización es lo más importante, identificando así insatisfacciones en la preparación de los sujetos en esta temática en las instituciones cubanas.

Otros autores cubanos como F. Lee (2003), V. Pérez (2006), K. García (2008), S. Ramírez (2008), J. Bidot (2009), J. C. Moro (2009), P. Ramos (2009), J. C. Tejeda (2009), B. Rojas (2009), J. A.López, (2010) y J. Argüello (2009); la Coordinadora de Emergencia en Redes y Telecomunicaciones de la Administración Pública de Argentina (ARCERT, 2006) y el Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas de España (ESCERT, 2009), reflejan en sus experiencias - mediante entrenamientos, adiestramientos, cursos de preparación, capacitación o de superación en Seguridad Informática - aquellos contenidos que forman parte del cuerpo conceptual de la preparación informática.

Otros autores revelan, de manera significativa, aportaciones dirigidas a la Seguridad Informática en el contexto educativo desde una concepción teórico-metodológica para la educación en Seguridad Informática del personal de las instituciones del Ministerio de Educación. Así, por ejemplo, Rodríguez, M. (2012) aporta un sistema de principios, los niveles de preparación del personal en este tema, la tipología de actividades y los recursos educativos, los que permitieron redimensionar la Seguridad Informática en las instituciones del MINED y contribuir a solucionar la dicotomía entre su enfoque técnico y administrativo.

En tal sentido, en la Universidad de Guantánamo se destacan varias investigaciones que han contribuido a potenciar el uso de las tecnologías de la información y las comunicaciones en varios escenarios pedagógicos. Lo anterior se manifiesta en las aportaciones de Reyes, E (2002) quien centra su investigación en el perfeccionamiento el proceso de capacitación informática para el logro de la eficiencia del uso de las TIC por los cuadros y reservas, mediante en un sistema de indicadores que permiten evaluar su impacto. De igual manera Llombart, R. (2015) aporta un sistema de acciones metodológicas para el perfeccionamiento del uso del vídeo educativo como medio de

enseñanza – aprendizaje en la carrera Ingeniería Agrónoma de la Universidad de Guantánamo.

Desde otra visión Durruthy, Y (2015) centraliza sus aportaciones en una metodología para la producción de aulas virtuales como apoyo de la educación presencial en la Universidad de Guantánamo

Particularmente ello exige en la Universidad de Guantánamo el fortalecimiento del empleo de la informatización de modo seguro mediante la integración de sistemas de Seguridad Informática que propicien el aseguramiento de la informatización de los procesos sustantivos sobre la base de educar en esos temas al personal implicado en la dirección de estos procesos, sobre todo a los técnicos de laboratorio de informática con el fin de ofrecer un servicio de calidad, así como para proteger, contra las amenazas existentes, a las tecnologías a su cargo.

Los resultados de un estudio de profundización efectuado por el autor en la Universidad de Guantánamo desde el año 2009 hasta el 2015, con la utilización de diferentes métodos del nivel empírico (observación, entrevistas, encuestas), revelaron en la práctica las siguientes insuficiencias:

- Los responsables en Seguridad Informática de cada área (técnicos de laboratorio de computación), carecen de preparación en este tema, para ofrecer un servicio con calidad, que propicien el aseguramiento de la informatización y sobre la base de educar a los usuarios en esta temática.
- No se aprovechan los diferentes escenarios y espacios para fortalecer el empleo de la informatización en el acompañamiento a través de la integración de sistemas de Seguridad Informática que propicien el aseguramiento de la informatización.
- La carencia de recursos informáticos adecuados al proceso de educación de los responsables de cada área sobre temas de Seguridad Informática en la Universidad de Guantánamo.

Desde estos referentes, se genera la contradicción existente entre la necesidad de implementar el uso sistemático de las Tecnologías de la Información y las Comunicaciones en los diferentes procesos sustantivos en la Universidad de

Guantánamo y la insuficiente fundamentación metodológica para lograr, de forma efectiva, la preparación en Seguridad Informática del personal técnico d dicha institución.

La situación analizada origina, como **problema científico**: ¿Cómo contribuir a la educación de los técnicos de laboratorio de computación en temas de Seguridad Informática en la Universidad de Guantánamo?

De ahí la necesidad de valorar como **objeto de la investigación**: el proceso de Seguridad Informática en la Universidad de Guantánamo.
Se precisa como **campo de acción:** la educación en los técnicos de laboratorio de computación de la Universidad de Guantánamo en Seguridad Informática.

A partir de estos elementos se formula como **objetivo de la investigación**: la elaboración de un sitio web para contribuir a la educación de los técnicos de laboratorio de computación de la Universidad de Guantánamo en Seguridad Informática.

Pregunta Científica:

1. ¿Cuáles son los antecedentes históricos que caracterizan el proceso de Seguridad Informática en la Universidad de Guantánamo?
2. ¿Qué referentes teóricos sustentan el proceso de Seguridad Informática?
3. ¿Cuál es el estado actual de la preparación de los técnicos de laboratorio de computación de la Universidad de Guantánamo en Seguridad Informática?
4. ¿Qué requerimientos teórico-metodológicos debe distinguir el sitio web para contribuir a educar en temas Seguridad Informática a los técnicos de laboratorio de computación de la Universidad de Guantánamo?
5. ¿Qué nivel factibilidad se logrará con la implementación del sitio web para contribuir a educar a los técnicos de laboratorio de computación en temas Seguridad Informática en la Universidad de Guantánamo?

Tareas científicas:

1. Determinar los antecedentes históricos que caracterizan el proceso de Seguridad Informática en la Universidad de Guantánamo.
2. Sistematizar los referentes teóricos que sustentan el proceso de Seguridad Informática.

3. Caracterizar el estado actual de la preparación en Seguridad Informática de los técnicos de laboratorio de computación de la Universidad de Guantánamo.
4. Fundamentar los requerimientos teórico-metodológicos para el diseño del sitio web para la educación en temas de Seguridad Informática a los técnicos de laboratorio de computación de la Universidad de Guantánamo.
5. Valorar el nivel de factibilidad del sitio web para contribuir a educar en temas Seguridad Informática a los técnicos de laboratorio de computación en la Universidad de Guantánamo.

Métodos y técnicas de investigación:

La investigación se fundamenta en el método dialéctico materialista, a partir de la utilización de diversos métodos, técnicas de investigación y la triangulación como procedimiento.

Como **métodos teóricos**, se emplean:

Análisis y síntesis: con el propósito de resumir los aspectos más importantes de la bibliografía relacionada con el uso de la Tecnología de la información y las comunicaciones, fundamentalmente en temas de Seguridad Informática.

I**nducción-deducción:** para extraer informaciones sobre el proceso de Seguridad Informática en todo el proceso de investigación.

Histórico y lógico: para valorar la evolución de las concepciones, definiciones, enfoques y estudios que históricamente están presentes en las investigaciones científicas y que estén relacionados con el proceso de Seguridad Informática y su concreción en la preparación de los técnicos de laboratorio de computación en el tema objeto de estudio.

La **modelación:** permite elaborar los fundamentos para la educación en temas de Seguridad Informática; además de abordar el problema en sí desde el proceso de informatización en la Universidad de Guantánamo.

Métodos empíricos:

La **observación** a técnicos de laboratorio de computación en el desarrollo de actividades docentes y su desempeño en materia de Seguridad Informática.

Se realizan **entrevistas y encuestas** a directivos, técnicos de laboratorio de computación, para constatar la preparación y educación en Seguridad Informática para enfrentar el servicio a usuarios en el proceso de informatización en función de diagnosticar el problema científico.

Talleres de opinión crítica y elaboración colectiva: Permite hacer valoraciones colectivas, realizar ajustes y considerar la factibilidad del sitio web para su perfección y validación a partir de un proceso sucesivo de acercamiento a la conciliación de opiniones autorizadas.

Estudio documental: durante el proceso de lectura y estudio de la bibliografía, documentación sobre el tema y regulaciones, dando como resultado el marco teórico que avala la investigación sobre temas de Seguridad Informática en la Universidad de Guantánamo.

Triangulación: para el procesamiento de los datos recogidos sobre del sitio web propuesta, por cuanto contribuye a elevar la objetividad del análisis de los datos y lograr mayor credibilidad de los resultados.

Métodos estadístico – matemáticos:

Estadística descriptiva: para realizar el cálculo porcentual y la tabulación de los resultados de los instrumentos aplicados durante la constatación del problema de investigación, así como para valorar la efectividad teórico metodológica para la implementación y concreción práctica del sitio web sobre el proceso de Seguridad Informática.

Población y muestra

Se seleccionó una **población** de 104 unidades de estudio, constituidas por el personal docente, administrativo y técnico de apoyo a los diversos procesos de informatización de

la Universidad de Guantánamo y los Centros Universitarios Municipales.

La **muestra intencional** seleccionada fue de 38 técnicos vinculados a la informatización distribuidos como sigue: técnicos de laboratorios (13), Grupo de Equipos (8), Infotecnología (6) y personal administrativo de los Centros Universitarios Municipales (9).

A**ctualidad de la investigación**: se dispone de un sitio web de Seguridad Informática que tributa al Modelo de Educación Superior y constituye una línea de investigación priorizada en la UG. Posee importancia y connotación social al contribuir a educar a los responsables de las áreas donde se prestan servicios informáticos con vista a su protección y manipulación no autorizadas.

Aporte práctico: radica en la propuesta del sitio web como medio para la contribución a la educación de los técnicos de laboratorio de computación en temas de Seguridad Informática en la Universidad de Guantánamo.

Significación práctica: se ofrece una herramienta teórico - metodológica para socializar y divulgar los resultados científicos generados para el intercambio científico y la superación del personal técnico. Todo ello concreta la prioridad del Ministerio de Educación Superior relacionada con la educación en Seguridad Informática a los profesionales de la Universidad de Guantánamo.

Novedad de la investigación: se integran los fundamentos teóricos, metodológicos y comportamentales de la Seguridad Informática, mediante el empleo del sitio web como una interfase de fácil acceso, acorde con las exigencias del Ministerio de Educación Superior; de esta manera se contribuye al mejoramiento del proceso de educación del personal técnico de la Universidad de Guantánamo.

CAPÍTULO I. REFERENTES TEÓRICOS METODOLÓGICOS PARA LA CONTRIBUCIÓN A LA EDUCACIÓN EN SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD DE GUANTÁNAMO

En el presente capítulo se realiza un análisis donde se exponen los fundamentos teóricos de la preparación de los sujetos en el uso de las TIC, como parte de la educación en Seguridad Informática en la Universidad de Guantánamo. Para ello, se determinaron las principales etapas y se caracterizó la evolución del objeto de investigación. Se precisa la situación actual en el desempeño de los técnicos de laboratorio de computación en la Universidad de Guantánamo en Seguridad Informática.

1.1 Principales tendencias históricas en el proceso de Seguridad Informática en la Universidad de Guantánamo

En el estudio del proceso de Seguridad Informática en la Universidad de Guantánamo se asume -como criterio esencial para profundizar en la perspectiva histórica sobre educación en Seguridad Informática en las condiciones de la Educación Superior en la Universidad de Guantánamo - los indicadores siguientes:

1. Nivel de conocimiento de los documentos normativos del proceso de implementación de las Tecnologías de la Información y las Comunicaciones, como parte de la Seguridad Informática.
2. Métodos y vías utilizadas por los responsables de cada área para desarrollar la Seguridad Informática en la Universidad de Guantánamo.
3. Nivel comportamental de los técnicos para implementar la Seguridad Informática en los diferentes escenarios de la Universidad de Guantánamo.

En el estudio se determinaron dos etapas fundamentales: primera etapa (1976-1989) y segunda etapa. (1990 hasta la actualidad).

Primera etapa (1978-1989): perfeccionamiento del sistema educacional en materia del proceso de informatización como parte de la Seguridad Informática.

La introducción de las Tecnologías de la Información y las Comunicaciones en la educación cubana, centró sus esfuerzos inicialmente en preparar a los recursos humanos

en temas de computación, dejando una brecha en los temas de la Seguridad Informática y la producción y protección de la información con la utilización de las diferentes aplicaciones y herramientas informáticas.

El desarrollo de las Tecnologías de la Información y las Comunicaciones en Cuba, así como su introducción en la gestión docente, económica y en las investigaciones pedagógicas, han constituido objetivos estratégicos del Ministerio de Educación Superior desde la década del 70.

A su vez, en la década del 80 se adquirieron microcomputadoras que posibilitaron su uso e incorporación en los diferentes planes de estudio de los diferentes niveles de preparación y, particularmente, en las carreras de Licenciatura en Educación, a finales de la década del 90, se incentivó el desarrollo extensivo de la tecnología informática y el uso de las redes en el organismo y sus instituciones. Ello exigió el necesario compromiso con la protección de ese proceso.

Uno de los pioneros en el tema de la Seguridad Informática fue P. J. Anderson (1980) quien, a solicitud del gobierno de Estados Unidos, produjo uno de los primeros estudios teóricos relacionados con el tema, donde se sientan las bases de palabras y definiciones que hoy se asumen como naturales en el ámbito de la Seguridad Informática. En Cuba a la Seguridad Informática se le han incorporado aspectos de prevención y gestión; se realiza el análisis de riesgos y vulnerabilidades, la validación de la seguridad en la red, la respuesta a incidentes y la recuperación de la información.

En Guantánamo los primeros pasos del empleo de la informática educativa se dan en el curso 1986/87, con la preparación de un grupo de profesores del área de ciencias exactas de la filial provincial del Instituto de Perfeccionamiento Educacional -IPE-, metodólogos provinciales, profesores de la Escuela Formadora de Maestros Primarios y el IPVCE “José Maceo”, y profesores del Instituto Superior Pedagógico.

En mayo de ese mismo curso escolar, con el auspicio del MINED y el MES se desarrolla el primer curso de formación emergente de Informática en Guantánamo, con la llegada al IPE provincial del primer laboratorio asignado. En él participó un total de 22 cursistas de

diferentes enseñanzas, que acometerían en el curso 1987/88 la introducción y desarrollo de esta materia en diez centros docentes seleccionados del territorio.

En ese mismo curso se introducen e instalan estos laboratorios por primera vez en el Instituto Pedagógico y en los preuniversitarios - con 10 a 12 puestos-; en los politécnicos – con 4 a 6 puestos- y dos puestos en las secundarias básicas. Se trabajó con el duodécimo grado del preuniversitario, un año de la carrera del politécnico y en noveno grado, como círculos de interés. Todos los contenidos estaban relacionados con los elementos de la programación, utilizando el lenguaje MSX – Básic.

Paralelamente, en este mismo curso escolar, se llevó a cabo la preparación en Informática de otro grupo de profesores en el IPE provincial. Este curso tuvo un año de duración y fue a tiempo completo. Los cursistas fundamentalmente fueron docentes de Educación Laboral reorientados al respecto que laborarían en las secundarias básicas.

En el curso escolar 1988/89 se instalan los laboratorios en el resto de los centros y se imparte la asignatura Informática en todos los grados. Se introduce también en la Escuela Pedagógica – antigua Formadora de Maestros.

Consideraciones generales en esta etapa:

La introducción de las Tecnologías de la Información y las Comunicaciones en la educación cubana, centró sus esfuerzos inicialmente en preparar a los recursos humanos en temas de computación, pero dejó una brecha para desarrollar la Seguridad Informática. Por las características de la tecnología existente hasta la década del 80 no constituía una prioridad abordar con los usuarios estos temas de Seguridad Informática.

Con la popularización de Internet a partir de 1980 y su auge al finalizar esta década, el surgimiento de los primeros virus informáticos demostró la vulnerabilidad de los sistemas informáticos cubanos, los riesgos en la protección de la información, pues ya no era solamente un problema de protección física: se incrementaban las amenazas externas.

Los aspectos anteriormente mencionados permiten inferir como cuestión esencial la evolución paulatina de la informatización de los procesos y la educación en temas de Seguridad Informática en el Centro Universitario en Guantánamo.

Segunda etapa (1990 hasta la actualidad): nuevas perspectivas en la Universidad de Guantánamo en la Seguridad Informática.

A partir del curso escolar 1990/91, se introduce experimentalmente la Informática en 128 escuelas primarias del país, 10 de las cuales correspondieron a Guantánamo, con prioridad para el 6to. Grado, aunque con extensión al resto de los grados, según las posibilidades.

En estos momentos se lleva a cabo en Cuba lo que justamente se ha venido denominando la Tercera Revolución Educacional, uno de cuyos pilares es el despliegue masivo del dominio de la computación, desde la enseñanza primaria hasta las actividades socioeconómicas cotidianas.

Ya es una realidad que todas las escuelas, en los diferentes niveles de enseñanza, así como las especiales, cuenten no sólo con computadoras de última generación, sino con televisores y videos que permiten llevar hasta el último rincón de nuestra provincia los programas priorizados por la Revolución cubana.

Con la entrada de las máquinas computadoras electrónicas en las aulas se crea una segunda alfabetización en el desarrollo de los procesos educacionales. En la capacitación del personal en Seguridad Informática este fenómeno se presenta con una marcada importancia.

En el Ministerio de Educación Superior se estableció en el año 1998, por primera vez, una resolución ministerial que aborda los aspectos referentes a la Seguridad Informática (RM 230/1998), única evidencia documental sobre su inicio en la educación, la cual regulaba las medidas técnicas, físicas y lógicas para proteger la información y los activos informáticos, para todas las entidades educacionales, incluidas las empresas.

En 1999 con el inicio del funcionamiento de la red del organismo central, se elabora el primer plan de Seguridad Informática, en el que se establecieron las medidas técnicas, físicas y lógicas para proteger la información y todos los activos informáticos, para todos los centros educacionales y empresas.

El Centro Universitario de Guantánamo se crea en mayo de 1997. Esto permitió que el país pudiera dar respuesta con una universidad territorial a las crecientes necesidades de

elevar la preparación del personal en la informatización desde el uso de las Tecnologías de la Informatización y las Comunicaciones, una de las vías más eficientes para lograrla, ya que se encontraría en condiciones de realizar su propia y autodidacta superación, al contar con las herramientas para acceder a la información en cualquier forma en que ésta se le presentara.

Se desarrollan semanalmente cursos de capacitación en Informática, con el objetivo principal de que adquieran habilidades básicas en la utilización de la informática como apoyo a sus actividades directivas, además de adquirir un conjunto de conocimientos y conceptos sobre Sistema Operativo Microsoft Windows -MS- 200, MS Word, MS PowerPoint, MS Excel, MS Access, Redes, Correo Electrónico, Internet, y otras formas de acceso a la información, lo que les permitirá una participación activa en el proceso de informatización de la sociedad cubana.

En la actualidad se constata que la Seguridad Informática precisa un enfoque general e integral, donde se incluya un conjunto de acciones - desde el punto de vista de las soluciones técnicas, organizativas, legales y educativas al problema - con el fin de minimizar los riesgos y los costos que acarrean la pérdida, la modificación y la propagación no deseada de información de alto valor para su poseedor.

De este modo se ha producido una comprensión de la Seguridad Informática como un saber emergente del hombre de estos tiempos y constituye un componente determinante en la preparación de los sujetos. No tener un compromiso con la Seguridad Informática es una forma de comportamiento irresponsable de los sujetos, aspectos que deben ser especialmente observados y educados para su corrección; de no hacerlo la conciencia en Seguridad Informática de los sujetos dejaría de ser importante.

Las primeras evidencias de la Seguridad Informática en Cuba las aporta S. Ramírez (2008), al plantear que uno de los pioneros de la protección de la información fue José Martí, pues el apóstol usaba un cifrado para proteger los mensajes que enviaba y en la actualidad todavía no se sabe el contenido de muchos de esos documentos, pues no se han podido encontrar las claves que utilizaba para descifrar su contenido.

Sobre esa base legal se inició el trabajo, por parte del estado cubano, representado por sus diferentes Ministerios e instituciones, al emitir una base regulatoria sobre la Seguridad Informática, lo cual queda reflejado en algunos de los siguientes documentos.

- Resolución No. 6/96 del Ministerio del Interior (MININT), sobre el reglamento de Seguridad Informática.
- Resolución no. 204/96 del Ministerio de la Industria Sideromecánica y la Electrónica, que pone en vigor el reglamento sobre la protección y seguridad técnica de los sistemas informáticos.
- Decreto Ley 199/99 del Consejo de Estado sobre la seguridad y protección de la información oficial.
- Instrucciones del VMP del MININT sobre la seguridad y protección de la información oficial.
- Resolución 188/01 del Ministerio de la Informática y las Comunicaciones (MIC), que establece los requisitos y procedimientos para la autorización del acceso a Internet por parte de las entidades cubanas.
- Acuerdo 6058/2007 del Comité Ejecutivo del Consejo de Ministros (CECM), sobre los lineamientos para el perfeccionamiento de la seguridad de las tecnologías de la información en el país.
- Resolución No. 188 /2006 del Ministerio del Trabajo y Seguridad Social (MTSS), sobre los reglamentos disciplinarios internos.
- Resolución 127/07 del Ministerio de la Informática y las Comunicaciones (MIC), sobre el reglamento de seguridad para las tecnologías de la información.
- Resolución No. 60/11 de la Contraloría General de la República de Cuba, sobre el control interno.

Estos documentos y resoluciones, entre otros, trazan políticas y directivas de Seguridad Informática en el país y también se fortalecen entidades como el Centro Nacional de Superación y Adiestramiento en Informática (CENSAI), Segurmática y aparecen otras

como: Citmatel, del Ministerio de Ciencia, Tecnología y Medio Ambiente, Desoft - del Ministerio de la Informática y las Comunicaciones (MIC) - y la empresa consultora DISAIC del SIME, que se dedican a brindar asesoría sobre estudio de riesgos y vulnerabilidades de los sistemas informáticos, implementan mecanismos de seguridad de la información en las empresas y capacitan especialistas en informática con un perfil más amplio en materia de Seguridad Informática, y en el caso de Segurmática elabora y comercializa softwares de protección o antivirus.

Como elemento importante en esta etapa se crea también la Oficina de Seguridad para las Redes Informáticas de Cuba (OSRI) del MIC, facultada para implementar cuántas disposiciones complementarias se requieran para dar cumplimiento a lo que se establece en la Resolución 127/07 sobre el reglamento de seguridad para las tecnologías de la información, así como controlar y evaluar el estado de la Seguridad Informática en todas las instituciones del país.

Consideraciones generales en esta etapa:

- La Seguridad Informática en Cuba estuvo mucho tiempo asociada generalmente a la protección física y en aspectos externos del soporte donde se procesa y almacena la información.
- Se centra el tema de preparación del usuario en los virus como aspecto esencial y se fortalece la base legal de la Seguridad Informática en el país.
- Se aprecia un incremento notable de la presencia de TIC en todos los sectores de la sociedad cubana, siendo la educación es una de las favorecidas.
- La base legal emitida por el país no encuentra respaldo, en una preparación en Seguridad Informática en los planes de preparación de los recursos humanos de las empresas, entidades, incluyendo los programas de estudio de la Educación General.

El estudio histórico realizado en la investigación permitió precisar las siguientes regularidades:

- Se concibe la preparación de los sujetos en el uso de las Tecnologías de la Información y las Comunicaciones como parte de la educación en Seguridad Informática del personal de Educación Superior, de forma paulatina y transitoria.

- Se aprecia un incremento de la participación del personal en temas de Seguridad Informática en los diferentes procesos universitarios.
- Hay un aumento e integración progresiva de la implementación de las tecnologías informáticas en los diferentes procesos universitarios y del personal en estas temáticas.

Las regularidades derivadas del estudio histórico avalan la necesidad de profundizar en las consideraciones teóricas, prácticas y comportamentales en educación sobre Seguridad Informática; precisa la necesidad de continuar implementando alternativas en función de normalizar e implementar la Seguridad Informática en los diferentes procesos universitarios.

1.2 Referentes que sustentan el proceso de Seguridad Informática como parte del uso de las Tecnologías de la Información y las Comunicaciones

El estudio de la Seguridad Informática parte de las diversas normativas de la Oficina de Seguridad para las Redes Informáticas (OSRI) como entidad nacional adscripta al Ministerio de la Informática y las Comunicaciones. Esta entidad tiene por objeto social:

- Llevar a cabo la prevención, evaluación, aviso, investigación y respuesta a las acciones, tanto internas como externas, que afecten el normal funcionamiento de las Tecnologías de la Información del país.
- Trabajar por el fortalecimiento de la seguridad durante el empleo de las Tecnologías de la Información y las Comunicaciones.

Precisamente, el propósito consiste en implementar un sistema que contribuya al ordenamiento de las actividades asociadas con las redes informáticas y de las comunicaciones, mediante el establecimiento de una concepción multidisciplinar que garantice niveles aceptables de seguridad, lo que requiere de la educación permanente en temas de Seguridad Informática.

Fundamentos filosóficos:

El escritor y político Vladimir Ilich Ulianov, Lenin, definió el papel de la actividad como principio y fin para construir colectivamente el conocimiento útil.

Se ha considerado la concepción de la práctica en la educabilidad del hombre y el papel que le corresponde a la preparación en Seguridad Informática, en la tarea de formar a las actuales y futuras generaciones, dispuestas a cumplir una encomienda social en un mundo laboral con alta presencia de las TIC, con un sentido de arraigo, compromiso, identidad y comprometido con su transformación.

Fundamentos éticos:

El proceso de preparación en Seguridad Informática tiene una alta implicación y contribución a la formación de los valores y la moral de los sujetos al usar las TIC; en consecuencia fueron sistematizados varios referentes, entre los que se destacan:

- El estudio de los valores por la axiología, el conocimiento de sus funciones en la sociedad, así como sus implicaciones en la educación, tienen gran importancia ya que poseen una función práctico-reguladora y orientadora de la actividad humana.
- Las relaciones que se establecen entre los hombres, y de ellos con las TIC, están condicionadas por un conjunto de exigencias que la sociedad plantea al hombre en su vida cotidiana, valores y normas que regulan su conducta; en este sentido es posible hablar de conducta moral**.** Estas exigencias tienen un carácter histórico-cultural y clasista y devienen en obligaciones del individuo para con otros individuos, la familia y la sociedad.
- El carácter regulador y orientador, expresado por E. Báxter, al enfatizar que “un factor importante en la formación de la personalidad lo constituyen las actitudes y valores que se forman y desarrollan hasta llegar a constituir su núcleo regulador y orientador, el cual caracteriza a las personas adultas maduras” (Báxter, E. 2002, p.3).

Fundamentos sociológicos:

Para Carlos Marx, la sociedad es el producto de la acción de los hombres. En su concepción no separa la sociedad de la naturaleza; al contrario, los seres humanos son vistos como parte del mundo material, que es la base real de todas sus actividades. Se asume la relación sociedad-naturaleza como un intercambio que se desarrolla

históricamente mediante el trabajo humano y, al mismo tiempo, crea y transforma las relaciones sociales.

Por su parte, en la Cumbre Mundial sobre la Sociedad de la Información (CMSI, 2003 y 2005), su declaración de principios aborda - entre los aspectos referidos al uso de las TIC y sus implicaciones sociales, los siguientes:

- La educación, el conocimiento, la información y la comunicación son esenciales para el progreso, la iniciativa y el bienestar de los seres humanos.
- Las TIC deben considerarse como un instrumento y no como un fin en sí mismas. En condiciones favorables estas tecnologías pueden ser un instrumento muy eficaz para acrecentar la productividad, generar crecimiento económico, crear empleos y posibilidades de contratación, así como para mejorar la calidad de la vida de todos.
- Reforzar el marco de confianza que abarca, entre otras cosas, la seguridad de la información y la seguridad de las redes. La autenticación, la privacidad y la protección de los consumidores es requisito previo para que se desarrolle la sociedad de la información.
- Impedir que las TIC se utilicen con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, lo que podría menoscabar la integridad de las infraestructuras nacionales al atentar contra la seguridad.
- Abordar nacional e internacionalmente la ciberseguridad y el envío masivo de mensajes electrónicos no solicitados, lo cual es un problema considerable y creciente para los usuarios, las redes e Internet en general.
- Crear un entorno de trabajo seguro y sano que sea adecuado para la utilización de las TIC, así como conforme a las normas internacionales pertinentes.

Los cambios sociales y culturales en la sociedad actual, en muchos casos estrechamente vinculados a la presencia de las TIC, tienen como consecuencia un impacto significativo no sólo en la producción de bienes y servicios, sino en el conjunto de las interrelaciones sociales.

La acumulación de información, la velocidad en su transmisión, la superación de las limitaciones o barreras espaciales, el empleo simultáneo de múltiples medios (imagen, sonido, texto, código) son, entre otros, los elementos que explican la enorme capacidad de cambio que aportan estas tecnologías. Su utilización obliga a modificar el valor de conceptos básicos como tiempo y espacio. La noción misma de realidad comienza a ser repensada, a partir de las posibilidades de construir realidades virtuales que plantean nuevos problemas e interrogantes de orden epistemológico (Área, M.2010).

Fundamentos psicológicos:

La referencia histórica y cultural, desde los aportes realizados por L. S. Vigotsky (1896-1934), resulta esencial para la preparación en Seguridad Informática, ya que representa una nueva manera de entender la relación entre sujeto y objeto en el proceso de la construcción del conocimiento; asimismo porque se considera la naturaleza social del hombre como elemento determinante de su desarrollo intelectual. Esta construcción del conocimiento la realiza el sujeto a partir de relaciones intra e interpersonales, de ahí el papel en la construcción del conocimiento de las funciones sociales. En ese sentido, se destacan los siguientes elementos:

- La importancia de la actividad (cognoscitiva, práctica y valorativa) y la comunicación
- El papel de la enseñanza y el aprendizaje en el desarrollo personal y profesional
- El papel mediador de los signos y las herramientas en el proceso de aprendizaje
- La llamada “zona de desarrollo próximo”
- El vínculo de lo individual con lo colectivo

Fundamentos pedagógicos:

En la gestión de los procesos sustantivos de la educación superior - al contarse con la presencia de las TIC para procesar información académica, administrativa y científica y satisfacer los objetivos propuestos por la sociedad – se necesitan individuos suficientemente preparados y educados en el uso de estos recursos. Lo anterior requiere profundizar - desde la pedagogía - cómo debe estar concebida la preparación en Seguridad Informática.

Según J. Chávez, pedagogo cubano, en el estudio de la pedagogía se comprende al hombre como ser vivo, biológico, psíquico, individual, social e histórico. “Lo humano en el hombre-en gran medida-lo engendran la vida en sociedad y la cultura creada por la humanidad” (Chávez, et al., 2005, p. 4); condición que genera la necesidad de educarse, lo cual es posible gracias a la capacidad del hombre de ser educado (educabilidad) debido a que posee en su propia naturaleza las potencialidades necesarias para este fin y para su autoeducación (Chávez, et al., 2005, p. 12).

La hablar del término educar, social y culturalmente, se refiere a formar al hombre para la vida, para que tengan una actuación en sociedad adecuada en términos valores y actitudes En particular, la preparación en Seguridad Informática debe integrase al proceso educativo, combinando los avances científico-tecnológicos más recientes y las particularidades de la subjetividad humana para su pleno desarrollo pleno, de manera que se dote al hombre de instrumentos que le permitan desarrollarse para enfrentar los retos de la época que le ha tocado vivir.

La instrucción y la educación constituyen una unidad dialéctica, en tanto toda instrucción implica una educación y toda educación estuvo precedida de una instrucción.

La instrucción incluye los conocimientos, tanto conceptuales (conceptos, hechos, datos) como los procedimentales (habilidades, hábitos, procedimientos, etc.), mientras que la educación se refiere a los contenidos actitudinales que tienen en su base a los valores.

El estado cubano se plantea como un objetivo estratégico de la formación de los futuros ciudadanos, el desarrollo de una educación moral basada en una formación de valores de amor a la justicia, la responsabilidad y la honestidad desde valores humanistas, cuestión que debe estar presente en cualquier concepción de preparación en Seguridad Informática.

Es incuestionable que la preparación en Seguridad Informática proporciona una nueva perspectiva en el uso seguro de las TIC, a partir de la creación de un nuevo espacio de reflexión ética, que contribuya a la configuración de un nuevo sistema de valores acerca de las TIC y su utilización por la sociedad.

Cuando la sociedad plantea a la educación, la necesidad de formar sujetos moralmente responsables, es pertinente valorar qué le puede aportar la Seguridad Informática como nuevo saber a la educación y, en particular, al proceso de preparación de la informática.

En el eslabón de base de la universidad cubana, la Seguridad Informática deberá contribuir a la educación de los sujetos en mayor medida cuando su diseño y su utilización se realizan de forma consciente e intencional. Es necesario una conjugación armónica de las relaciones intergrupales para el desarrollo de los sujetos, ya que el proceso de socialización del hombre es una vía para su educación plena.

Fundamentos tecnológicos:

En la actualidad la educación a distancia empleando los entornos virtuales es ampliamente utilizada en la preparación de profesionales de distintas áreas del conocimiento, en particular, en relación con la preparación de los recursos humanos en temas de Seguridad Informática.

Las redes telemáticas han permitido la colocación de los entornos virtuales; desde los cuales se han alcanzado valiosos resultados en el orden pedagógico en la educación, con alternativas viables en la elaboración de recursos educativos con los presupuestos del enfoque histórico cultural (Collazo, R. 2004; Herrera, E. 2005; Pérez, V. 2006; Lima, S. 2009a; Sánchez, Y 2011, Fernández, F. 2012a; entre otros).

Estos entornos virtuales (EV) son considerados espacios configurados en las redes telemáticas, los cuales agrupan un conjunto considerable de herramientas que permiten la diversidad de formas de comunicación sincrónica y asincrónica (Foro, Chat, correo electrónico, listas de discusión o distribución, wiki, blog, videoconferencia, audio-conferencia, entre otras); en tanto facilita, amplía y diversifica las variantes de preparación de los recursos humanos gracias a la flexibilidad en tiempos y espacios, en aras de posibilitar una formación continua que permita a los sujetos apropiarse de una cultura general e integral a lo largo de la vida.

Es importante destacar que la preparación en Seguridad Informática, a través de los entornos virtuales, requiere de una indispensable orientación pedagógica desde las herramientas comunicacionales de la web 2.0 y 3.0, pues estas brindan diferentes formas

de utilizar las redes sociales en la educación. (Herrera, E. 2005; Pérez, V. 2006; Lima, S. 2009a; Sánchez, Y. 2011 y Fernández, F. 2012a).

Se asume lo aportado por (Herrera, E. 2005; Pérez, V. 2006 y Lima, S. 2009a), sobre los aspectos a tener en cuenta para el diseño didáctico de los cursos en entornos virtuales de aprendizaje y que se señalan a continuación:

1. Diagnóstico de necesidades y planificación del programa de los cursos, estudio de posibles beneficiarios y las posibilidades reales de estudio en este tipo de programa.
2. Planificación y oferta de cursos, organización de los aprendizajes a impartir y las metodologías que se utilizarán, teniendo en cuenta las necesidades reales de formación y actualización de sus destinatarios.
3. En el diseño didáctico de los cursos se debe tener presente los canales de comunicación entre todos los implicados en los cursos: profesores, estudiantes, tutores. En cuanto a la confección de los materiales básicos para los cursos se deberá atender a su asequibilidad, esencialmente en lo relacionado con el lenguaje y abordar sus núcleos básicos del contenido de los cursos que se traten.
4. En la implementación de los cursos se debe tener en cuenta su distribución, servicios de consulta que se ofrecerán; además con qué medios se harán y se utilizarán: el teléfono, el correo postal, el e-mail, el chat, entre otras vías.
5. Evaluación de los estudiantes.

Se asumen los ejes metodológicos para el diseño didáctico de los cursos a distancia en entornos virtuales de aprendizaje aportados por (Herrera, E. 2005 y Lima, S. 2009a). Los ejes metodológicos que se ofrecen constituyen requisitos generales básicos a considerar durante el proceso del diseño didáctico de un curso, en aras de aprovechar las potencialidades de los entornos virtuales para un proceso de preparación desarrollador a distancia. Estos ejes metodológicos son los siguientes:

- Instrumentación desarrolladora del diseño didáctico debe aprovechar las potencialidades de los entornos virtuales para que eleve al nivel superior posible el desarrollo de cada sujeto y grupo, potenciando futuros aprendizajes.

- Relevancia personal, social y profesional se fundamenta en la necesidad de que el aprendizaje se produzca a partir la reestructuración crítica y creadora de saberes previos, mediante la activación de procesos y mecanismos cognitivos y afectivos que propicien el sentido personal de lo aprendido y favorezcan futuros aprendizajes.
- La colaboración se fundamenta en la importancia del trabajo colaborativo, como forma de organizar el diseño de los cursos. (La calidad del diseño didáctico depende en gran medida de la naturaleza y el equilibrio del intercambio y la colaboración que se logre, al evitar la polarización hacia aspectos informático-tecnológicos que condicionan; pero no determinan, la orientación y naturaleza de la actividad que se modela).
- Diversificación de la mediación pedagógica en entornos virtuales, lo que condiciona la singularidad del rol mediador del profesor, soportado en los materiales didácticos y medios de que se dispone.
- Sensibilidad a las potencialidades de los entornos virtuales de aprendizaje para el diseño didáctico de los cursos: se refiere al constante cuestionamiento de estas para propiciar un proceso de preparación, a partir del conocimiento de estos entornos y de sus recursos para alcanzar dicha finalidad.
- Viabilidad y sostenibilidad del diseño didáctico: se refiere a la necesidad de tener en consideración las condiciones reales para su concepción e implementación en aras de la viabilidad y sostenibilidad del proceso de preparación a distancia que se diseña, de modo que pueda ser realizado, y que los cursos contengan potencialidades para su adecuación y generalización.
- Articulación entre lo pedagógico, lo tecnológico y lo organizativo: ello evidencia la importancia de armonizar lo pedagógico, lo tecnológico y lo organizativo, de modo que se seleccionen los recursos materiales y humanos y se decidan las demás condiciones requeridas, acorde con el modelo pedagógico asumido y las circunstancias concretas en que se elaborarán y desarrollarán estos cursos, para la consecución de las finalidades educativas planteadas.

En la educación superior se utiliza la plataforma Moodle como sistema de gestión del aprendizaje para la preparación de los sujetos, a partir del empleo de materiales multimedia en diversos formatos, con facilidades de integración y utilización de las diferentes herramientas de comunicación sincrónica y asincrónica. Teniendo en cuenta lo anterior para la preparación en Seguridad Informática del personal de las instituciones se emplea está plataforma utilizando sus amplias posibilidades dentro de las cuales se señalan las siguientes: cuestionarios, glosario, carpeta, foro, chat, wiki, blog y otros.

1.3 Caracterización del estado actual de la educación en Seguridad Informática de los técnicos de laboratorio de la Universidad de Guantánamo

El criterio de selección de la muestra fue aleatoria estratificada, con el objetivo de garantizar representatividad de sujetos por las distintas funciones y responsabilidades que desempeñan.

Se trabaja con una población de 1104 unidades de estudios comprendida por personal docente, administrativo y técnico de la Universidad de Guantánamo y los CUM, y con una muestra intencional de 58 técnicos vinculados a la informatización.

Para la exploración diagnóstica fue necesario determinar si existen en los documentos rectores del Ministerio de Educación Superior las orientaciones metodológicas necesarias para el desarrollo de la educación en Seguridad Informática del personal de sus instituciones. Para ello se usaron métodos y técnicas empíricas y estadísticas que permitieron realizar las valoraciones cualitativas y cuantitativas que apoyan las reflexiones teóricas.

Se realizó la observación participante de cuatro actividades en el desempeño de los técnicos de laboratorio de computación en el desarrollo de actividades profesionales la cual evidenció la existencia de fisuras en el cumplimento del Plan de Seguridad Informática en cuanto a:

- Política de Seguridad Informática.
- Estructura de Gestión.
- Sistemas de Medidas de Seguridad.

- Plan de Contingencia.
- Programa de Seguridad.
- Plan de Formación.

Se realizaron tres entrevistas y encuestas grupales a directivos y técnicos de laboratorio de computación, todas para constatar la preparación y educación en Seguridad Informática para enfrentar el servicio a usuarios en el proceso de informatización en función de diagnosticar el problema científico. Tras la aplicación de dichos métodos se constatan limitaciones en el conocimiento y aplicación de medidas sobre Seguridad de las Tecnologías de la Información en cuanto a:

- El nivel de seguridad para los diferentes niveles de informaciones.
- Pobre conocimiento acerca de la preservación de los bienes informáticos.
- Poca percepción de las vulnerabilidades de las amenazas a la Seguridad Informática.
- Desconocimiento de los diferentes tipos de delitos Informáticos.

Durante el estudio documental se procedió a lectura y estudio de la bibliografía, documentación sobre el tema y las diferentes regulaciones, en tal sentido, se revisaron los siguientes documentos:

- Orientaciones emitidas por el Ministerio de Educación Superior a sus instituciones sobre Seguridad Informática, como resoluciones y circulares.
- Los programas de la asignatura Informática para las diferentes en las diferentes carreras.
- Programa para la educación en informática en los eslabones de base.
- Los registros de las inspecciones realizadas por el Ministerio de Educación Superior a sus dependencias en los tres últimos años.

Estos documentos permitieron constatar las fuentes de que dispone el personal de la Universidad de Guantánamo para su educación en Seguridad Informática, así como la calidad de la información que contiene cada fuente.

En los registros de inspecciones se señalan insuficiencias en el personal técnico, tales como:

- No se realizan acciones continuas de educación al personal sobre Seguridad Informática.
- Antivirus no actualizados.
- Uso del gestor de correo electrónico de forma inadecuada.
- Contraseñas mal configuradas y poco seguras.
- Escritorios de las computadoras con grandes volúmenes de información, incluidas algunas de carácter limitado.
- Navegación por páginas de Internet que no son fundamentales para el trabajo de la institución.
- No se realizan salvas periódicas de la información contenida en las computadoras, como procedimiento para proteger la información.
- Los planes de Seguridad Informática son muy generales y no parten del análisis del sistema informático de la institución.
- No garantizan en algunos casos las medidas de seguridad física.
- En ocasiones faltan las medidas de seguridad técnicas.
- No se recogen con claridad en los planes de prevención las medidas de seguridad administrativas/organizativas y de seguridad de operaciones.
- No siempre se discuten con los trabajadores las medidas de seguridad legales.
- Falta de sistematicidad en la superación del personal medidas de seguridad educativas/concientización.

Sobre el estudio documental se puede resumir que:

Lo anterior confirma que existen documentos contentivos de información relacionada con la Seguridad Informática para el personal de las instituciones del MES, aunque esta resulta insuficiente en lo relacionado con la educación que necesita el personal, pues en

ella predomina lo regulatorio y normativo, y no lo metodológico y de orientación para hacer y saber hacer.

En la planificación y ejecución de la asignatura Informática del plan de las diferentes educaciones y los de las carreras pedagógicas, así como en los cursos que se imparten al personal, no se aprovechan las potencialidades existentes para contribuir a la educación en Seguridad Informática, con vista a reforzar el conocimiento y la aplicación responsable del plan de contingencia y dentro de él, a saber:

- Definición general del plan contingencia.
- Determinación de vulnerabilidades en cada escenario.
- Selección de los recursos alternativos para preservar los bienes informáticos y los intangibles.
- Preparación detallada del plan con responsabilidad administrativa.
- Pruebas de vulnerabilidades.
- Mantenimiento de los equipos.

En resumen puede señalarse que la aplicación de los instrumentos posibilitó constatar que aún es insuficiente el nivel de orientación y educación del personal de las instituciones del MES hacia los temas de la Seguridad Informática, así como el no aprovechamiento desde el punto de vista organizativo de los espacios que tienen para realizar actividades de educación con su personal en este tema. **(Anexos 1, 2, 3 y 4).**

Conclusiones del capítulo I.

El estudio que caracteriza el proceso de Informatización en la Universidad de Guantánamo la Seguridad Informática constituye el soporte de cambio en el proceso de dirección educacional.

Precisamente, en este tipo de acción para contribuir a la educación es indispensable operar desde la interdisciplinariedad en la superación de los técnicos de laboratorio - tanto en el plano individual, profesional como social - en las diversas situaciones de aprendizaje con el fin de solucionar las insuficiencias que todavía se manifiestan en la gestión de los procesos sustantivos de la Universidad de Guantánamo.

CAPITULO II: SITIO WEB PARA LA EDUCACIÓN EN SEGURIDAD INFORMÁTICA DE LOS TÉCNICOS DE LABORATORIO EN LA UNIVERSIDAD DE GUANTÁNAMO

En el presente capítulo se presenta una sistematización teórico-metodológica para la educación en Seguridad Informática; se argumentan los componentes teórico y metodológico como parte de la educación en Seguridad Informática en la Universidad de Guantánamo. Se describe el diseño gráfico e interfaz del sitio web sobre Seguridad Informática con los productos de Macromedia. Finalmente, se corrobora la factibilidad de la propuesta para contribuir en la educación sobre Seguridad Informática de los técnicos de laboratorio de computación en la Universidad de Guantánamo.

2.1 Requerimientos teórico-metodológicos del sitio web para la contribución a la educación en Seguridad Informática

La modelación teórico-metodológica d la web propuesta desde su estructura y contenido se manifiesta a través de sus relaciones esenciales tanto en lo teórico como en lo metodológico.

Se asume que el diseño del sitio web para la contribución a la educación en Seguridad Informática parte de los fundamentos filosóficos, ideológicos, sociológicos, psicológicos y pedagógicos asumidos en el capítulo uno de esta tesis y dos componentes: uno teórico y otro metodológico que se complementan e integran dialécticamente en el proceso de la educación en Seguridad Informática.

El componente teórico presenta los siguientes requerimientos:

En la actualidad la Seguridad Informática y su educación enfrentan retos de importancia a nivel global y, particularmente, en el personal de las instituciones del Ministerio de Educación Superior.

Esto presupone un esfuerzo mancomunado de los miembros del consejo de dirección, funcionarios, personal docente y no docente para lograr que los sujetos estén cada vez mejor preparados para enfrentar los retos del uso más seguro de las tecnologías

existentes y avizorar los nuevos problemas de seguridad que se introducirán con las tecnologías emergentes.

El sustento teórico metodológico de este sitio web, como proyecto de mejoramiento profesional y humano, está dirigido al perfeccionamiento de la educación en Seguridad Informática en la Universidad de Guantánamo.

El componente teórico lo forman los fundamentos de las TIC en la educación, conceptos fundamentales asociados con la educación en Seguridad Informática y los principios para la educación en Seguridad Informática

El componente metodológico presenta los siguientes requerimientos:

El componente metodológico estructura y orienta el proceder para la educación en Seguridad Informática del personal de en correspondencia con las demandas de su práctica actual.

Está integrado por:

- La estructura por niveles de la educación en Seguridad Informática.
- Tipología de actividades para la educación en Seguridad Informática.
- Los recursos educativos.

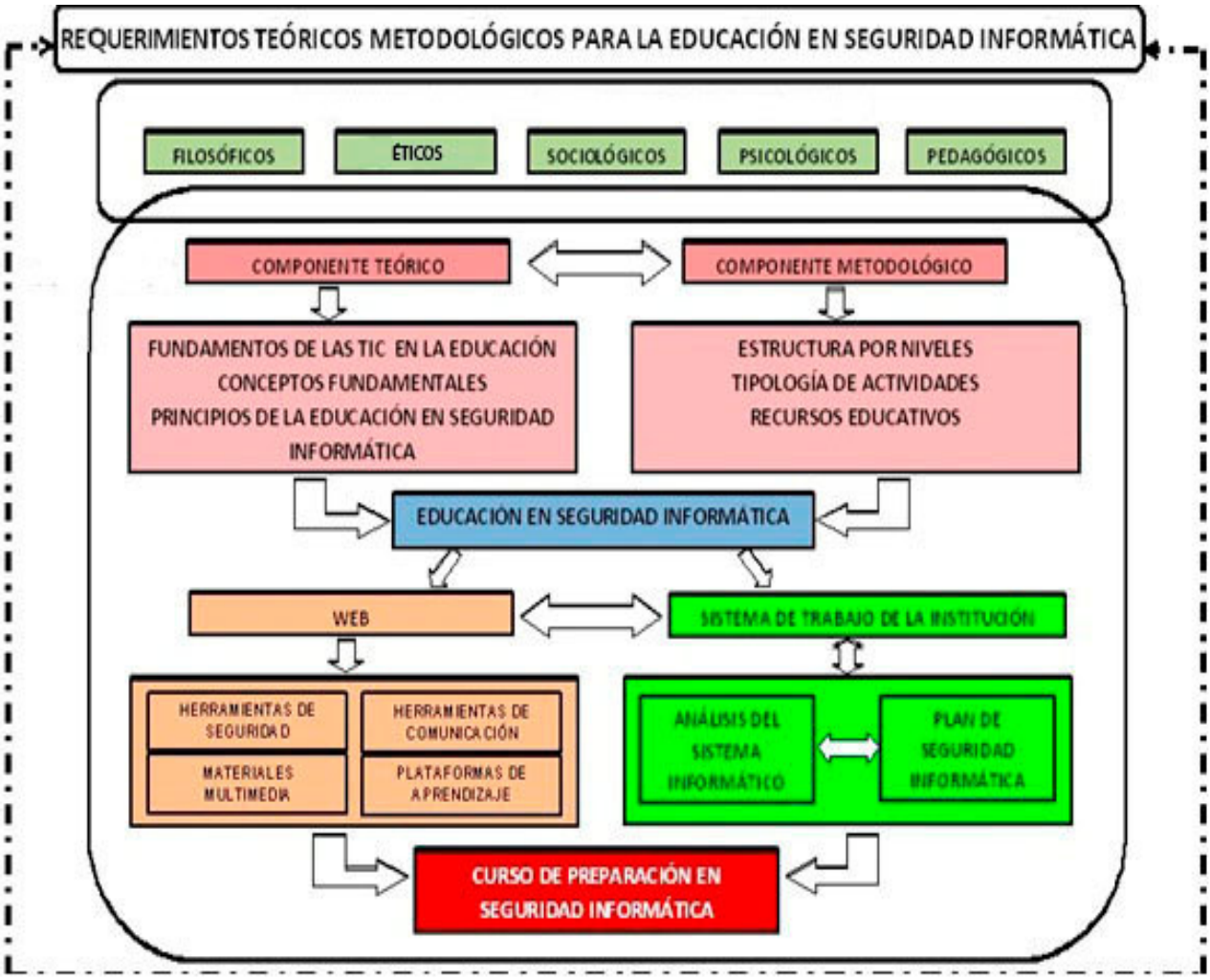
Vale destacar que en la propuesta se establecen las relaciones esenciales entre los componentes teórica metodológica de la web, donde los fundamentos para la educación en Seguridad Informática (filosóficos, éticos, sociológicos, psicológicos y pedagógicos) desempeñan un papel de orientación instrumental. Esta relación establece la dependencia de los fines de la educación en Seguridad Informática del personal de acuerdo a las necesidades, demandas y problemas sociales que se deben resolver a través de la educación delos miembros de la comunidad universitaria.

La relación entre el componente teórico y el metodológico, se expresa en que el primero es el determinante (conceptos, leyes, principios, categorías relacionados con la educación

en Seguridad Informática) y la metodológica estructura y orienta el proceder de la educación en Seguridad Informática para satisfacer las demandas de su práctica actual.

Aunque el nivel de relaciones de lo teórico sobre lo metodológico es predominante, ambos se complementan, ya que este último es la aplicación práctica de lo primero.

Representación de los requerimientos teóricos y metodológicos del sitio web sobre Seguridad Informática.



Los componentes teórico y metodológico se integran en el proceso de la educación en Seguridad Informática ya que es allí donde se manifiestan y concretan los elementos teóricos y prácticos de la web, mientras la educación en Seguridad Informática actúa como eje articulador de varios componentes, entendido como el contenido fundamental alrededor del cual giran varios componentes, que este permite unir, enlazar y organizar con el fin de transformar la educación del personal de las instituciones del Ministerio de Educación Superior en Seguridad Informática.

Para la web propuesta, la educación en Seguridad Informática constituye el eje temático articulador, considerado un componente esencial para el éxito del proceso de educación del personal en Seguridad Informática. Posee, entre sus peculiaridades, la búsqueda de las vías que armonicen y favorezcan la educación de los sujetos en este tema y en su contexto de actuación; se sustenta en los dos elementos básicos: la web y el sistema de trabajo de la institución donde sus relaciones son de complementación.

La web, como espacio virtual, facilita el uso de los recursos educativos a través de: las herramientas de comunicación, materiales multimedia, herramientas de Seguridad Informática y las plataformas de aprendizaje; se complementan a través de la divulgación y la comunicación todos los aspectos que desde el sistema de trabajo de la institución se tracen en el análisis del sistema de Seguridad Informática y su concreción en políticas, medidas y procedimientos en el plan de Seguridad Informática, a su vez tendrán su salida en los cursos de educación en correspondencia con las carencias de los sujetos.

Elemento importante de los requerimientos teórico metodológicos de la web es su retroalimentación como todo proceso, a partir de diagnosticar las deficiencias y reorientan las acciones para corregirlas. Este aspecto tiene un carácter sistemático, organizado y planificado.

A continuación se desarrolla el contenido del componente teórico en que se sustenta el sitio web propuesto.

Fundamentos de las TIC en la Educación: se asumen los fundamentos de las TIC en la educación abordados en el capítulo uno de la memoria escrita; entre ellos se tuvieron en cuenta los siguientes:

• El empleo de plataformas de aprendizaje para la educación a distancia.

• Como medio para apoyar la educación del personal a través de materiales multimedia.

• El uso de herramientas de comunicación.

• El empleo de herramientas para la Seguridad Informática de fácil comprensión para los sujetos.

Conceptos fundamentales de la educación en Seguridad Informática.

Se consideran como conceptos fundamentales: tecnología, TIC, Seguridad Informática, sistema informático, educación en Seguridad Informática y educación en Seguridad Informática. (La fundamentación y definiciones de los conceptos fundamentales se encuentran explicados en el primer capítulo).

La estructura de la educación en Seguridad Informática por niveles: se organizan los cursos de educación en Seguridad Informática por niveles de acuerdo con las características de los técnicos de laboratorio de la Universidad de Guantánamo.

Nivel I. General:

Incluye los fundamentos de la Seguridad Informática en la educación, los conceptos esenciales sobre esta temática, bases legales y normativas existentes en Cuba y en la institución y su incidencia en la responsabilidad personal y social en el uso de las TIC. Las principales amenazas y vulnerabilidades asociadas a la Seguridad Informática, obstáculos que impiden un comportamiento responsable hacia la Seguridad Informática

Nivel II. Intermedio:

Contempla la Seguridad Informática en las tareas cotidianas de la educación, a partir de las actividades que realiza el personal de una institución con el uso de las TIC. Abordará

los conocimientos necesarios desde las TIC, para su desempeño y utilización, violaciones de la Seguridad Informática en la institución, programas malignos, necesidad de las claves de acceso, sus características, medidas de prevención ante el uso de dispositivos externos, necesidad de salvas de información, navegación por Internet para la búsqueda de información; uso del correo electrónico de forma más segura y los incidentes de Seguridad Informática.

Nivel III. Superior:

Incorpora las configuraciones de manera más segura en las herramientas y aplicaciones informáticas utilizadas en la educación y en particular en la institución. Abordará los conocimientos necesarios para realizar configuraciones seguras de las herramientas y aplicaciones informáticas esenciales para su utilización, como: el uso de carpetas y su protección, la organización de la información y la protección de documentos que por su importancia merecen ser protegidos (el correo electrónico, mensajería instantánea, aplicaciones ofimáticas, navegadores de Internet), reconocimiento y protección de navegación por páginas dinámicas, procedimientos para la búsqueda y localización de información en Internet, actualizaciones del sistema operativo, antivirus, necesidad de detectar y reportar incidentes. Permitirá desarrollar habilidades prácticas en el diseño de políticas de seguridad en las herramientas y aplicaciones informáticas más utilizadas por el personal de las instituciones del MES.

Nivel IV. Específico:

Abarca la metodología para el diseño de un sistema de Seguridad Informática, entre los que se incluyen aquellos elementos esenciales para realizar un análisis del sistema informático de una institución, a partir del diseño. Procurará identificar sus vulnerabilidades, así como las medidas y procedimientos que deberán ser elaborados - a partir de la situación real de cada lugar, además de las implicaciones que tendrá todo el personal.

Los niveles planteados tienen carácter de sistema, lo cual le imprime un orden lógico y una condición de precedencia, dada por la subordinación de los niveles inferiores a los

superiores, es decir, que para llegar al nivel superior debe haber vencido los que le anteceden, lo que no limita que cada nivel pueda ser alcanzado en diferentes momentos del desempeño del personal.

Se pueden emplear diferentes vías para alcanzar los objetivos planteados en cada nivel. Ello conduce a la utilización de variadas formas, según lo establece la Resolución No. 29/06 del Ministerio de Trabajo y Seguridad Social (MTSS) donde se reglamenta la planificación, organización, ejecución y control del trabajo de capacitación y desarrollo de los recursos humanos en todas las entidades laborales del país, además de lo establecido en la Resolución Ministerial 132/2004 del Ministerio de Educación Superior sobre el Reglamento de postgrado.

Entre las actividades orientadas durante el desarrollo de los cursos se encuentran:

- Observación de materiales didácticos.
- Realización de consultas bibliográficas en los materiales elaborados para los cursos y el uso de otros materiales como bibliografía complementaria.
- Confección de resúmenes de la información presentada mediante diapositivas.
- Uso de las ayudas de los sistemas de aplicaciones y herramientas informáticas.
- Visitas al sitio web de Seguridad Informática y otros relacionados con esta temática, para la búsqueda de información sobre un tema.
- Actualización del glosario de términos.

A continuación se muestra una muestra del glosario de términos sobre Seguridad Informática que contiene el sitio web:

GLOSARIO

Bucaneros:

Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos " Crackeados " pasan a denominarse " piratas informáticos " así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

Copyhackers:

Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año mas de 25.000 millones de pesetas sólo en Europa.

En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los " bucaneros " personajes que serán detallados mas adelante.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello " extraen " información del verdadero Hacker para terminar su trabajo.

La principal motivación de estos nuevos personajes, es el dinero.

Crackers:

Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Para los grandes fabricantes de sistemas y la prensa este grupo es el mas rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica hay, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica. Mas adelante hablaremos de los Cracks más famosos y difundidos en la red.

Hackers:

El primer eslabón de una sociedad " delictiva " según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de " he estado aquí " pero no modifican ni se llevan nada del ordenador atacado.

Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones o emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso.

Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

2.2 Diseño de sitio web para la contribución a la educación en Seguridad Informática.

Para el diseño gráfico e interfaz de sitio web Seguridad Informática, se eligieron como herramientas los conocidos productos de Macromedia: Dreamweaver MX y Adobe PhotoShop, por su entorno cómodo y fácil para el diseño web y las múltiples herramientas que poseen, encaminadas a este tipo de trabajo, sin olvidar las bondades estéticas que son capaces de ofrecer al usuario final.

Como lenguaje para manipular los datos en páginas dinámicas se escogió PHP, por sus cualidades de lenguaje multiplataforma con código sencillo basado en Perl y C++ y que constituye un excelente manipulador de ficheros. Esta elección unida a la de MySQL como gestor de bases de datos constituye la combinación más efectiva, veloz y robusta empleada en la actualidad.

Otra razón para la elección de MySQL es que no se necesita pagar licencias por su uso. Este gestor de base de datos se adscribe al contrato de fuente abierta.

PHP: el PHP -acrónimo de "PHP: Hypertext Preprocessor"-, es un lenguaje interpretado de alto nivel embebido en páginas HTML y ejecutado en el servidor.

Ventajas de PHP

- Capacidad de conexión con la mayoría de los manejadores de base de datos que se utilizan en la actualidad.
- Leer y manipular datos desde diversas fuentes, incluyendo datos que pueden ingresar los usuarios desde formularios HTML.
- Capacidad de expandir su potencial utilizando la enorme cantidad de módulos (llamados ext's o extensiones).
- Es libre, por lo que se presenta como una web de fácil acceso para todos, entre otras.

Requerimientos mínimos

Memoria RAM 64 MB, velocidad del micro 533 HZ, Capacidad de disco duro 700MB, 4. Kit de memoria, Lector de CD 4x y Windows 9X, NT o XP.

Construcción del sitio web

El diseño es la parte del proceso de desarrollo del sitio web cuyo propósito primario es decidir cómo el sistema se llevará a cabo. Durante el diseño, se toman decisiones estratégicas y tácticas para cumplir los requerimientos funcionales y de calidad del sistema para dar respuesta a la pregunta de: ¿cómo hacer?

El sitio web que se adjunta en CD fue diseñada partiendo de la situación problémica abordada en la introducción. Se trazó una estrategia en la cual se tuvieron en cuenta diversas concepciones teóricas que lo promueven: como medio de enseñanza, medio de información, interrelación estudiante- tecnología. (Anexo 6)

La información que se publica en el sitio web Seguridad Informática son cuestiones referentes a la asignatura Seguridad Informática, con el objetivo de que sirva como medio de auto-aprendizaje al instructor y que a través de la utilización sistemática de ella se apropien de los conocimientos de la asignatura.

Reglas generales para el diseño del sitio web:

Existen varias normas, recomendaciones y requerimientos con estos fines, a modo de resumen, se asumen algunas consideraciones generales:

- **Análisis del medio y el receptor**: las expectativas de cómo los lectores usarán el portal y las propias cualidades de los receptores típicos, deben ser los elementos que gobiernen la línea de diseño.
- **No imponer un estilo**: el estilo gráfico y editorial del sitio debe evolucionar de acuerdo con sus intereses y, como consecuencia natural y lógica, de su uso y propósitos.
- **Maximizar el uso del encabezado del sitio:** el segmento que ocupa las primeras cuatro pulgadas es completamente visible por cualquier monitor. **Utilizar colores sutiles**: el uso de colores es importante para lograr un buen efecto visual. La selección del color debe ser cuidadosa.
- **Cuidado con la iconografía y el "embellecimiento" gráfico**: el uso de las líneas horizontales, los íconos y otros marcadores gráficos de acuerdo al Manual de Imagen Corporativo de la Universidad de Guantánamo.

- **Buenas Prácticas:** una de las características que hace tan popular a la tecnología web es su facilidad para mostrar contenidos de manera gráfica y para vincular de manera fácil documentos de diferentes orígenes.

Por otro lado, El diseño de interfaz de usuario es una tarea que ha adquirido relevancia en el desarrollo de un sistema. La calidad de la interfaz de usuario puede ser uno de los motivos que conduzca a un sistema al éxito o al fracaso, es por eso que uno de los aspectos más relevantes de la usabilidad de un sistema es la consistencia de su interfaz de usuario.

La Interfaz de Usuario (IU) de un programa es un conjunto de elementos hardware y software de una computadora que presentan información al usuario y le permiten interactuar con la información y con la computadora. También se pueden considerar parte de la Interfaz de Usuario (IU) la documentación -manuales, ayuda, referencia, tutórales- que acompaña al hardware y al software.

Si la Interfaz de usuario (IU) está bien diseñada, el usuario encontrará la respuesta que espera a su acción. Si no es así puede ser frustrante su operación, y puede provocar que el usuario abandone el sistema.

Es por esto que la interfaz del sistema se ajustará a los estándares establecidos para el desarrollo de un buen diseño. Deberá tener consistencia con el mundo real de manera que los conceptos manejados sean conocidos y familiares por los estudiantes para que les sea fácil su uso y aprendizaje.

Estará diseñada de modo tal que el usuario pueda ir de un punto a otro dentro de ella con gran facilidad, estarán visibles todas las opciones disponibles, en el momento requerido. Se trata de que la aplicación sea lo más interactiva posible. El sitio web sobre Seguridad Informática como medio de enseñanza brinda una interfaz simple y de fácil uso para que el usuario, no tenga dificultad al interactuar con el sistema.

El correcto diseño del sitio web transita por una serie de etapas:

- Análisis de la información que presentará el web.
- Búsqueda y organización.

- Diseño informacional del sitio o diseño gráfico.
- Elaboración de la interfaz.

Posteriormente para la construcción de la interfaz gráfica del sitio web se utilizan las del lenguaje PHP y el diseñador gráfico Photoshop, las páginas se construyeron a partir de una de las plantillas disponibles.

Elaboración del material en formato electrónico

Paso 1

- Planificar el sitio web.
- Elaborar el árbol o esquema del módulo (realizar una representación gráfica en papel de las páginas web y los enlaces entre las componentes que configurarán el material).
- Decidir la información que se presentará en cada pantalla o página y redactarla. Cada página se archivará como un fichero o archivo independiente.

Paso 2

- Desarrollar el material en formato HTML.
- Decidir y desarrollar los aspectos formales de las páginas (fondos, iconos) para un entorno de presentación. Debe ser homogéneo para un grupo de páginas similares.
- Establecer los enlaces hipertextuales (internos y externos al módulo).
- Incorporar íconos de enlaces y activarlos.
- Determinar los colores e imágenes, que se adapten al contenido en cuestión.
- Probar en un navegador Internet explorer o Netscape y revisar los posibles fallos.

En el diseño del sitio web confluyen conocimientos procedentes de diversas disciplinas como las ciencias de la información y la comunicación, el diseño informacional y la cibernética, así como potentes editores web: Lotus World Pro, Microsoft Front Page, Netscape Comunicator, Macromedia Dreamweaver.

El autor de esta tesis considera que el sitio web es un medio de enseñanza por las siguientes razones.

- La información situada en el soporte magnético es muy abundante y existen posibilidades de impresión; además permite a los estudiantes el acceso a la bibliografía en tiempo de máquina y la interacción con la computadora.
- Vincular la asignatura con la utilización de las computadoras durante el desarrollo de los temas, lo cual contribuye mejorar el proceso y lograr mayor motivación por esta.

- Todas las máquinas tienen un visualizador web.
- Las posibilidades para el trabajo en red a nivel de laboratorio y a distancia.
- Permiten acceder a hipervínculos e imágenes para favorecer la comprensión del contenido.

En el sitio web aparecen:

Al introducir este recurso informático en la educación, se deben producir cambios en las categorías principales del sistema didáctico: objetivos – contenidos - métodos y que, en este caso, el sitio como medio se integra al sistema didáctico, con lo que resulta un sistema más complejo: objetivos – contenidos – métodos – medios.

En este sistema hay que considerar el sitio web no como un medio tradicional capaz de transmitir determinada información, sino como un componente integrado al proceso que modifica la concepción del tema al ser portador de características particulares que lo hacen diferentes a todos los demás medios de enseñanza y que se han visto en epígrafes anteriores. El autor considera que para la introducción del sitio web como medio de enseñanza se hace necesario, entre otras condiciones, que se pueda contar con el equipamiento adecuado en los centros, con el personal preparado en el manejo de este medio y con una concepción didáctica que permita orientar a los usuarios en este sentido.

La inserción de la Seguridad Informática en la Educación Superior impuso la necesidad de la formación del personal docente capaz de asumir la dirección del proceso de enseñanza aprendizaje de esta asignatura, es decir capacitar a los usuarios de Seguridad Informática para derivar los objetivos del tema a partir de los objetivos del programa, los contenidos, los métodos, los medios, la forma de evaluación.

De modo que puedan planificar y ejecutar la dirección del proceso de educación de esta disciplina, para de esta forma propiciar que los estudiantes participen conscientemente y no como sujetos pasivos necesitados de adquirir conocimientos, desarrollar habilidades y capacidades que los formen en correspondencia con las exigencias de la sociedad cubana actual.

Es necesario diferenciar la variedad existentes entre tipos virus y anti-virus. Desarrollar habilidades en la determinación del hardware específico para desarrollar actividades

afines. Conocer las tipologías y las partes de una red de computadoras. Contribuir a la formación integral de los estudiantes a partir de la concepción científica del mundo y trabajar en la formación de valores.

De estos objetivos se derivan los específicos para cada unidad y de estos con cada tema. En estos temas se seleccionaran los tipos de métodos y medios de enseñanza que permitan el desarrollo del proceso.

Facilidad de uso:

- Cómodo de usar de manera que los estudiantes puedan utilizarlos sin dificultad.
- Ver realizados sus propósitos de localizar información.
- Obtener materiales y encontrar enlaces.
- Encontrar el contenido de un tema específico.

En cada momento el estudiante debe conocer el lugar del sitio web donde se encuentra y tener la posibilidad de moverse según sus preferencias: retroceder, avanzar.

Calidad del entorno: el sitio web posee un entorno comunicativo. Algunos de los aspectos que, en este sentido, se tuvieron en cuenta son los siguientes:

- Diseño general claro y atractivo de las pantallas: No existe exceso de texto y que resaltan a simple los aspectos notables.
- Calidad técnica y estética en sus elementos:
- Títulos, menús de opciones, ventanas, iconos, botones, espacios de texto, imagen, formularios, barras de navegación, elementos hipertextuales y fondo.
- Elementos multimedia: gráficos, fotografías, animaciones y vídeo.
- Estilo y lenguaje, color, composición, entre otros.
- Adecuada integración de medios, los que se encuentran al servicio del aprendizaje, sin sobrecargar la pantalla, bien distribuidas, con armonía.

La calidad en los contenidos: al margen de otras consideraciones pedagógicas sobre la selección y estructuración de los contenidos según las características de los usuarios, se tuvieron en cuenta las siguientes cuestiones:

- La información que se presenta es correcta y actual, se presenta bien estructurada diferenciando adecuadamente: los diferentes menú: el principal, el del usuario y acceso a la web.
- Los textos no tienen faltas de ortografía y la construcción de los contenidos es correcta.

Capacidad de motivación:

- Resulta atractivos para los estudiantes.
- Un medio de enseñanza que despierta el interés en los alumnos.
- Resulta motivador para los estudiantes a fin de potenciar los aprendizajes.

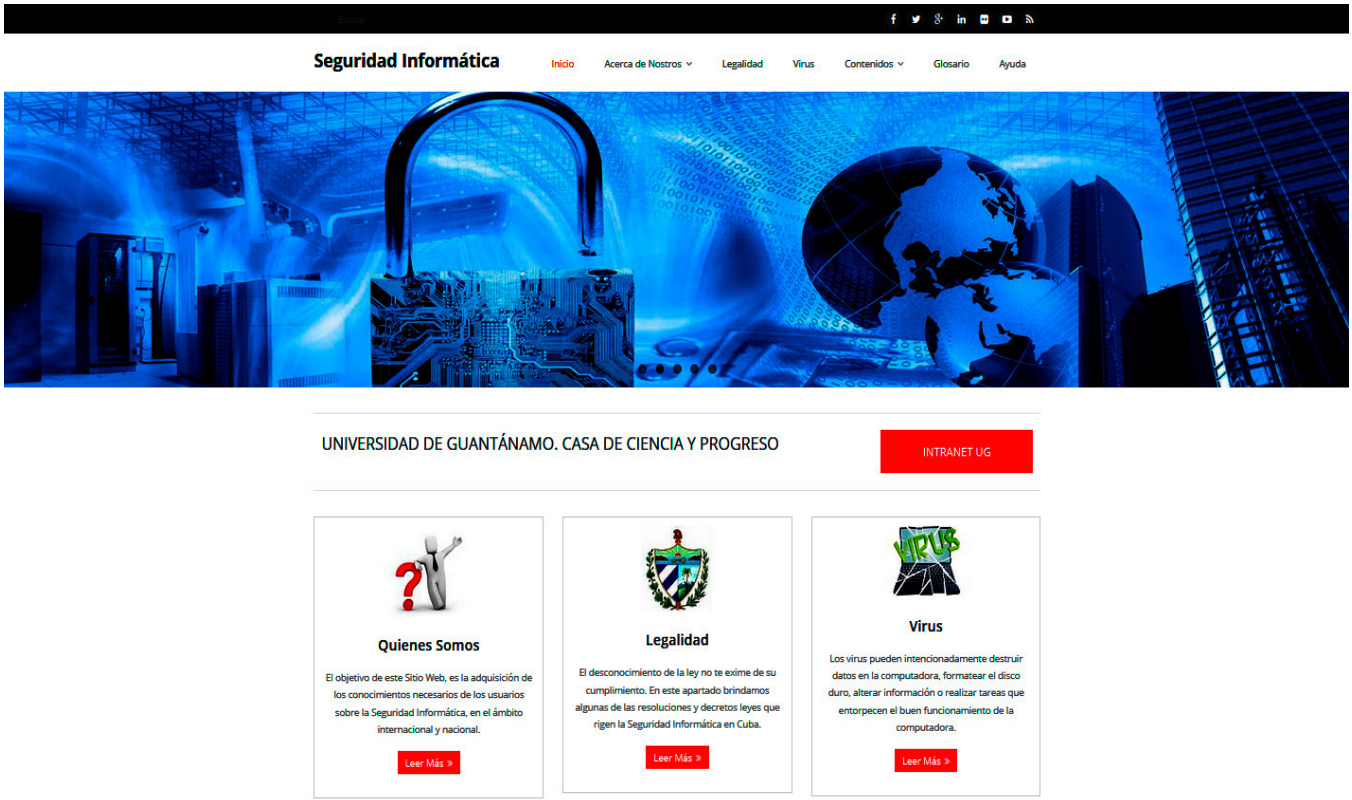
En este sentido las pantallas y las actividades despiertan y mantienen la curiosidad y el interés de los usuarios hacia la temática de su contenido.

Fomenta el autoaprendizaje:

- Potencia el aprendizaje de los estudiantes.
- Proporciona herramientas cognitivas para que los estudiantes hagan el máximo uso de su potencial de aprendizaje.
- Contribuye a decidir las tareas a realizar, la forma de llevarlas a cabo y puedan auto controlar su trabajo.

Diagrama de flujo del sitio web

La interfaz gráfica del sitio no cambia se mantiene estático, solamente cambian el contenido de las secciones cuando el usuario hace un clic en algunas de ellas, en dependencia de los módulos en los que se encuentran navegando, lo que permite mayor usabilidad.



Ventana principal

Figura. No. 1 Diagrama del sitio web Seguridad Informática

El menú superior o barra de navegación contiene las opciones:

Inicio Temas sobre legalidades, Virus, Glosario y Ayuda

Inicio: Al hacer clic me lleva siempre a la página de inicio.

Temas: permite acceder a todos los temas con sus momentos.

- **Legalidad**: permite visitar las resoluciones que rigen la Seguridad Informática.
- **Virus**: hace una breve referencia a los distintos virus existentes.
- **Glosario:** un pequeño diccionario técnico.
- **Ayuda:** breve explicación de la web

También presenta al igual que las demás ventanas una barra de navegación en la parte superior debajo del banner y título de la página, con el menú que está el contenido de la web y sus botones interactivos que llevan a un contenido, que se explica más abajo.

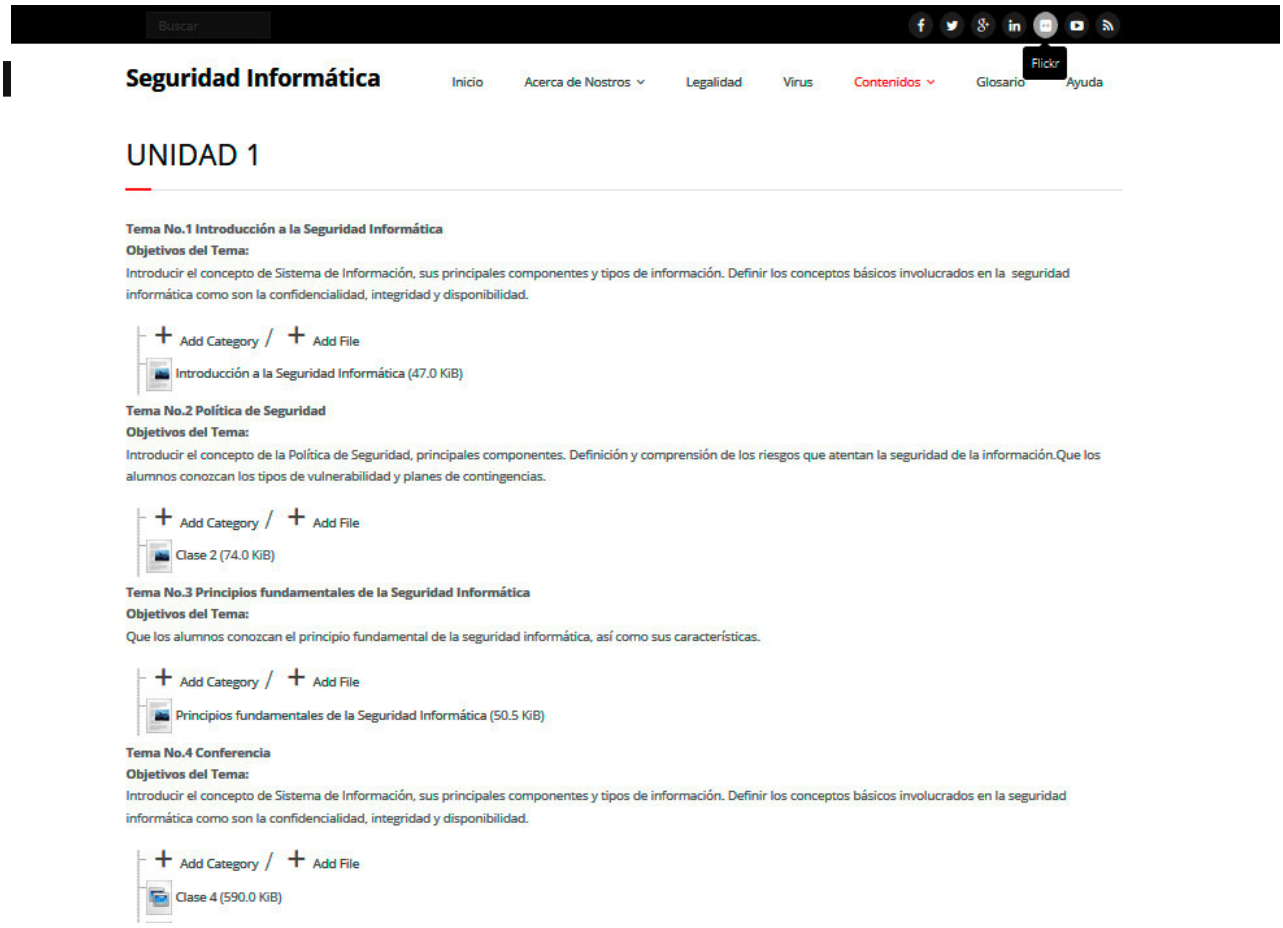


Figura. No. 2 Contenido del sitio web

El sitio web

Menú temas: desglosa de seis unidades una introducción y un módulo base material de estudio que sirve de consulta a usuarios y alumnos.

Implementación del sitio web

Análisis. En esta etapa se hace un análisis de la situación, con el fin de identificar fallas en el proceso, proponiéndose soluciones a los problemas existentes.

En esta etapa se hace un diagnóstico de la situación que presenta la asignatura objeto de estudio. Proceso orientado al examen sistemático, suficientemente riguroso, para determinar las características de la situación en que se encuentra el proceso de

educación de la asignatura y evaluación del grado de incidencia que tienen los factores internos y externos para el cumplimiento de sus objetivos.

Se desarrolla a través de seis salidas: presentación del equipo consultor e identificación del grupo de expertos, caracterización de la asignatura objeto de estudio, condiciones en que se desarrolla el proceso de educación en la Universidad de Guantánamo, diagnóstico de la situación actual de la asignatura, condiciones actuales -tecnológicas, conocimiento sobre el tema que presentan los usuarios de Seguridad Informática al tema objeto de investigación y otras

Determinación de requerimientos:

- El tipo de material a desarrollar los requerimientos de equipos, materiales y recursos humanos.
- El lenguaje se va a diseñar el sitio web, qué programas complementarios van a utilizar.

Diseño de Instrucción: comprende la determinación de la conducta de entrada, el planteamiento de objetivos terminales y de objetivos específicos.

Es por estas razones que se hace necesario el planteamiento de los objetivos del sitio web como medio de enseñanza.

- Determinación de contenidos: en función de los objetivos específicos.
- Determinación de secuencias de aprendizaje. Clasificación del contenido.

En esta etapa se seleccionan qué contenidos debe tener el sitio web, cuáles son encaminados a trabajarlos en los temas y que van servir como medio de enseñanza y los que se van a utilizar para orientar como trabajo independiente.

El diseño del sitio web comprende: el diseño de la información (su adecuada organización, redacción clara y precisa de forma tal que los estudiantes se sientan motivados con los contenidos que comprende dicho sitio); el diseño de la estructura (clara, fácil de navegar, que los estudiantes visualicen la información, que los hipervínculos sean correctos e indiquen la ruta hacia dónde verdaderamente estén enlazados) y la elaboración de un mapa de navegación en el sitio propuesto.

Diseño comunicacional: comprende el diseño de la interfaz (la determinación de los controles de navegación -botones, opciones de menú, zonas activas de pantalla o hipertexto)

La etapa de desarrollo comprende: digitalización de los elementos multimedia (textos, imágenes: fijas y en movimiento, sonidos y efectos especiales).

Pruebas: prueba de interfaz y de funcionamiento. Con estas se pueden detectar: errores de funcionamiento, fallas en los enlaces y aceptación del sitio web por parte de los usuarios a los cuales va dirigida.

Prueba de efectividad: esta prueba permite determinar el impacto del sitio web como medio de enseñanza, Se realiza en una situación real de aprendizaje, utilizándola como apoyo instruccional en el desarrollo de un curso normal.

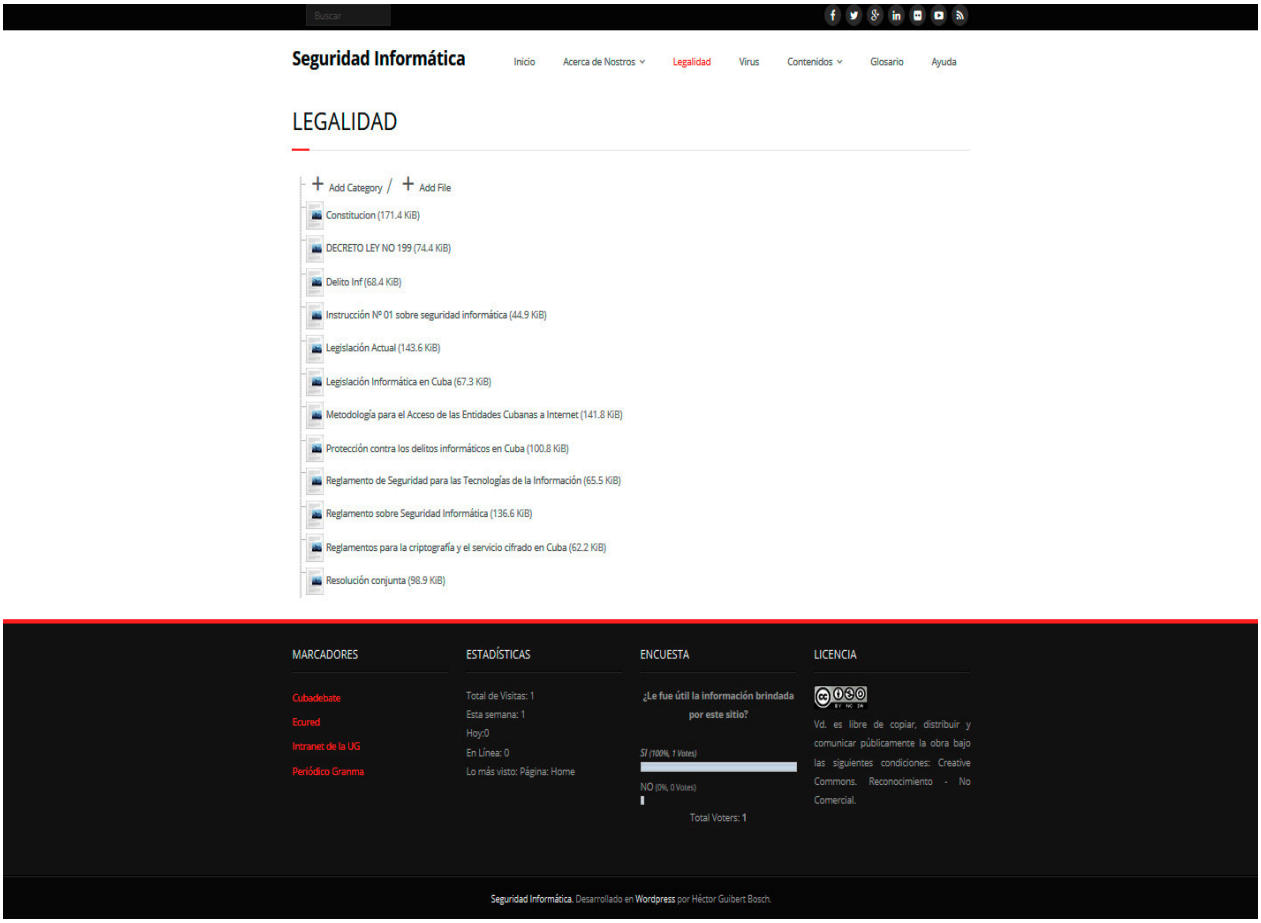
Utilización del sitio web como medio de autoaprendizaje

El sitio web sobre Seguridad Informática es un medio de enseñanza muy apropiado para el proceso de educación de la Seguridad Informática, en tanto pone al alcance de los técnicos de laboratorio de computación, fuentes de información que sería imposible hacerles llegar a todos los usuarios como, por ejemplo: imágenes de los diferentes tipos y generaciones de virus que afectan componentes de la computadora; videos, tablas, glosario de términos, entre otros.

La capacidad del hipertexto de orientar en múltiples direcciones las rutas de exploración y navegación en la web, según la opción e interés del usuario, amplían y profundizan el contenido que esta brinda, construir, en cada caso, una comunicación, un nivel de información y una narrativa diferente.

La estructura del sitio web debe ser constructiva, al tiempo que debe provocar el descentramiento temático en oposición, tanto a la segmentación del contenido a enseñar, como a lo unilateral-instrumental del conocimiento, todo ello para el logro de una intersubjetividad internalizada que posibilite el acceso a la objetividad racional ante los distintos universos temáticos.

Es que un entorno virtual dado por un sitio web debe atender tres rasgos característicos: la interacción, la variedad y la autorregulación, necesarias en la educación, en las modalidades presenciales, semipresenciales y sobre todo, a distancia.



Precisamente, en el siguiente ejemplo se demuestra lo anterior:

Figura No. 3 Aspectos legales dela Seguridad Informática

Sugerencias para la utilización del sitio web sobre Seguridad Informática

La propuesta presentada permite utilizar el sitio web como un medio de enseñanza para mejorar el proceso de educación en Seguridad Informática en la Universidad.

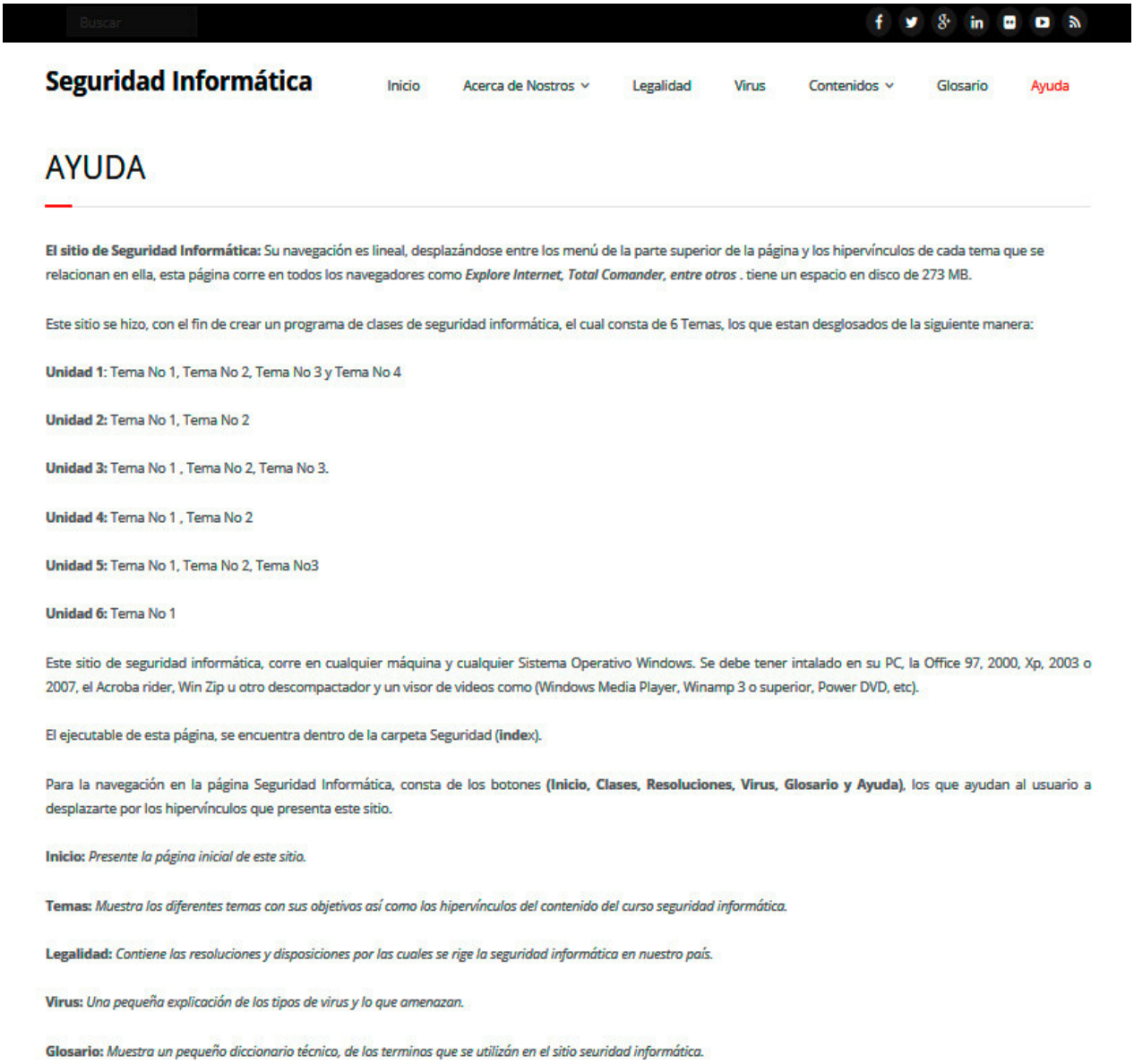


Figura No. 4 Sistema de ayuda para navegar en el sitio web

Es por ello que se proponen seis temas con diferentes temáticas, lo cuales se estructuran se de la siguiente forma:

Metodológicamente con objetivos definidos, además en cada tema aparecen preguntas de comprobación acerca de cada una de las temáticas que se tratan las que transitan desde una introducción a la Seguridad Informática hasta metodologías para la elaboración de un plan de Seguridad Informática.

A continuación se recoge el ordenamiento del curso:

Unidad 1: (consta de cuatro momentos)

Tema 1.- Introducción a la Seguridad Informática

Objetivos del tema:

Introducir el concepto de Sistema de Información, sus principales componentes y tipos de información.

Definir los conceptos básicos involucrados en la Seguridad Informática como son la confidencialidad, integridad y disponibilidad

1.1 Introducción.

1.2 Conceptos básicos.

1.2.1. Información y Sistema Informático.

1.2.2 Aspectos clave en la Seguridad en Sistemas de Información.

1.2.3. Definición de Seguridad Informática.

1.2.4. Confidencialidad.

1.2.5. Integridad.

1.2.6. Disponibilidad.

1.2.7. Otros aspectos relacionados.

Tema 2.- Política de Seguridad.

Objetivos del tema:

Introducir el concepto de política de seguridad y sus principales componentes.

Definición y comprensión de los riesgos que atentan contra la seguridad de la información.

Que los alumnos conozcan los tipos de vulnerabilidad y planes de contingencia.

1.3. Política de seguridad.

1.3.1 Análisis y gestión de riesgos.

1.3.2. Evaluación del valor del sistema informático (Cr).

1.3.3 Vulnerabilidad, amenazas y contramedidas.

1.3.4. Tipos de vulnerabilidad.

1.3.5. Tipos de amenazas.

1.3.6. Tipos de medidas de seguridad o contramedidas.

1.3.7. Planes de contingencia.

Tema 3.- Principios fundamentales de la Seguridad Informática.

Objetivos del tema:

- Introducir el tema Seguridad Informática conociendo su evolución histórica.
- Definir los conceptos fundamentales relacionados con la Seguridad Informática.
- Clasificar los distintos tipos de ataques informáticos y mecanismos de defensa.
- Establecer los principios básicos de Seguridad Informática.

Unidad 2 (consta de dos momentos)

Tema 1.- Seguridad Informática y Criptografía.

Objetivos del tema:

Definir qué es la criptografía y sus aplicaciones en los sistemas de cifra actuales así como una introducción general y amplia de las técnicas de protección de la información.

- Introducción. Conceptos básicos.
- Principios básicos de la criptografía.
- Tipos de ataque.
- Algoritmos criptográficos clásicos.
- Algoritmos criptográficos modernos.
- Algoritmos de clave simétrica.
- Función Resumen (MD4 , MD5).
- Firma Digital.
- Certificados Digitales.
- Entidades Certificadoras.

Tema: 2. Criptografía y Criptosistemas.

Objetivos del tema:

- Puesta en práctica de los conceptos de llaves públicas, privadas y firma digital estudiados usando la herramienta PGP.
- Utilizar la aplicación PGP para cifrar y/o firmar documentos.
- Utilizar la aplicación PGP para descifrar y/o comprobar firmas de documentos.
- Encriptación de ficheros, pasar el password, Ministerio de Educación Superior, certificados y firmar documentos.

Unidad 3 (consta de tres momentos)

Tema 1. Control de acceso. Identificación y autenticación.

Objetivos del tema:

- Introducir el tema del control de acceso como mecanismo esencial en la protección de la información.
- Definir los conceptos fundamentales relacionados con el control de acceso.
- Explicar las principales técnicas de identificación y autenticación.
- Describir los modelos fundamentales empleados para el control de acceso a los recursos.

Sumario:

- Introducción a los sistemas de control de acceso. Control de acceso. Conceptos fundamentales.
- Técnicas de identificación y autenticación.
- Autorización. Modelos de control de acceso.

Tema 2. Muros de seguridad o firewalls. Cortafuegos.

Objetivos del tema:

- Introducir el tema de los muros de seguridad como mecanismo esencial en la protección de las redes.
- Exponer los conceptos fundamentales de los cortafuegos .Explicar los modelos, tipos y arquitecturas de los muros de seguridad.

Sumario:

Introducción a los cortafuegos. Conceptos fundamentales de los muros de seguridad. Modelos de cortafuegos. Tipos de firewalls. Arquitecturas de cortafuegos.

Tema: 3 Sistemas de identificación y autenticación. (Seminario).

Objetivos del tema:

- Explicar el funcionamiento de los sistemas de identificación y autenticación más actuales.
- Realizar una búsqueda sobre el equipamiento tecnológico relacionado con estos sistemas, que permita identificar los principales fabricantes a nivel mundial y realizar una comparación de precios.
- Tarjetas inteligentes o smartcards.

- Verificación de huellas digitales.
- Análisis del iris y la retina.
- Verificación de voz.
- Patrones de escritura y firma.

Unidad 4 (consta de dos momentos)

Tema: 1 ISO 17799: La nueva norma técnica global de seguridad.

Objetivos del tema:

Que los cursistas conozcan cómo surge y evoluciona las normas técnicas de seguridad de la información reconocida a nivel mundial que incluye las prácticas exitosas de seguridad de la información.

- El origen de ISO 17799.
- Marco de las recomendaciones.
- Las diez áreas de control de ISO 17799.
- Beneficios de la norma técnica ISO 17799.
- La norma técnica ISO 17799.
- Mayor información.
- Artículos relacionados.

Tema 2

Taller (Cómo elaborar un Plan de Seguridad Informática.

Para cada uno de los casos se necesita hacer un análisis de riesgos y vulnerabilidades para posteriormente formular el conjunto de políticas de Seguridad Informática y realizar el análisis correspondiente para la determinación del sistema de medidas de seguridad o medidas y procedimientos.

Unidad 5 (consta de tres momentos)

Tema: 1 Ataque Informáticos y medios de defensa

Objetivos del tema:

- Conocer los términos empleados para referirse a los individuos que realizan ataques informáticos.
- Comprender los pasos a seguir por los atacantes para penetrar los sistemas informáticos.
- Enumerar y explicar las técnicas de ataques informáticos más comunes.

- Ejemplificar los mecanismos de defensa y medidas de Seguridad Informática.

Sumario:

- Términos empleados para distinguir a los atacantes.
- Pasos a seguir por los atacantes.
- Amenazas y ataques informáticos.
- Mecanismos de defensa y medidas de Seguridad Informática.

Tema: 2 Sistema de Prevención de Incidentes de Seguridad.

Objetivos del tema:

- Introducir el tema de los programas malignos detallando su evolución histórica.
- Definir el concepto de programa maligno y caracterizar los diferentes tipos de malware.
- Describir las técnicas empleadas por los virus informáticos para su propagación y defensa.
- Describir los mecanismos empleados por los antivirus para la detección de virus.
- Mencionar los principales productos antivirus, así como los aspectos fundamentales a tener en cuenta para su elección y evaluación.
- Comentar la evolución de los programas malignos en el último año y los pronósticos para el futuro inmediato.

Sumario:

- Introducción a los programas malignos.
- Definición y tipos de programas malignos.
- Técnicas empleadas por los virus.
- Antivirus. Mecanismos empleados en la detección de programas malignos.
- Productos antivirus. Aspectos a tener en cuenta para su selección y comparación.
- Evolución de los programas malignos en el 2006 y pronósticos para el 2007.

Tema 3: Calidad de información y programas malignos.

Objetivos del tema:

- Mediante el estudio de las características de los virus y formas de defensa contra ellos, los estudiantes comprendan la importancia del aprendizaje para prevenir daños en la información.

Unidad 6 (consta de un momento)

Tema: 1 Teleconferencia de Seguridad Informática.

Objetivos del tema:

- Que los cursistas profundicen los conocimientos adquiridos durante el curso en su autoaprendizaje de Seguridad Informática.

Cuando el facilitador de Seguridad Informática se va a enfrentar a un medio de enseñanza como este se hace necesario conocer primeramente qué opciones va a utilizar, hacia dónde va a dirigir la atención de los cursistas dentro del proceso, para de esta forma lograr una mejor utilización del medio de enseñanza.

Lo que conduce a un proceso de selección en dependencia de las categorías didácticas (objetivos, contenido y método a utilizar):

- Son el soporte material de éstas.
- Demuestra cómo utilizarlos, en el sentido de conocer su ambiente.
- Indica cómo navegar dentro de él.
- Muestra sus particularidades
- Señala en qué momento dentro del proceso debe utilizarlo.
- Revela para qué el estudiante puede usarlo y buscar información orientada por él.
- Contiene determinados ejercicios, dónde puede usarlo en el tema, en el trabajo independiente o en su estudio individual.

El sitio web se utilizará como un medio de enseñanza, teniendo en cuenta que en los resultados arrojados en el diagnóstico inicial en la Universidad de Guantánamo no cuenta con una bibliografía que sirva de material de estudio de la temática sobre Seguridad Informática.

2.3 Validación teórico - metodológica del sitio web para la contribución a la educación en Seguridad Informática.

Se sometió la web a criterios de quince especialistas en informática, los que corroboran los aspectos siguientes:

1. El sitio web muestra su alto grado de flexibilidad y adaptabilidad a las necesidades y características de los participantes que lo reciben.

2. Se logró la portabilidad del sitio web a distancia para memoria flash, como vía de facilitar su distribución y acceso a los sujetos.

3. Mostró un alto grado de aceptación por parte de los sujetos que estaban siendo preparados como profesores del curso.

4. Los contenidos abordados del sitio web mantuvieron su permanencia y solo fueron adaptadas las situaciones problémicas y los casos reales o hipotéticos que se presentan.

5. Se mantuvieron las aplicaciones y herramientas informáticas que se utilizan en el curso como medios de enseñanza y se incorporaron otras afines a las instituciones.

6. Se ajustaron algunos aspectos en las orientaciones metodológicas y de la evaluación.

7. Se actualizaron todos los planes referidos a la Seguridad Informática, con la participación de todo el personal, incluyendo los altos directivos.

Para la puesta en práctica de la web, se tendrá en cuenta el diagnóstico de la situación del personal de la Universidad de Guantánamo, así como y las experiencias obtenidas por entidades cubanas y foráneas en el desarrollo de entrenamientos, adiestramientos y capacitaciones desarrolladas sobre este tema.

Los módulos del sitio web están dirigido a dar respuesta a las demandas de la práctica actual de la Seguridad Informática en la Universidad de Guantánamo. Debe destacarse que diversas presentaciones han sido realizadas en reuniones de trabajo y talleres con los especialistas de informática en las facultades y CUM, los cuales han contribuido al perfeccionamiento de la propuesta.

Al procesar las consideraciones de los instrumentos aplicados en el estudio diagnóstico afloran las limitaciones siguientes:

(Anexos 1, 2,3 y 4)

1. Desconocimiento de las bases legales y éticas de la Seguridad Informática en Cuba.
2. No protegen la información contenida en su PC.
3. No protegen la información contenida en carpetas y archivos con copias de respaldo.
4. Las contraseñas utilizadas no cumplen con las características necesarias.
5. La infección por virus informáticos.
6. No conocen los procedimientos de cómo actuar al enfrentar un virus informático.
7. No conocen los procedimientos para actualizar la base de datos del antivirus.
8. No ejecutan el procedimiento para no recordar contraseña en los navegadores de Internet.
9. No utilizan procedimientos para proteger su pantalla y escritorio.
10. No reconocen cuáles son las amenazas a su sistema informático.
11. No saben el procedimiento que deben ejecutar al producirse un incidente de Seguridad Informática.
12. No conocen el plan de Seguridad Informática de la institución.
13. Los directivos y funcionarios no conocen sus responsabilidades y no se implican en los temas de Seguridad Informática.
14. Los directivos no incluyen en el sistema de trabajo de la institución el control a las actividades de la Seguridad Informática.

Debe señalarse que de los 38 usuarios a los que fue aplicado el instrumento, el 52,7% otorgó calificaciones de adecuado, el 27,1% de bastante adecuado y el 17,7% de muy adecuado, además el promedio general del puntaje de todos los ítem aplicados fue 3,60 con lo cual se considera como adecuada la web teórico metodológica de educación para la Seguridad Informática del personal de la UG. El 97,5% de los usuarios que participaron en la consulta, evaluaron entre adecuado y muy adecuado los ítems que fueron sometidos a su consideración, mostrando una notable aceptación, lo que demuestra validez y pertinencia de teórico-metodológica de web a nivel de los posibles facilitadores y cursistas en las facultades y CUM.

Regularidades generales resultantes de los criterios ofrecidos por los especialistas:

La propuesta del sitio web sometida a consideración de 11 especialistas de Informatización del Ministerio de Educación Superior, reconociendo su pertinencia para ser introducida en el reforzamiento de la educación del personal en Seguridad Informática, por cuanto la web ofrece las siguientes funcionalidades:

1. Es adaptable a la situación concreta de cada lugar.
2. Ofrece la bibliografía básica y complementaria para el acceso.
3. Cuenta con un conjunto de materiales elaborados como medios de enseñanza que facilita la comprensión de los contenidos.
4. Acceso a diversas variantes de casos reales o hipotéticos para ser analizados.
5. Brinda diversas variantes de la evaluación para ser aplicadas a los sujetos participantes.
6. Rigor de los contenidos que se abordan y su implementación educativa.

Conclusiones del capítulo II.

El empleo del sitio web propuesta para la educación en Seguridad Informática tanto en la autosuperación como en la forma presencial constituye una herramienta teórico metodológico para el perfeccionamiento de la gestión universitaria, para ello se diseña, emplea y valida un sitio web para la educación en Seguridad Informática.

CONCLUSIONES GENERALES

Las consideraciones ofrecidas en la investigación favorecen arribar a las conclusiones siguientes:

- La unidad de los fundamentos teóricos de la propuesta permite aprovechar las potencialidades del sitio web en el proceso de educación sobre Seguridad Informática, así como las potencialidades individuales, grupales y de la comunidad universitaria en el proceso de profesionalización de los técnicos de laboratorio y otros miembros de la comunidad universitaria en el fortalecimientos de valores compartidos en su desempeño profesional en los diferentes escenarios de la Universidad de Guantánamo.

- La efectividad teórico metodológica del sitio web sugerido se evidencia en el perfeccionamiento del proceso de educación en Seguridad Informática que parte de la concepción dialéctica de las categorías actividad, personalidad y grupo, así como del reconocimiento de las insuficiencias manifestadas, las que se mejoran mediante la implementación del curso virtual alojado en el sitio web como medio para el aprendizaje grupal e individual en las complejas condiciones de las transformaciones permanentes en la Universidad de Guantánamo.

- La usabilidad del sitio web en el proceso de educación de los técnicos de laboratorio de computación y otro personal en materia de Seguridad Informática están avalados por los resultados cuantitativos y cualitativos obtenidos, así como mediante la aplicación práctica de la experiencia y por el consenso mostrado por los criterios de los especialistas consultados, los que reconocen la factibilidad de la propuesta para otros escenarios de la Universidad de Guantánamo.

RECOMENDACIONES

Los resultados en la investigación permiten formular las siguientes recomendaciones:

1. Plantear a la dirección de la Universidad de Guantánamo que implemente este sitio web como medio de apoyo al sistema de preparación del personal técnico vinculado con la informatización para fortalecer la socialización, prevención, evaluación, aviso, investigación y respuesta a las acciones sobre Seguridad Informática, tanto interna como externa, que afecten el normal funcionamiento de las Tecnologías de la Información en las facultades y Centros Universitarios Municipales.
2. Que se conforme un proyecto institucional en la Universidad de Guantánamo con el propósito de contribuir al perfeccionamiento de la gestión educacional en los eslabones de base (colectivos, departamentos y facultades) sobre Seguridad Informática para la superación y el autodesarrollo de los técnicos de laboratorio y otro personal de apoyo al proceso docente educativo del Ministerio de Educación Superior.

BIBLIOGRAFÍA

1. Acevedo, J. (2003). Creencias sobre la tecnología y sus relaciones con la ciencia. Revista Electrónica de Enseñanza de las Ciencias Vol. 2 Nº 3 (2003). P.10.
2. Acuerdo 6058 CECM. (2007). Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información en Cuba. Comité Ejecutivo del Consejo de Ministros. Cuba, 2007 .
3. Addine, F. y García, G. (2004). Componentes del proceso de enseñanza aprendizaje. En Temas de introducción a la formación pedagógica. Editorial Pueblo y Educación. Cuba, p. 4:159.
4. Álvarez, C. (1996). "Una escuela para la Excelencia". Editorial Academia, La Habana.
5. Amoroso, Y. (1991). El Delito Informático. Conferencia Magistral Diplomado de Criminalística. La Habana. Cuba. 2002.
6. Área, M. y Guarro, .A. (2012). La alfabetización informacional y digital: fundamentos pedagógicos para la enseñanza y el aprendizaje competente. Revista Española de Documentación Científica, N. º Monográfico, p.46:74, 2012. ISSN: 0210-0614.
7. ArCERT, (2006). Manual de Seguridad en Redes. Coordinación de Emergencia en Redes y Telecomunicaciones. Administración Pública Argentina, 2006.
8. _____. (2007). Manual del instructor en seguridad de la información. Versión 1.0. Coordinación de Emergencia en Redes y Telecomunicaciones. Administración Pública Argentina, – Noviembre 2007.
9. Ávila, H (2006), Introducción a la metodología de la investigación, consultado en febrero de 2008, http://www.eumed.net/libros/2006c/203/2k.htm.
10. Baluja, W. (2006). Arquitectura y Sistema para la gestión de Seguridad de las redes de Telecomunicaciones. Tesis presentada en opción al grado científico de Doctor en Ciencias Técnicas, Instituto Superior Politécnico José Antonio Echeverría. La Habana, Cuba, 2006.
11. Bidot, J. (1999). La protección contra los virus informáticos. Experiencia en Cuba. Revista CID. Electrónica y proceso de datos en Cuba. La Habana. 1999. p. 37:41; pp13.

12. _____. (2009). Algunos aspectos de la Seguridad Informática en Cuba. Ponencia presentada en el IX Seminario Iberoamericano de Seguridad en las TIC. Evento Internacional Informática. Cuba, 2009.
13. Bermúdez L. y Lima, M., S. (2011). Metodología para la concepción de los cursos a distancia en línea de la MCE de amplio acceso diseñados actualmente de forma semipresencial. IPLAC. Cuba.
14. Bello, M., 2007. Tecnología de la Información y Comunicación: Competencias - Rol de los Profesores y Estudiantes. En J. Sánchez (Ed.): Nuevas Ideas en Informática Educativa. Volumen 3, p. 44:54, Santiago de Chile: LOM Ediciones.
15. Bermúdez, L. (2009). Algunas técnicas para la enseñanza y el aprendizaje en entornos virtuales. IPLAC. Cuba.
16. Bernaza, G. y Lee F. (2010). El aprendizaje colaborativo: una vía para la educación de posgrado. Material digital para la preparación del examen de mínimo de nuevas tecnologías en la educación para el doctorado en ciencias de la educación. MES, Consultado 2010.
17. Blogs.telnet, (2010). Computer Security theart, monitor and service, February 26, 1980. Reviised: April 15, 1980, consultado en febrero 2010 http://blogs.technet.com/ponicke/archive/2007/04/19/seguridadinformatica-un-poco-de-historia.aspx .
18. Bringas, J. (1999). “Propuesta de Modelo de Planificación Estratégica Universitaria” tesis presentada en opción al grado de Doctor en Ciencias Pedagógicas. Universidad de Ciencias Pedagógicas Enrique José Varona”.
19. Cano, M. (2001). Diseño y Aplicación de un Sistema Integral de Seguridad Informática para la UDLA. Tesis presentada en opción al título de Máster en Ciencias con Especialidad en Ingeniería en Sistemas Computacionales. Departamento de Ingeniería en Sistemas Computacionales, Escuela de Ingeniería, Universidad de las Américas, Puebla. Mayo.2001.
20. Caro, L. E. (2010). Estrategia de superación para el mejoramiento del Desempeño Profesional Pedagógico del Profesor General Integral de Secundaria Básica, en la utilización de la Informática en el proceso de enseñanza-aprendizaje. Tesis

presentada en opción al grado de Doctor en Ciencias Pedagógicas, UCP Rafael María de Mendive, 2010, p.24.

21. Cardona, G. (2009). Tendencias Educativas para el Siglo XXI. Magíster en Educación Universidad Javeriana, Candidato a PhD Ciencias Pedagógicas. Tomado de. Educación Virtual Online y @Learning. Elementos para la discusión; p3.
22. Cobo, R. (2005). Organización de la información y su impacto en la usabilidad. Facultad de Ciencias de la Comunicación de la Universidad Autónoma de Barcelona. Departamento de Comunicación Audiovisual y Publicidad. Ciudad de México, marzo de 2005.
23. Coello, J. L. (2006). La organización del proceso enseñanza-aprendizaje de la escritura con fines profesionales basado en una nueva concepción teórico-metodológica del enfoque y el método comunicativo. Resultados de la validación pedagógica. Universidad de Oriente. En www.umcc.cu/pu/2004/DFP_9_1_4.htm . (Consultado 24 de agosto 2010).
24. Colegio de Defensa Nacional CODEN (2011). La Seguridad Nacional ante los retos de las Nuevas Tecnologías de la Información. Compilación. Cuba.
25. Colectivo de autores. (2006). Los detectives y la prevención de la criminalidad informática. Editora Política. La Habana. Cuba, 2006.
26. Collazo, R. (2004). Una Concepción teórico metodológica para la producción de cursos a distancia basados en el uso de las Tecnologías de la Información y las Comunicaciones. Tesis doctoral presentada en opción al título de Doctor en Ciencias de la Educación. Instituto Superior Politécnico José Antonio Echeverría Centro de Referencia para la Educación de Avanzada. Cuba, 2004. p. 38:78.
27. Contraloría General de la República. (2011). Resolución No. 60/2011 de la Contraloría General de la República de Cuba.
28. Consejo de Estado. (1999). Decreto ley 199/1999 del sobre la seguridad y protección de la información oficial. Material digital. p.2.
29. Curbelo, M. (2003). Sistema analizador de log para la detección de intrusos. Tesis presentada en opción al título de ingeniero en Informático en el Instituto Superior Politécnico José Antonio Echeverría. La Habana, Cuba, 2003.

30. CMSI, (2003). Cumbre Mundial de la Sociedad de la Información, Ginebra, Suiza. (2003). Consultado en febrero 2009 en http://www.oei.es/revistactsi/numero6/documentos01.htm,
31. _____. (2005). Cumbre Mundial de la Sociedad de la Información, Túnez. Consultado en diciembre 2009 en http://www.itu.int/wsis/implementation/index-es.htm,
32. Díaz, G. (2006). Concepción teórico-metodológica para el uso de la computadora en el proceso de enseñanza aprendizaje de la educación primaria. Tesis presentada en opción al grado científico de Doctor en Ciencias Pedagógicas, Instituto Superior Pedagógico "Enrique José Varona", Ciudad de La Habana.
33. Díaz, A. (2006). Metodología para la creación de páginas web docentes. ISP Félix Varela, Santa Clara, Villa Clara, Cuba, Tesis doctoral. Tesis presentada en opción al título científico de Doctor en Ciencias Pedagógicas, Santa Clara, p.26:40.
34. Dolón, A. (2006). Aplicación de la Seguridad Integral en las Empresas de región de Murcia. Tesis presentada en opción al grado científico de Doctor en Ciencias Técnicas. Universidad Politécnica de Cartagena, España.
35. Eduardo, J. (2010). La importancia de la Seguridad Informática. Material publicado en UBA y en la Universidad Nacional del Comahue (UNCO), 2010. Consultado en http://www.suite101.net/content/laimportancia-de-la-seguridad-informtica-a21644, enero del 2011.
36. Espinosa, M. P. y Pinzón, F. (2007). Identificación de vulnerabilidades, análisis forense y atención a incidentes de seguridad en los servidores de la UTPL. Universidad Católica de Loja, 2007.
37. Fabelo, J. (1989). Práctica, conocimiento y valoración. La Habana, Cuba: Editorial Ciencias Sociales; 1989, p.18:19.
38. Febles, J. (2012). Curso de Seguridad Informática. Consultado en septiembre 2012 en www.slideshare.net/jpfebles1/tema
39. Fernández, G., Ana M. y otros (2001). Comunicación Educativa. Editorial Pueblo y Educación. La Habana. Cuba.
40. _____. (2004). Aprender a comunicarnos y comunicarnos para aprender. (“learning to communicate and communicate to learn”).

41. Fernández, F. (2012a). Entornos virtuales de aprendizaje en La web 2.0 Y 3.0, p.4. consultado septiembre 2012. Material digital. Revista IPLAC, p. 6.
42. Fuentes, S. (2005). Defiende tu PC Guía de seguridad para ordenadores personales. Barcelona. España, consultado en febrero 2010 en http://www.defiendetupc.com
43. Garnier, J. C. (2006) La información y su papel en la Seguridad Nacional de la Información. La Habana. Cuba. Material digital.
44. García, K. (2008). Factor humano en la seguridad de la información, Ponencia presentada en el evento nacional de Seguridad Informática. Segurmática-MIC, Cuba, 2008. Material digital.
45. Pierrat, G. (2007). Retos de las nuevas tecnologías. Un mundo diferente. Ponencia. En formato digital. Oficina de Seguridad para las Redes Informáticas. La Habana. Cuba. 2007.
46. García, A. y Galicia, S. (2012). Ocho metodologías relacionadas con el arte y la ciencia de enseñar. Curso 8. Congreso internacional Universidad 2012. Material digital, p.12.
47. González, V. (1999). Conferencia impartida en el curso de Maestría en Ciencias de la Educación. Centro de Estudio para el Perfeccionamiento de la Educación Superior. Universidad de La Habana.
48. González, P. (2000). Discurso inaugural del Evento Internacional Informática (2000). Material digital. Consultado en mayo 2010, p.2.
49. González, M., López, J. y. Luján, J., 1996. Ciencia, tecnología y sociedad. Una introducción al estudio social de la ciencia y la tecnología. Tecnos, Madrid, p.130.
50. Globalmedia, (2012). Tecnología emergente para seguridad. Consultado en septiembre 2012 en http://www.globalmedia-it.com/index.php/analysis/47548-Tecnologa-emergente-para-seguridad.html.
51. Gisbert, M y González, A., 1996. Las nuevas tecnologías en la educación. Las nuevas tecnologías en la educación', en Salinas: 'Redes de comunicación, redes de aprendizaje',

52. Helios, C. (2008). Origen de los problemas de Seguridad Informática. Departamento de Seguridad Informática. Instituto de Investigación y Desarrollo de Ingeniería de Software Universidad Autónoma de Guadalajara, p.35.
53. Hernández, L. (2011). Seguridad Informática: Estado Actual en México y en el Mundo. Presentación publicada en Laboratorio de Seguridad Informática. Centro Tecnológico, FES- Aragón. UNAM, XIX Aniversario. FI Culiacán, UAS, septiembre 2011.
54. Herrera, E. (2005). Concepción teórico-metodológica desarrolladora del diseño didáctico de cursos para la superación a distancia de profesores en ambientes virtuales de enseñanza-aprendizaje. Tesis presentada en opción al grado científico de Doctor en Ciencias Pedagógicas, Instituto Superior Pedagógico E. J. Varona. Ciudad Habana, p 76:77.
55. _____. (2012b). Perspectivas tecnológicas: educación superior en Iberoamérica 20122017. The New Media Consortium, eLearn Center Universitat Oberta de Catalunya. ISBN 978-09846601-9-3. p.16:20.
56. Lee, F. (2003). Estrategia Maestra de Informatización del Ministerio de Educación Superior para los cursos 2003-2007. Material digital, Ministerio de Educación Superior de Cuba.
57. Leblanch, I. (2012). Página Web Educativo para desarrollar una cultura en Seguridad Informática en los Institutos Politécnicos de Informática de la Educación Técnica y Profesional. Tesis de maestría presentada en el IPLAC, Cuba, p.50.
58. Ilich, Vladimir Lenin. (1964). Cuadernos Filosóficos. Obras Completas. La Habana 1964.
59. _____. (1973). Materialismo y Empirocriticismo. (Pág. 139-145). Ed. Progreso.--Moscú,
60. Lima, S. y otros (2003). Transformaciones para lograr un aprendizaje desarrollador de la computación en el nivel medio. Informática 2003, ISBN 959237095-8.
61. Lima, S. (2005). La mediación pedagógica con uso de las tecnologías de la información y las comunicaciones (TIC). Curso del Congreso Pedagogía 2005, Palacio de Convenciones, La Habana, Cuba, ISBN: 959-18-0077-0, p.7:13.

62. Lizama, J, y Farías, M. (2003). Analfabetismo digital y sus implicaciones en la Seguridad Informática. Artículo publicado por la Facultad de Ciencias Políticas, Universidad Nacional Autónoma de México, 2003.
63. López, J. A. (2010). Entrenamiento en Seguridad Informática. Entrenamiento de Empresa del Consultora DISAIC del Ministerio de la Industria Sidero-mecánica. Cuba, abril 2010. Consultad en Consultado y tomado de http://www.disaic.cu/modules.php?name=Services&type_id=1, mayo 2009.
64. López, M. (2009). Elaboración de Planes de Seguridad Informática. Adiestramiento de la empresa Segurmática. Ministerio de la Informática y las Comunicaciones, mayo 2009.
65. López, S et al. (2006). Por un enfoque social en el concepto de nuevas tecnologías de la informática y la comunicación, Revista Pedagogía Universitaria, Vol. XI, no. 4, La Habana, Cuba, p.101.
66. López, A. 2001. ¿Son un peligro las NTIC? Problemas socioeconómicos, políticos, culturales y éticos, consultados en septiembre 2009 en http://contexto-educativo.com.ar/2001/5/nota-10.htm.
67. Martínez, F. (2003). El profesorado ante las nuevas tecnologías. Medios y herramientas de comunicación para la educación universitaria. Editorial Sucesos Publicidad. Ciudad de Panamá.: 2003. p. 213.
68. Martínez, E. (2011). Una nueva convergencia tecnológica cambiará a la sociedad en el 2020. Consultado en http://www.tendencias21.net/Una-nueva-convergencia-tecnologica-cambiara-a-lasociedad-en-2020_a1171.html, mayo 2011.
69. Manunta, G. (2004). Seguridad una Introducción. Consultado en http://www.seguridadcorporativa.org, 2004, p.10.
70. MES, (1998). Política Nacional de Informática del Ministerio de Educación Superior. Material digital.
71. _____. (2004). Resolución 132/2004. Reglamento de la Educación de Posgrado de la República de Cuba. Ciudad de La Habana, material digital.

72. _____. (2009). Normas y Procedimientos para la Gestión del Posgrado. Anexo del Reglamento de la Educación de Posgrado de la República de Cuba. Ciudad de La Habana, material digital.
73. MES, (2001). Resolución 18/2001 del MES. Perfil de Técnico medio en Informática. Cuba, MES, 2001.
74. _____. (2007). Resolución 176/07 del MES. Reglamento de Seguridad Informática en la Actividad Educacional del Ministerio de Educación, Cuba, MES, 2007.
75. MINREX, (2005). Cuba: hacia una sociedad de la información justa, equitativa y solidaria. Informe de Cuba a la primera fase de la cumbre de la sociedad de la información en Túnez. Consultado el 6 de abril de 2007, desde http://www.cubaminrex.cu/Sociedad_Informacion/Cuba_SI/Cuba_SI.htm
76. MININT, (1996). Resoluciones 6/96 del Ministerio del Interior. Reglamento sobre la Seguridad Informática. Cuba junio 1996.
77. MTSS, (2006). Resolución 188/2006 del Ministerio del Trabajo y Seguridad Social sobre los Reglamentos Disciplinarios Internos del 21 de agosto de 2006, Cuba, 2006.
78. Montesino, R. (2009). Gestión de la Seguridad Informática: de la Teoría a la Práctica. Ponencia presentada en el evento Internacional Informática 2009. Material digital.
79. Montenegro, H. (2006). Un conocimiento básico de seguridad debería ser parte sustancial de la formación de cualquier profesional informático. Consultado y tomado de Tribuna de Opinión suplemento del nº 3, mayo / junio 2006.
80. Moro, J. C. (2009). Seguridad en las Tecnologías de la Información. Adiestramiento de la Empresa Segurmática del Ministerio de la Informática y las Comunicaciones, mayo 2009.
81. Muñoz, I. (2004). Aspectos Legales y Éticos de la Seguridad Informática. Una reflexión local y global. Consultora externa de la Dirección General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública de México que anualmente publica el Electronic Privacy Information Center.

82. Oficina de Seguridad para las Redes Informáticas de Cuba. OSRI (2008a). Metodología para el diseño de un sistema de Seguridad Informática. Cuba.
83. ONU. (2005). Prevención al delito y Justicia penal. XI Congreso sobre la prevención al delito y justicia penal promulga declaración final, consultado diciembre 2008 en http://www.cinu.org.mx/11congreso/UN/prensa.htm, p.2.
84. Parets, G. (2009). Sistema de Gestión de la Seguridad de la Información desde la óptica de las normas ISO/IEC 27000. Ponencia presentada en el evento Nacional de Seguridad Informática Cuba. Segurmática-MIC. Noviembre 2009.
85. Rodríguez Cuervo, Alejandro Miguel. (2012) .Una concepción teórico-metodológica para la educación en Seguridad Informática del personal de las instituciones del Ministerio de Educación. Tesis en opción al grado científico de doctor en Ciencias de la Educación. IPLAC. La Habana.

Anexo 1

Guía para el análisis de las fuentes documentales

Objetivo: Constatar las fuentes de que disponen los técnicos de laboratorio de la Universidad de Guantánamo para su preparación en temas de Seguridad Informática en su actividad profesional

Documento: _____

1. Si tiene información vinculada a los temas de Seguridad Informática en su actividad profesional.

2. Claridad de la información y precisión de las orientaciones.

3. ¿Cómo contribuye a la orientación del personal respecto al uso de las vías, métodos y procedimientos asociados a la Seguridad Informática?

Anexo 2

Entrevista al personal de las facultades y CUMS

Estimado (a) colega:

Necesitamos su colaboración en una investigación encaminada a diseñar un sitio web para la educación en Seguridad Informática. Para ello es imprescindible su participación en el intercambio que se desarrollará a continuación. Le agradecemos sus criterios sinceros.

Preguntas para el intercambio:

1. ¿Consideran que es necesaria la educación en Seguridad Informática para el personal de las instituciones del MES?

2. ¿Consideran que la introducción de la educación en Seguridad Informática contribuye a estimular la motivación y aprendizajes reflexivos y significativos?

3. ¿Son suficientes las orientaciones que aparecen en los documentos y resoluciones emitidos por el MES sobre esta temática, programas y orientaciones metodológicas y libros de texto o de consulta para desarrollar la preparación en Seguridad Informática?

4. ¿Se orientan actividades en su institución referidas a la Seguridad Informática a través de la realización de actividades de búsqueda de información, valoración ética, de aplicación en la práctica en la solución de problemas de contenido de Seguridad Informática?

5. ¿Son suficientes las orientaciones y preparación recibida sobre Seguridad Informática en los cursos de informática orientados por el MES?

6. ¿Es adecuada su educación para configurar y utilizar de manera más segura las aplicaciones y herramientas informáticas utilizadas en sus actividades profesionales?

7. ¿Qué impacto han tenido estas actividades en su Facultad o CUM?

Anexo 3

Guía de observación del desempeño profesional en Seguridad Informática de los técnicos de laboratorio dela Universidad de Guantánamo.

Objetivo: Evaluar el desempeño en Seguridad Informática de los técnicos de laboratorio al configurar e interactuar con las aplicaciones y herramientas informáticas.

Se otorgarán las categorías Inadecuado (I), Poco adecuado (PA), Adecuado (A), Bastante adecuado (BA) y muy adecuado (MA), los que muestren pleno dominio y conocimiento del procedimiento se les otorga la categoría de Muy Adecuado. Los que muestren dominio del procedimiento; pero solo lo completan parcialmente se les otorga la categoría de Bastante adecuado. Los que muestren un dominio del procedimiento y no logran completarlo alcanzará la categoría de Adecuado, los que dominan parcialmente el procedimiento y no logran completarlo se les otorga la categoría de Poco adecuado y los que no dominan el procedimiento y no logran completarlo se les otorga la categoría de Inadecuado.

Cada categoría será evaluada según la escala

5 Muy Adecuado, 4 Bastante Adecuado, 3 Adecuado, 2 Poco Adecuado, 1 Inadecuado.

No	Ítem	I	PA	A	BA	MA
1	Conoce el procedimiento para conformar las claves de acceso, su utilización y resguardo.					
2	Conoce los procedimientos para configurar y utilizar de forma más segura el correo electrónico y el navegador de Internet que utiliza en su institución para el intercambio y la búsqueda de información.					
3	Conoce el procedimiento para identificar y actuar ante un incidente de Seguridad Informática.					
4	Reconoce y domina los procedimientos para proteger la información contenida en carpetas o archivos, el escritorio de la computadora y el uso de dispositivos externos.					
5	Reconoce los procedimientos que realizan un antivirus, su instalación, configuración y actualización.					
6	Domina el procedimiento para configurar y utilizar de forma más segura las aplicaciones ofimáticas.					
7	Domina el procedimiento para actuar ante la infección por un virus informático					
8	Domina el procedimiento para configurar de forma segura el Sistemas Operativos que utiliza.					

Anexo 4

Encuesta en Seguridad Informática del personal de la comunidad universitaria

Estimado colega, necesitamos su colaboración en una investigación encaminada a diseñar una Web para contribuir a la educación en Seguridad Informática. Para ello es imprescindible su participación en el intercambio que se desarrollará a continuación. Le agradecemos sus criterios sinceros.

No	Ítem	SI	NO
1	Conoce el procedimiento para conformar las claves de acceso, su utilización y resguardo. En caso afirmativo menciones dos:		
2	Conoce los procedimientos para configurar y utilizar de forma más segura el correo electrónico y el navegador de Internet que utiliza en su institución para el intercambio y la búsqueda de información. En caso afirmativo menciones dos:		
3	Conoce el procedimiento para identificar y actuar ante un incidente de Seguridad Informática. En caso afirmativo menciones dos:		
4	Reconoce y domina los procedimientos para proteger la información contenida en carpetas o archivos, el escritorio de la computadora y el uso de dispositivos externos. En caso afirmativo menciones dos:		
5	Reconoce los procedimientos que realizan un antivirus, su instalación, configuración y actualización. En caso afirmativo menciones dos:		
6	Domina el procedimiento para configurar y utilizar de forma más segura las aplicaciones ofimáticas. En caso afirmativo menciones dos:		

7	Domina el procedimiento para actuar ante la infección por un virus informático En caso afirmativo menciones dos:		
8	Domina el procedimiento para configurar de forma segura el Sistemas Operativos que utiliza. En caso afirmativo menciones dos:		