Universidad de Guantánamo

CENTRO DE ESTUDIOS DE EDUCACIÓN

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

Alternativa metodológica B-learning para la preparación en seguridad Informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"

AUTOR: Lic. Esteban Fernández Sánchez

Guantánamo, 2015

CENTRO DE ESTUDIOS DE EDUCACIÓN

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

Alternativa metodológica B-learning para la preparación en seguridad Informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"

AUTOR: Lic. Esteban Fernández Sánchez

TUTOR: Dr. C. Alfredo Cabrera Hechavarría

Guantánamo, 2015

DEDICATORIA

A mi hija y a mi esposa.

A mi madre donde quiera que esté.

A todos los amigos por su apoyo y comprensión.

AGRADECIMIENTOS

A mi hija Elizabeth, fuente de mi inspiración.

A mi esposa Yoanna, por su paciencia y apoyo incondicional.

A mi padre y a mi tía Cachita por sus consejos, ayuda y comprensión en los momentos difíciles.

A mi tutor, Alfredo Cabrera Hechavarría y al consultante Andrés Ballester Gouraige, por su dedicación y asesoramiento consecuente.

A todos los profesores de la maestría, mi infinito agradecimiento.

RESUMEN

En la introducción e implementación de las Tecnologías de la Información y las Comunicaciones en el sistema educativo cubano ha sido decisiva la preparación del docente, no sólo para el logro de las metas propuestas, sino también para llevar a cabo la conservación y seguridad tanto de la información como de las tecnologías existentes en función de hacer un uso ético y responsable de las mismas lo que demanda poseer una cultura básica en materia de seguridad informática.

Desde este contexto, en la presente tesis se propone una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", dicha alternativa fue elaborada tomando como premisa el modelo Pedagógico Profesional de la Educación Técnica y Profesional en Cuba desde donde se determina el modo de actuación del docente que se desempeña desde estas condiciones. En ella se ofrece la estructuración de los contenidos para la preparación en seguridad informática del docente de forma presencial y a distancia con el empleo de Entornos Virtuales de Enseñanza Aprendizaje.

La forma en que se proyecta la alternativa contribuye a la búsqueda de nuevos conocimientos en materia de seguridad informática, de una forma colaborativa y reflexiva, incluyendo en este accionar a los demás factores responsables de la dirección del proceso pedagógico profesional desde la entidad educativa anteriormente mencionada.

La factibilidad de la propuesta fue evaluada por un grupo de especialistas, los cuales corroboraron que es viable y aplicable en correspondencia con los fines que guiaron su elaboración.

ABSTRACT

In the introduction and uses of the Information and Communication Technologies in the Cuban Educational System, it has been decisive the teachers´ preparation; not only to achieve the expected goals but also to carry out the maintenance and security of the information and the existing technologies, in order to use them in an ethical and responsible way, that's why teachers should have a basic culture about informatic security.

From this context, in this research it is proposed a B-Learning methodological alternative to guide the teachers from polytechnic "Julio Antonio Delgado Reyes" to be prepared on informatic security. This alternative was made taking into account the Pedagogical Professional Model of the Technical and Professional Education in Cuba, what determines the behaviour of the teachers who work in this context. All these determined a new structure of the contents to accomplish with the teachers´ preparation on informatic security in two ways of teaching: by traditional and online lessons with the use of teaching – learning virtual aids.

This alternative contributes to the searching of new knowledge about informatic security in a collaborative and reflexive way including the other responsible leaders of the Professional Pedagogical Process from the school mentioned before.

The effectiveness of the proposal was evaluated by a group of specialists who corroborated it as effectual and appropriate in correspondence with the goals that led its elaboration.

INTRODUCCIÓN

En la actualidad, el desarrollo experimentado por las diferentes ramas de la ciencia, la técnica y la tecnología ha provocado considerables cambios en la vida social, económica, política y cultural caracterizada por el crecimiento acelerado de la información científica generadora de avances importantes en el campo de las Tecnologías de la Información y las Comunicaciones (TIC).

Ante estas circunstancias, la humanidad se enfrenta al uso de las TIC en un escenario cada vez más complejo, donde la paz y la seguridad del planeta se encuentran constantemente en peligro, en medio de políticas neoliberales y el desarrollo de megaproyectos de espionaje, basados en una ciberguerra impuesta por las grandes potencias capitalistas del mundo, las cuales han tratado de establecer un patrón único donde impere el desconocimiento de las potencialidades y la cultura de los pueblos (Hurtado, F. 2007; Martínez, J. 2012).

Precisamente en este contexto, la introducción de las TIC en Cuba ha estado mediatizada por la implementación del Programa de Informatización de la Sociedad Cubana, cuya finalidad es satisfacer la creciente demanda de información y conocimientos en todas las esferas de sociedad así como elevar los niveles de eficiencia y eficacia tanto en los servicios como en los procesos productivos que se generan, siempre con el apoyo de estrategias de seguridad que garanticen la continuidad y el acceso a las mismas.

Por lo tanto, la seguridad de la información y por ende de las Tecnologías Informáticas (TI), constituyen un tema de vital importancia pues a medida que aumenta el desarrollo de las TIC, aumenta el número de riesgos asociados a las constantes amenazas a los sistemas informáticos, provocando entre otras cuestiones: la pérdida de información, la denegación de servicios y a las fuentes de información, el incremento tanto de virus informáticos como de herramientas de ciberespionaje y la puesta en marcha de actividades subversivas.

En correspondencia, autores como Sosa, M., Vialart, N. y Vidal, M. (2012), plantean que con el creciente desarrollo de las TIC y el aumento de la conectividad, los sistemas de información y las redes informáticas son cada vez más vulnerables y están expuestos a un número mayor de amenazas. Ello posibilita el surgimiento de la nueva sociedad de la información la cual necesita alcanzar mayor conciencia y entendimiento en materia de seguridad.

Por su parte, Cáceres, J. A. (2012), en su libro titulado “Virus Informáticos”, enfatiza que a diario se reciben reportes de ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados, las computadoras se vuelven inoperables, se ha copiado información confidencial sin autorización, se ha remplazado el software para agregar puertas traseras de entrada, y miles de contraseñas se han descifrado.

En este mismo sentido, Bidot, J. (2012: 21), director de la empresa cubana "Segurmática", en el informe titulado "Escenario de la seguridad informática en los inicios del año 2013" expresó:

(…) "*el escenario de la seguridad informática es el más complejo de los vividos y ni la industria de las tecnologías informáticas, ni los usuarios, ni los gobiernos están preparados para enfrentarlo de forma proactiva, es por tanto una asignatura pendiente a nivel internacional que urge resolver*".

Sobre esta misma idea, Rodríguez, A. M. (2011: 4), director de Informática Educativa del MINED, al realizar un análisis sobre la situación relacionada con los usuarios de las TIC y la seguridad informática, destacó:

- ✓ *Los usuarios conocen muy poco sobre los distintos tipos de incidentes de seguridad informática que pueden presentarse y el impacto que de ello se deriva, considerando además, que sus sistemas informáticos están bien protegidos y no están expuesto a ningún riesgo.*

- ✓ *Se subestiman las soluciones técnicas minimizando las educativas y preventivas, de ahí, que a pesar de los esfuerzos realizados en el ordenamiento legal de las TI, el usuario final continúe desprotegido, desorientado y no prevenido, aspecto aún no resuelto y con posibilidades de su incremento*.

Con las reflexiones antes expuestas, se puede apreciar que en la sociedad contemporánea, no sólo basta que los usuarios sepan utilizar adecuadamente las TIC, sino que deben estar de igual forma bien preparados para instrumentar procedimientos y técnicas de seguridad informática que permitan salvaguardar la información y los sistemas informáticos empleados en su creación.

De ahí que la preparación de los recursos humanos en materia de seguridad informática sea primordial para garantizar la integridad, disponibilidad y confidencialidad de la información que se procese, almacene o transmita empleando este tipo de tecnología.

Todo lo expuesto motivó el interés del autor, de este trabajo, en buscar propuestas relacionadas con la problemática que se investiga, dirigida especialmente al ámbito del sistema educativo cubano, donde se ha venido implementando en todos los tipos y niveles de enseñanza las llamadas TIC, convirtiéndose en importantes medios de apoyo de maestros y profesores en la formación de las presentes y futuras generaciones.

Como parte de la sistematización realizada, se pudo constatar la existencia de consideraciones efectuadas por varios autores, desde lo internacional (Borghello, C. F. 2001; Bisogno, M. V. 2004; Mayol, R. N. 2006; Monzón, C. J. 2009) y en el orden nacional (Ramírez, S. 2008; de los Ángeles, N. 2010; Peñalver, N. 2010; Hernández, L. 2012; Valdés, M. 2012; Rodríguez, A. M. 2012), todos ellos, desde diferentes perspectivas, abordan el tema de la preparación en seguridad informática dirigida a profesionales de la especialidad informática, dígase: responsables de seguridad informática, administradores de red, Web Máster entre otros. Estos estudios han sido realizados

debido al limitado tratamiento de contenidos en seguridad informática desde la disciplina principal integradora planificada para la formación inicial de estos profesionales.

Esta problemática, no sólo se manifiesta en la formación inicial del técnico medio y licenciados en Educación especialidad Informática desde las instituciones del Ministerio de Educación (MINED), sino en mayor o menor medida se presenta en la formación de ingenieros en informática, es por ello que desde el año 2008 se han venido desarrollando cursos de preparación por los especialistas de la empresa cubana "Desoft" pertenecientes al Ministerio de la Informática y las Comunicaciones.

De manera predominante, estas propuestas de preparación en seguridad informática, se han orientado al análisis de la legislación vigente, la clasificación de virus informáticos, la instalación y configuración de programas antivirus, la aplicación del código de ética, el estudio de las metodologías a tener en cuenta en la elaboración del plan de seguridad informática y plan de contingencias, las técnicas para la salva de la información y la implementación de herramientas para el control de esta actividad en la red telemática.

Es importante destacar que los estudios realizados permiten encauzar en alternativas para dar solución a esta problemática, sin embargo, la sistematización efectuada por el autor de esta investigación ha permitido profundizar en determinados contenidos que a pesar de su importancia se han dejado de tratar.

Tal es el caso de la determinación de los riesgos y vulnerabilidades relacionados con la obtención de información confidencial a través de las llamadas técnicas de ingeniería social, la participación de los usuarios en las redes sociales de comunicación, la protección de las TIC a partir de la puesta en marcha de los sistemas de tierra física, de alarma contra incendios y contra intrusos, la elaboración de proyectos de redes informáticas en correspondencia con el sistema de seguridad a implementar, las medidas a tener en cuenta en la explotación de equipos móviles de cómputo desde las instituciones educativas, las técnicas para la protección de información contenida no sólo en soportes digitales sino también en soportes impresos.

A partir las carencias antes mencionadas, fue necesaria, la realización de una exploración relacionada con la preparación en seguridad informática de los docentes que laboran en el Politécnico "Julio Antonio Delgado Reyes", tomando como premisas: la observación, el análisis de seminarios nacionales de preparación para docentes, así como el intercambio de ideas con directivos de las Direcciones Municipales y Provinciales de Educación de Guantánamo, lo que posibilitó llegar a las siguientes insuficiencias:

- Es limitado el número de actividades de preparación planificadas y desarrolladas en materia de seguridad informática; las que se realizan se centran únicamente en el análisis superficial de determinadas resoluciones, abordándose aspectos de carácter teórico vinculados con el qué hacer y no con el cómo hacer, excluyéndose

algunos elementos atendiendo a lo tecnológico, organizativo, educativo e ideológico. Todo ello obstaculiza el tratamiento de estos contenidos desde la formación inicial del futuro técnico medio y obrero calificado en esta entidad educativa.

- De igual manera, es insuficiente el dominio del lenguaje técnico relacionado con la seguridad de las TIC, lo cual causa incomprensión sobre la legislación vigente y de los procedimientos incorporados a esta actividad.

- Por demás, existe carencia en los aspectos a tener en cuenta para la conservación, protección y seguridad de las TIC, unido a la limitada cultura archivística provocando afectaciones a la información disponible en fuentes digitales e impresas y al desarrollo del propio proceso pedagógico profesional.

- Por ende, es escaso el número de bibliografía referida a la seguridad informática, las que se poseen presentan una lectura secuencial que restringe el nivel de interactividad y dificulta el proceso de actividad y comunicación según el nivel de preparación y necesidades de los usuarios.

Por otro lado el autor, en su búsqueda y revisión bibliográficas, no ha podido hallar propuestas de preparación en seguridad informática que desde la Educación Técnica y Profesional (ETP) posibiliten su generalización y la adecuación sistemática de los contenidos para ser utilizados desde otros contextos y en condiciones concretas.

Tampoco ha encontrado otras que permitan implementar un sistema de seguridad informática para el uso eficiente y seguro de las TIC en los centros educacionales cubanos, para garantizar la preparación sistemática de los docentes en correspondencia con las exigencias sociales y el continuo desarrollo experimentado por la ciencia y la técnica en sentido general.

Tales condiciones, no posibilitan la realización de ejercicios, situaciones de aprendizaje y metas cuya consecución facilite la apropiación de conocimientos y el desarrollo de hábitos y habilidades.

A estas limitaciones se une el nivel de operatividad alcanzado en el desarrollo del proceso pedagógico profesional desde las escuelas politécnicas, lo que impide movilizar a una gran cantidad de personas para llevar a cabo acciones de preparación referidas a la problemática investigada.

De ahí la necesidad de utilizar nuevas formas de preparación atemperada a las condiciones históricas actuales que garanticen una eficiente profesionalización de este personal de la educación en materia de seguridad informática.

En consecuencia puede considerarse como **problema científico**: ¿Cómo perfeccionar la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”?

El **objeto de investigación** lo constituye el proceso de preparación en seguridad informática de los docentes de las instituciones educativas.

El **campo de acción** se enmarca en la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes".

Para dar cumplimiento a las expectativas del problema, se plantea el siguiente **objetivo de investigación**: elaborar una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes".

A partir del objetivo planteado, se proyectaron las siguientes **preguntas científicas**:

1. ¿Cuáles son los antecedentes históricos del desarrollo de la seguridad informática en Cuba y su contextualización en la preparación de docentes?

2. ¿Qué referentes teóricos y metodológicos sustentan la preparación en seguridad informática de los docentes en Cuba y a nivel internacional?

3. ¿Cuál es el estado actual de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"?

4. ¿Qué características debe poseer una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"?

5. ¿Qué factibilidad tendrá la alternativa metodológica B-learning elaborada para dar solución al problema planteado en la investigación?

Para dar respuesta a las preguntas científicas y cumplimiento al objetivo de investigación se formularon las siguientes **tareas de investigación**:

1. Caracterización de los antecedentes históricos del desarrollo de la seguridad informática en Cuba y su contextualización en la preparación de docentes.

2. Sistematización de los referentes teóricos y metodológicos que sustentan la preparación en seguridad informática de los docentes en Cuba y a nivel internacional.

3. Diagnóstico del estado actual de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes".

4. Elaboración de una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes".

5. Valoración de la factibilidad de la alternativa metodológica B-learning elaborada para dar solución al problema planteado en la investigación.

Para el desarrollo de las tareas científicas, se planificaron los siguientes **métodos de investigación**:

DEL NIVEL TEÓRICO:

- **Histórico y lógico**: para analizar la evolución histórica del desarrollo de la seguridad informática en Cuba y su contextualización en la preparación de docentes.
- **Enfoque sistémico**: para determinar los elementos estructurales de la alternativa metodológica B-learning propuesta como vía de solución al problema de esta investigación.
- **Inducción-deducción**: para determinar los contenidos fundamentales a incluir en la preparación en seguridad informática, así como para la elaboración de la alternativa metodológica B-learning que constituye la propuesta de solución al problema científico planteado, y así facilitar el arribo a conclusiones parciales y totales en el trabajo.
- **Análisis y síntesis**: para analizar las diferentes concepciones teóricas y metodológicas relacionadas con la investigación dirigida a la preparación en seguridad informática de docentes y conformar el marco teórico en que se sustenta la investigación.
- **Modelación**: para analizar las relaciones tanto internas como externas que se establecen entre los elementos que integran la alternativa metodológica B-learning propuesta para la preparación en seguridad informática de docentes y así dar solución al problema planteado en esta investigación.

DEL NIVEL EMPÍRICO:

- **Entrevistas**: dirigidas a los docentes del Politécnico "Julio Antonio Delgado Reyes", con la finalidad de obtener sus criterios relacionados con la preparación recibida en relación con la seguridad informática.
- **Encuestas**: para diagnosticar el nivel de preparación en seguridad informática alcanzado por los docentes del Politécnico "Julio Antonio Delgado Reyes".
- **Estudio documental**: para analizar diferentes documentos relacionados con la preparación en seguridad informática, tales como: resoluciones, leyes, informes, planes, estrategias o seminarios de preparación o superación de docentes.
- **Prueba pedagógica (de desempeño)**: se empleará en la etapa del diagnóstico con la finalidad de evaluar el nivel de preparación en seguridad informática alcanzado por los docentes del Politécnico "Julio Antonio Delgado Reyes".

- **Criterio de especialistas**: para ser aplicado a especialistas nacionales, con el objetivo de evaluar el grado de aceptación de la alternativa metodológica B-learning propuesta para dar solución al problema de investigación y posibilitar su constante perfeccionamiento.

DEL NIVEL MATEMÁTICO y ESTADÍSTICO:

- **Análisis porcentual**: para cuantificar el resultado de los instrumentos aplicados en el estudio del problema y la valoración de la factibilidad de la propuesta.

- **Tablas y gráficos**: para tabular y graficar los datos obtenidos durante el proceso de investigación y así lograr mayor comprensión de las ideas que se pretenden expresar.

Población y muestra:

Para realizar el diagnóstico de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", se seleccionó como población a los 112 docentes que laboran en el Politécnico antes mencionado. De ellos, 103 son Licenciados en Educación que realizan diversas funciones y 11 se desempeñan como docentes habilitados. De esta población, se escogió intencionalmente una muestra de 41 docentes, representada por 30 Licenciados en Educación y 11 habilitados los que representan un 36.6 % del total de la población.

NOVEDAD CIENTÍFICA: se sustenta, en la propia naturaleza de la alternativa metodológica B-learning propuesta, que desde un enfoque pedagógico y sistémico garantice la organización, estructuración de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", atendiendo a las TIC existentes y a las características del proceso pedagógico profesional que se desarrolla desde la entidad educativa.

SIGNIFICACIÓN PRÁCTICA: radica en que conjuntamente con la alternativa metodológica B-learning, se presenta un programa de preparación con orientaciones y sugerencias metodológicas que apoyen la elaboración, implementación y evaluación de la alternativa de preparación en seguridad informática, conjugándose encuentros presenciales y a distancia desde Entornos Virtuales de Enseñanza Aprendizaje (EVEA).

La investigación está vinculada al proyecto de investigación "La formación a distancia del personal docente" y responde a la línea de investigación "Diseño y modelación de entornos virtuales" de la 5ta Edición de la Maestría en Ciencias de la Educación de la Universidad de Guantánamo.

CAPITULO I. LA PREPARACIÓN EN SEGURIDAD INFORMÁTICA DE LOS DOCENTES DE LAS INSTITUCIONES EDUCATIVAS

En este capítulo se exponen los antecedentes históricos del desarrollo de la seguridad informática y su contextualización en la preparación de docentes, los referentes teóricos y metodológicos que fundamentan la propuesta de la tesis, así como el estado actual de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes

1.1. Antecedentes históricos del desarrollo de la seguridad informática en Cuba y su contextualización en la preparación de docentes

En este epígrafe se revelan las regularidades que caracterizan los antecedentes históricos del desarrollo de la seguridad informática y su contextualización en la preparación de docentes, enmarcadas en la Revolución en el Poder, en función de determinar sus tendencias, se establece para ello, tres etapas o periodos, asumiendo la periodización como "*una síntesis de varios lapsos de tiempo donde no ocurren cambios significativos en el desarrollo de la historia"* (Hernández, A. Y., y Pérez, A. 2013).

Etapa I: (1986 – 1999). Introducción masiva de la computación.

Etapa II: (2000 – 2007). Formación de la Cultura General Integral.

Etapa III: (2008 – Actualidad). Nueva era del uso de las TIC.

Para el análisis tendencial del objeto y el campo de investigación se consideraron los indicadores siguientes:

- Política educacional dirigida a la preparación en seguridad informática de los docentes.
- Contenidos tratados en la preparación en seguridad informática de docentes.
- Principales disposiciones legales que rigen el proceso de implementación de la seguridad informática y su relación con la preparación de los docentes.

Etapa I: (1986 – 1999). Introducción masiva de la computación.

En aras de dar cumplimiento a los lineamientos del Programa del PCC aprobado en el 3er. Congreso 1986, se inicia en el cursos escolar 1986 – 1987, la introducción masiva de la Informática Educativa en diferentes tipos y niveles de enseñanza en el Ministerio de Educación (MINED), incluyendo los Institutos Superiores Pedagógicos (ISP) conocidos en la actualidad como Universidades de Ciencias Pedagógicas (UCP), con la finalidad de ser empleadas en la formación inicial y permanente de los profesionales de la educación en casi todas las especialidades.

Todo ello facilitó el incremento de actividades prácticas en función de las tecnologías disponibles sustentadas en las modificaciones realizadas a los programas de estudio (Plan “B”) que incluían 2 asignaturas, las cuales se dirigieron básicamente al estudio de lenguajes de programación como: el MSX –Basic y el QBasic y algunos sistemas de aplicación bajo el Sistema Operativo MS-DOS como: WordStar, DBase y el Supercalc (Blanco, L. 2004; Pérez, V. 2006).

Se implementa además un plan director de Informática Educativa en la Educación, jugando un papel fundamental la preparación de docentes para el uso de la Informática a partir de la realización de conferencias científicas, cursos de postgrados, talleres, entrenamientos, diplomados, etc.

Desde todos los Institutos Superiores Pedagógicos del país, como centros de formación del personal docente para el Sistema Nacional de Educación, se crea la licenciatura en Educación en la especialidad de Matemática-Computación (Blanco, L. 2004).

Desde este contexto, se formaron de manera emergente, aproximadamente 3500 profesores de Informática, que habían sido ya graduados como Licenciados en Educación en otras asignaturas. Posteriormente, se inició la formación de profesores de Informática, como Licenciados en Educación en los Institutos Superiores Pedagógicos, los cuales se desempeñaron como profesores de esta especialidad desde los diferentes niveles y tipos de educación incluyendo la ETP.

Lo anterior posibilitó, no sólo el desarrollo de hábitos y habilidades así como el aumento del procesamiento, almacenamiento y transmisión de la información mediante las TI desde la instituciones educativas, sino también la entrada y propagación de programas malignos desde los inicios de la década de los años ochenta, donde la cantidad de este tipo de programas ya sobrepasaba los cien y la epidemia comenzaba a causar estragos proliferándose los mismos por los diferentes sistemas informáticos de Cuba y del mundo (Blanco, L. (2004), y Cáceres, J. A. (2012).

Esta problemática conllevó a la realización de actividades de preparación en seguridad informática desde las propias vías utilizadas en la formación inicial y continua de los profesionales de la educación. Así y todo, las acciones de preparación en seguridad informática fueron dirigidas al estudio de los diferentes tipos de virus y sus posibles manifestaciones.

Destacar que en este escenario, se produce además el derrumbe del campo socialista originando una crisis económica en Cuba, trayendo como consecuencia la pérdida de fuentes de financiamiento, se recrudece el bloqueo económico y financiero de Estados Unidos contra Cuba y con ello las actividades subversivas empleando entre otras vías las TIC con la finalidad de destruir la Revolución Cubana.

En el MINED se establece por primera vez una legislación referida a la seguridad informática, la Resolución Ministerial 230 del año 1998, la cual establecía las medidas técnicas, físicas y lógicas para proteger la información y activos informáticos, entre los años 1999 y el 2000 se desarrollan en el organismo central del MINED diversas acciones relacionadas con la seguridad informática (Rodríguez, A. M. 2012), tales como:

- Se inicia la creación de la red informática del organismo central.
- Se elabora el primer plan de seguridad informática.
- Se crea el grupo central de seguridad informática a nivel nacional y en las Direcciones Provinciales y Municipales de Educación, los cuales tenían la función de dirigir y controlar las políticas de seguridad informática emitidas, dentro de ellas la preparación del personal docente dirigidas a aquellos graduados de las especialidades informáticas que cumplían funciones de administradores de redes o responsables de seguridad informática.

Etapa II: (2000 – 2007). Formación de la Cultura General Integral.

En el año 2000 se crea en Cuba el Ministerio de la Informática y las Comunicaciones (MIC) para desarrollar las tareas y funciones que hasta ese momento realizaba el Ministerio de Comunicaciones, así como de la Informática y la Electrónica que ejecutaba el Ministerio de la Industria Sidero - Mecánica, que en unión al MININT constituían los rectores de las acciones de seguridad informática a ejecutarse en todo el país así como llevar a cabo la dirección del Programa de Informatización de la Sociedad Cubana el cual alcanzó la totalidad de las escuelas cubanas.

Todo ello condujo al aumento de las acciones de preparación dirigidas al personal docente para el uso eficiente de estas tecnologías con el fin de asumir los cambios que en materia de educación se venían realizando tales como: el establecimiento del Programa Audiovisual, el reinicio de la televisión escolar en el año 2000, la creación del Canal Educativo en el año 2002 y posteriormente el dos, los cuales mostraron gran diversidad de programas que abarcaban la superación profesional de los docentes, unido al proceso de universalización de las carreras pedagógicas en el cual se utilizaron productos multimedia en CD-ROM y la Maestría de Amplio Acceso en Ciencias de la Educación iniciada en el curso escolar 2005 – 2006.

Desde la ETP se crean carreras de perfil informático para la formación de técnicos en esta especialidad, si bien ello constituía un avance para el desarrollo informático y la formación de personal calificado, se tenía como principal limitación que los programas de estudio se centraban en el desarrollo de hábitos y habilidades para dar solución a problemas vinculados con la informática, siendo limitado el tratamiento de contenidos en seguridad informática que respondiera al uso seguro y ético de las TIC (Leblanch, I. 2012).

Así y todo, continuaban los esfuerzos para la preparación en materia de seguridad informática dirigidos a los docentes, los contenidos fueron destinados por un lado a la protección de la información y de los sistemas informáticos del ataque de programas malignos sobre la base del estudio y clasificación de los virus informáticos y por otro al análisis de las legislaciones vigentes sobre seguridad informática, como por ejemplo la Resolución Ministerial 176 del año 2007 del MINED, constituyendo el reglamento de seguridad para ser utilizado en todas las entidades educativas.

Lo anterior estuvo sustentado a partir de la Resolución 127 promulgada por el MIC, la cual constituye aún el Reglamento de Seguridad para las Tecnologías de la Información en Cuba. Este documento que se ha de implementar en todas las entidades estatales cubanas incluyendo las educativas.

Se asume como aspecto importante lo relacionado con la determinación de las responsabilidades que se le atribuyen a cada usuario de los diferentes sistemas informáticos. Ello permite proyectar un sistema de preparación acorde con el rol o función que desempeñan cada uno en el mismo.

En este mismo sentido, en las actividades de preparación en seguridad informática comienzan a incluirse contenidos relacionados con diferentes metodologías para llevar a cabo la elaboración del Plan de Seguridad Informática, el Plan de Contingencia y los requerimientos para la salva de la información y el acceso a Internet por entidades cubanas.

Etapa III: (2008 – Actualidad). Nueva era del uso de las TIC.

Desde este etapa se introduce a escala internacional determinadas tecnologías emergentes, las cuales facilitan el acceso y procesamiento global de la información, además traen aparejadas nuevos riesgos y vulnerabilidades tales como: el espionaje informático entre naciones, la existencia del madware móvil (avisos publicitarios engañosos), la sobre confianza en el uso de las redes sociales de comunicación, aumento de las técnicas de ingeniería social, la computación en la nube acrecienta la importancia de la seguridad de la información, entre otros aspectos.

Lo anterior exige nuevos retos para la preparación en seguridad informática de los diferentes tipos de usuarios, es por ello que a partir del año 2008, algunas instituciones cubanas imparten cursos de preparación en seguridad informática dirigidos fundamentalmente a recursos humanos graduados dentro de las especialidades informáticas incluyendo los de la educación.

Si bien esto fue un punto de partida para el aumento de una cultura en seguridad informática, estos cursos se desarrollaban para un personal muy limitado pues por un lado, estaban relacionados con las especialidades a fines y por otro, se exigía el cobro para la matrícula de los diferentes usuarios. En el caso de Guantánamo las

empresas (SEPSA, CITMA, DESOFT) entre otras, se han mantenido impartiendo estos tipos de cursos hasta la actualidad.

En la revisión bibliográfica realizada por este autor, se hallaron investigaciones y publicaciones científicas que incluían la preparación en seguridad informática de determinados recursos humanos. En todos los casos se pudo constatar que los contenidos de seguridad informática tratados continúan siendo dirigidos al estudio de las indicaciones realizadas por los diferentes ministerios, incluyendo además la Resolución 17 del año 2010 destinada a la aprobación de las políticas de acceso de los centros educacionales a los servicios telemáticos de la red informática del MINED.

En consecuencia con lo anterior, en el Seminario Nacional de preparación para docentes en función del desarrollo del curso escolar 2013 – 2014, se abordó un tema relacionado con la seguridad de la información y la seguridad informática desde las entidades educacionales cubanas, al respecto, el contenido tratado se circunscribió a la importancia de esta actividad en el marco del uso de las TIC.

En la actualidad, las actividades de preparación en seguridad informática continúan siendo centralizadas y desarrolladas desde las Direcciones Municipales y Provinciales de Educación, participando solamente los graduados de especialidades informáticas como se había explicado anteriormente, de ahí, que los demás docentes de los diferentes tipos y niveles de enseñanza incluyendo los de la ETP permanezcan desorientados y necesitados de adquirir una cultura en materia de seguridad informática que contribuya al uso ético y seguro de las TIC.

Desde este contexto es insuficiente el tratamiento de contenidos dirigidos al logro de la responsabilidad o papel a ejercer por los diferentes tipos de usuarios, según la constante actualización o desarrollo que van alcanzando las TIC, trayendo como necesidad no sólo la implementación de nuevos cursos sino también la actualización de las legislaciones existentes.

En consecuencia, el análisis histórico realizado en las tres etapas asumidas en relación al desarrollo de la seguridad informática en Cuba y su contextualización en la preparación de docentes, ha permitido revelar las siguientes regularidades**:**

- El inicio de una nueva era en el uso de las TI en la década de los años 80, sustentada por la propagación de virus informáticos de ahí que las acciones de preparación en seguridad informática fuesen destinadas al estudio de los virus informáticos y sus posibles manifestaciones.

- Las actividades de preparación en seguridad informática del personal de la educación se realizan de forma centralizada desde las Direcciones Provinciales y Municipales de Educación, dirigidas fundamentalmente a

trabajadores de especialidades informáticas, tales como: administradores de redes informáticas, Web Master, responsables de seguridad informática y profesores de informática, limitándose el acceso a esta actividad a otros profesionales de la educación.

❖ Desde los centros educacionales se mantiene la tendencia de llevar a cabo la preparación en contenidos de seguridad informática a través del estudio de las legislaciones previamente establecidas en función de su posterior cumplimiento e implementación.

1.2. Referentes teóricos y metodológicos que sustentan la preparación en seguridad informática de los docentes en Cuba y a nivel internacional

La incorporación de las TIC sustentada en el Programa de Informatización de la Educación, ha provocado una transformación en la forma de enseñar y aprender en el ámbito educativo cubano, al abrir nuevas posibilidades respecto al acceso a la información, en la adquisición de conocimientos y el desarrollo de hábitos y habilidades, así como en la transformación de los modos de actuación ante las tareas de aprendizaje. Esto permite que estas tecnologías sean un importante instrumento para el desempeño de los docentes en la formación integral de los educandos.

Sin embargo, resulta interesante que en el noble empeño de introducir las TIC en el ámbito educativo cubano las acciones de preparación de los docentes se hayan encaminado fundamentalmente al conocimiento de las potencialidades tecnológicas y su posterior utilización en los diferentes contextos educativos, y se le ha restado importancia a la preparación integral de los mismos donde se tengan en cuenta aquellos aspectos que garanticen la conservación y seguridad de las mismas.

Sobre esta base, Horruitiner, P. (2006), al referirse al término preparación integral del docente, destaca la necesidad de lograr la formación de valores que hagan de éste un ser más pleno, dotado de cualidades de alto significado humano, capaz de poner sus conocimientos al servicio de la sociedad, lo que implica también crear a un profesional creativo, independiente, preparado para asumir su autoeducación durante toda la vida, en correspondencia con la velocidad con que actualmente se produce la transformación de los conocimientos y los constantes cambios de la tecnología.

Este mismo autor destaca las nuevas concepciones asumidas a partir del modelo cubano de formación y preparación de los profesionales desde y fuera de las universidades cubanas, para ello pone énfasis en:

- La reducción de la presencialidad, fundamentalmente de las horas de clases, para favorecer las tareas que refuercen el autoaprendizaje y la autopreparación.
- Las transformaciones del proceso de formación con el apoyo de la computación y las TIC.

- Las transformaciones en el sistema de evaluación del aprendizaje de los estudiantes, desde un enfoque más cualitativo e integrador y centrado en su propio desempeño.
- El fortalecimiento de la formación humanística.

De lo anterior se evidencia la necesidad de un análisis del término preparación el cual ha sido estudiado a partir de diferentes puntos de vista y enfoques, con lo que se tributaría a una clara perspectiva sobre el mismo, así por ejemplo, el diccionario de la Real Academia Española (DRAE), la designa como la acción y efecto de preparar o prepararse, de prevenir o disponer a un sujeto para la acción que ha de seguir para un fin determinado.

Por otro lado, Álvarez, C. (1999: 20) señala que reviste gran importancia la preparación de las nuevas generaciones en función de satisfacer las necesidades de la sociedad (encargo social) a partir de la apropiación de la cultura legada por la humanidad de generación en generación, permitiendo el desarrollo de potencialidades espirituales, físicas y la apropiación de valores sobre la base de un contexto social e histórico concreto.

Autores como: Díaz, R. C, y Del Carmen, E. (2010: 9), conciben la preparación desde el punto de vista pedagógico *como* "*la existencia de posibles necesidades de desarrollo no satisfechas desde la formación inicial del profesional cuando alude al desarrollo se refiere al proceso continuo y sistemático dirigido a alcanzar habilidades, destrezas y valores que le permiten un desempeño satisfactorio para asumir los cambios y transformaciones que se producen en al ámbito escolar o las que emergen del propio proceso científico, tecnológico y social*".

No obstante, hay que considerar que las definiciones antes analizadas, abordan aspectos de relevancia los cuales constituyen referentes teóricos para esta investigación, se asume la definición dada por Pérez, V. (2006: 49), en su tesis doctoral, cuando plantea que la preparación "*constituye un proceso de apropiación de conocimientos, hábitos, habilidades, valores y a la vez el resultado de este, para lo cual se utilizan diferentes vías que combinan procesos de formación permanente y de autopreparación, enriquecidos en la práctica, con el desempeño del rol dentro del equipo docente y la colaboración e intercambio que establece con sus compañeros de trabajo y con los estudiantes*".

Esta misma autora destaca que toda preparación en el área del saber está asociada a la apropiación de contenidos relacionados con esa esfera, de ahí que en su base se hallen procesos de formación entendido este en su sentido más amplio; agrega además que, atendiendo a las formas organizativas empleadas, la preparación puede determinarse como básica o sistemática.

La básica se apoya en diferentes formas curriculares correspondientes al pregrado o el postgrado y la sistemática se lleva a cabo mediante la conjugación de procesos de preparación y autopreparación en los que ocupan un

lugar importante las experiencias individuales y colectivas obtenidas en la propia práctica y mediante el intercambio y colaboración entre los participantes del proyecto educativo.

A su vez, Rodríguez, A. M. (2012: 60), especialista cubano que ha profundizado en el tema objeto de análisis, se refiere a nuevos términos como el de educación en seguridad informática y puntualiza que es la preparación alcanzada por el personal del MINED para trabajar de manera segura con las TIC, mostrando adecuados conocimientos, habilidades, actitudes y valores al aplicar procedimientos de seguridad informática en la resolución de problemas prácticos asociados con la prevención, detección y así como para dar respuesta a las acciones que pongan en riesgo la integridad, confidencialidad y disponibilidad de la información.

Este mismo autor plantea que un sujeto tiene preparación en seguridad informática, cuando posee los conocimientos, destrezas y actitudes necesarias para utilizar de forma segura las TIC en su actividad profesional a fin de resolver los problemas profesionales de forma autónoma y flexible, asimismo está preparado para colaborar con la mejora del sistema informático en su entorno profesional.

Obsérvese que desde este contexto se hace referencia a las terminologías “educación en seguridad informática” y “preparación en seguridad informática”, entre las que existe una relación de coordinación y subordinación; en este sentido se destacan como elemento de vital importancia para esta investigación que desde los ámbitos educacionales cubanos, la seguridad informática no se debe circunscribir solo a las TI, sino a las TIC.

Es por ello que para comprender la necesidad de llevar a cabo la preparación en seguridad informática de docentes es preciso el análisis de la terminología seguridad informática, la cual se ha abordado por numerosos autores desde diferentes puntos de vista.

Sobre esta base, Bugarini, F. (2007), plantea la existencia de cierto grado de incertidumbre en las definiciones sobre seguridad informática; pues las existentes abarcan múltiples y diversas áreas que van desde la protección física del ordenador como componentes del hardware hasta la protección de la información que contienen las redes que la comunican con el exterior.

En este sentido, el autor de esta tesis, advierte la tendencia a la identificación del término seguridad informática con el de seguridad de la información, como si fuesen lo mismo sin tener en cuenta cuáles son sus particularidades. Este considera que la seguridad de la información es más amplia que la seguridad informática aunque hay elementos del primero que pertenecen sustancialmente al segundo, aspecto que se tendrá en cuenta para la estructuración de la propuesta de preparación de docentes que se propone.

Algunos autores como Mayol, R. N. (2006); Monzón, C. J. (2009) conciben la seguridad informática como un conjunto de métodos y herramientas determinadas para proteger la información, por ende los sistemas informáticos ante cualquier amenaza o proceso en el que además intervienen las personas.

En sentido similar, Muñoz, A. y Aguirre, J. R. (2013); Mayorga, C. (2014), describen la seguridad informática como el conjunto de normas y procedimientos que tienen como objetivo, garantizar el uso de la información que reside en los sistemas informáticos.

Como se puede apreciar, ambas consideraciones exponen la necesidad de llevar a cabo la protección de la información existente en los sistemas informáticos, para lo cual se necesita la determinación de vías y formas (métodos, procedimientos y herramientas) necesarias para el logro de la protección y seguridad de las mismas; sin embargo, sólo en la primera se aborda la responsabilidad de intervención de los recursos humanos en función de alcanzar los objetivos propuestos.

A diferencia de las anteriores definiciones, autores como Peláez, R. (2012); Ramiro, J. (2006), caracterizan la seguridad informática como aquellas prácticas y condiciones particulares a tener en cuenta en dependencia de los sistemas de procesamiento de la información y su almacenamiento, con lo que no queda claro el tipo de tecnología a utilizar ni la relación que se establecerá con los usuarios a partir del papel que les corresponda desempeñar.

Por otro lado, en el sitio web Redyseguridad.firp.unam.mx, se identifica la seguridad informática como las medidas que impiden la ejecución de operaciones no autorizadas sobre sistemas o redes informáticas, especificando que cuando se habla de medidas, se refieren al uso de regulaciones legales aplicadas a cada sector o tipo de organización dependiendo del marco legal de cada país.

Aunque esta definición es más amplia que las anteriores, se puede constatar que se circunscribe sólo a determinados aspectos vinculados con la seguridad de redes informáticas que dependen de la aplicación de medidas técnicas o de la implementación de determinadas disposiciones jurídicas de ahí su naturaleza tradicional y reduccionista.

Importante para esta investigación resulta la concepción del término seguridad informática que aparece en el Decreto Ley 199 del año 1999, al considerarla como el conjunto de medidas: administrativas, organizativas, físicas, técnicas, legales y educativas, con enfoque integral y tratamiento en sistema, dirigidas a prevenir, detectar y responder a las acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca o conserve a través de las tecnologías informáticas.

Como se puede apreciar en esta nueva definición se hace referencia a nuevas cualidades como la necesidad de implementar en forma de sistema, no sólo las medidas técnicas o jurídicas determinadas, sino también aquellas que en el orden de lo educativo, lo organizativo permitan garantizar la protección tanto de la información como de los sistemas utilizados durante su realización y para su almacenamiento o transmisión.

Aun así el autor de esta investigación considera que la definición que más se ajusta a los requerimientos para estructurar la preparación en seguridad informática de docentes, es la abordada desde la Orden 35 del MININT del año 2012 donde, desde una concepción holística y abarcadora se asocia la seguridad informática con la terminología de seguridad de tecnologías de infocomunicaciones,

En ese sentido, se le caracteriza como el estado en el cual se garantiza la protección de la información, las comunicaciones seguras y se minimizan las vulnerabilidades mediante el conjunto de medidas técnicas, físicas, legales, educativas y organizativas a implementar en la instalación, por la administración, los usuarios, el servicio técnico, en correspondencia con los resultados de la investigación y el desarrollo alcanzado por las tecnologías de la información.

Desde este punto de vista, a partir de las medidas de seguridad antes analizadas se le concede gran importancia a aquellas que tienen que ver no sólo con los recursos humanos como responsables del uso y conservación tanto de las tecnologías como de la información que se procese, almacene o transmita sino también como responsables de aplicar dichas medidas en aras de garantizar la confidencialidad, disponibilidad e integridad de las mismas según el rol que les corresponde desempeñar y por otro lado, la visión de incluir la investigación como forma o vía de descubrir nuevos conocimientos en correspondencia con el desarrollo tecnológico que se va alcanzando desde las diferentes instituciones y a escala global.

A partir de la posición antes analizada, se asume que la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes” debe estructurarse tomando como base la concepción del método dialéctico - materialista de la filosofía marxista – leninista, donde se fundamenta, que a partir del análisis de la práctica se propicia la contextualización y estructuración de la investigación de acuerdo con las demandas sociales y el desarrollo tecnológico alcanzado, favoreciendo la relación teoría – práctica, así como la actividad reflexiva y transformadora en aras del desarrollo profesional y personal de los implicados.

Desde esta concepción se asumen, además, sus principios tales como la objetividad, la concatenación universal, el movimiento, el, desarrollo, el análisis histórico concreto, el análisis multilateral y la flexibilidad, MINED. (2005: 6). Estos principios facilitan la comprensión de la preparación en seguridad informática de los docentes a partir del análisis de la práctica del proceso pedagógico profesional que se desarrolla desde el Politécnico “Julio Antonio Delgado Reyes”.

No de forma aislada, sino sobre la base del estudio de las ciencias y disciplinas relacionadas con las TIC desde el contexto histórico actual determinándose cuáles son los nuevos aspectos, cualidades y propiedades que orientan la preparación en seguridad de docentes partiendo de las regularidades de la realidad y su proyección hacia formas superiores de desarrollo.

De ahí la necesidad de emplear nuevas formas de enseñar y aprender que les permita a los sujetos adquirir los conocimientos necesarios en materia de seguridad informática, pues esta en parte determina la forma de uso de las TIC (Alfonso, A., y Arocha. H. C. 2010).

Es por ello, que desde la realidad cubana se ponen de manifiesto las exigencias del Programa de Informatización de la Sociedad, donde se puntualiza el uso masivo de las TIC y la necesidad de que todos los sujetos adquieran una cultura general integral al respecto.

Desde este paradigma, la seguridad informática juega un importante papel en función de mantener los logros sociales conquistados por la Revolución Cubana, constituyendo una de las dimensiones de la Seguridad Nacional (Quesada, R., Ceballos, C., Miranda, E. H. 2007: 20).

En correspondencia con lo anterior, se toma en consideración en esta investigación lo plasmado en los Lineamientos de la Política Económica y Social, expresión de la voluntad del pueblo cubano y de la política del Partido, el Estado y el Gobierno de la República de Cuba, en función de actualizar el modelo económico cubano para garantizar la continuidad e irreversibilidad del socialismo, el desarrollo económico del país, la elevación del nivel de vida de la población sobre la base de valores éticos y políticos de los ciudadanos cubanos.

Lo anterior tiene relación con la problemática que se investiga desde el epígrafe V: “Política de ciencia, tecnología, innovación y medio ambiente” en los Lineamientos: 131 y 135, desde los que se plantea sostener y desarrollar los resultados alcanzados en el campo de la biotecnología, la industria del software, el proceso de informatización de la sociedad y definir una política tecnológica que comprenda el control de las tecnologías existentes (PCC, 2011, p.21:22).

Asimismo en el epígrafe VIII Política industrial y energética, en el lineamiento 223 se plantea elevar la soberanía tecnológica en el desarrollo de la infraestructura de telecomunicaciones (PCC, 2011, p.30).

Si se tiene en cuenta la actual situación de la sociedad cubana, que se halla en constantes amenazas proyectadas por los gobiernos de los Estados Unidos de Norteamérica y se materializan por organizaciones como la Agencia de Estados Unidos para el Desarrollo Internacional (USAID), así como la puesta en marcha, entre otras cuestiones, del proyecto anti cubano conocido como Zunzuneo donde se promueve a través de equipos

móviles de cómputo y tecnologías emergentes, acciones subversivas dirigidas a los más jóvenes con la finalidad de fomentar inestabilidad en Cuba y otros países del mundo.

Por eso, el encargo social de los docentes es estar bien preparados para cumplir con su papel de agente socializador y así poder transmitir a las presentes y futuras generaciones los conocimientos, valores y buenas formas de actuación en relación al uso eficiente y seguro de las TIC (Rodríguez, A. M. 2012).

Por otro lado, constituyen referentes teóricos para esta investigación la Teoría Histórico Cultural de L.S. Vigotsky, pues en ella se presenta al aprendiz como un sujeto activo en constante interacción con los objetos de aprendizaje y con otros sujetos; de ahí la importancia que se le concede a esta concepción para llevar a cabo la preparación en seguridad informática de los docentes, a partir de que toma como centro al sujeto que aprende teniendo en cuenta sus intereses, convicciones, necesidades, etc., en correspondencia con las condiciones reales y socioculturales existentes.

De igual forma, adquiere gran significación para esta investigación, lo relacionado con la mediación que se establece por la interacción dialéctica derivada de los procesos de actividad y comunicación entre los sujetos participantes en la preparación en seguridad informática, las cuales desde las influencias de un contexto histórico determinado y a partir de los diferentes signos e instrumentos socioculturales establecidos por estos y las TIC existentes contribuyen al intercambio, la colaboración y el protagonismo de los implicados atendiendo a las condiciones organizativas, tecnológicas, culturales y humanas necesarias para acceder a los nuevos conocimientos y valores.

Otro aspecto de vital importancia para esta investigación, se le atribuye a la concepción de Vigotsky referente a la Zona de Desarrollo Próximo (ZDP), entendida según Bermúdez, R., y Pérez, L. M. (2004: 52), como la distancia o diferencia entre lo que el sujeto es capaz de hacer por sí mismo (nivel de desarrollo real) y aquello que sólo puede hacer con ayuda de los demás (nivel de desarrollo potencial).

Desde esta perspectiva, llevar a cabo la correcta orientación de la estructuración de la comunicación entre los protagonistas de la preparación en seguridad informática en el contexto donde se produce dicha interacción y los contenidos en seguridad informática, tiene un gran significado pues determinará la naturaleza de la dirección del desarrollo de los implicados y, estimulará el uso adecuado de las TIC en la entidad educativa en función de lograr el cuidado y conservación de las mismas.

A partir de los referentes antes asumidos, se toma en consideración que toda preparación en seguridad informática, debe proyectarse atendiendo a las necesidades de carácter social, a las reflexiones de la práctica histórica concreta y al desarrollo tecnológico alcanzado; abarcando además no sólo conocimientos,

procedimientos, hábitos, habilidades sino también formas de actuación y valores que promuevan al crecimiento personal y desarrollo integral de los docentes.

Desde este contexto, la preparación en seguridad informática de los docentes, debe adoptar las nuevas situaciones de enseñanza aprendizaje que promueven la participación en experiencias educativas altamente interactivas empleando diferentes espacios de comunicación como, por ejemplo el uso de la Web 2.0 que constituye una nueva actitud para acceder a la red y al conocimiento (González, I. y Blanco, L. 2013).

Los anteriores autores plantean que estos espacios promueven nuevas formas para la comunicación e intercambio de informaciones, lo cual propicia una nueva etapa para el diseño y desarrollo de materiales didácticos digitales, así como la aparición de recursos educativos abiertos que suponen cambios en la manera de compartir e implementar los recursos educativos y la gestión del conocimiento.

En relación con lo anterior, otros autores como Guevara, J. (2014); Martínez, O. L. (2014), puntualizan la necesidad de lograr un papel activo en los aprendices con el importante apoyo y orientación de los docentes, a partir de la transmisión de determinadas habilidades y modos de actuación respecto a la manera de cómo hallar y acceder a la información, para ello hay que aprovechar las oportunidades que brindan las TIC. Con ello se pone de manifiesto la personalización de la enseñanza centrada en el estudiante.

Desde esta concepción se han introducido, a partir del propio desarrollo alcanzado por las TIC y en especial de la Educación a Distancia (EAD), determinadas opciones como los sistemas E – learning desde los cuales se materializa el aprendizaje basado en la interactividad y la comunicación pedagógica.

Ejemplo de lo anterior, lo constituye el empleo de los llamados EVEA para la preparación de docentes, caracterizados según los criterios de los doctores en ciencias pedagógicas: Herrera, E. (2005); Pérez, V. (2006); Sánchez, Y. (2011), como espacios configurados en la red telemática a partir de las herramientas y facilidades que brindan en situaciones de enseñanza y aprendizaje en que sus protagonistas pueden interactuar y realizar las tareas docentes.

Estos mismos autores exponen que las actividades de enseñanza y aprendizaje que se realizan desde EVEA se caracterizan por el predominio de la separación física de sus protagonistas, sin embargo, gracias a las múltiples herramientas de actividad y comunicación tanto sincrónicas (chat, teleconferencias u otras) como asincrónicas (correo electrónico, foro, etc.) propician una comunicación multidireccional y diversificada.

En este sentido, Herrera, E. (2005: 40) afirma que en la elaboración de un curso a distancia que se desarrolla con el empleo de entornos virtuales de enseñanza - aprendizaje, se hace necesario aludir a aspectos o etapas tales

como: la concepción, el diseño, el montaje, el control, la evaluación y la validación, aspectos que se asumen en la investigación.

En la etapa de concepción del curso, aboga por la identificación de los problemas profesionales y la determinación de las necesidades de los sujetos, se justifique su pertinencia y a quiénes se dirige; se seleccione el equipo de trabajo que lo realizará planificando el proceso de elaboración y el inicio de la preparación básica de los especialistas.

Desde la etapa de diseño, plantea que se modela el EVEA y las acciones para la enseñanza y el aprendizaje en interrelación con el diseño informático a utilizar, lo cual dará paso al montaje y adecuación de los espacios del entorno virtual creando además el sistema de materiales didácticos a emplear.

El control y la evaluación se orientan hacia el seguimiento y la valoración de la elaboración del curso y sus resultados con su consecuente retroalimentación y corrección; con la primera versión del curso realizada se proyecta la validación del mismo de forma integral, todo con la finalidad de comprobar el cumplimiento de las indicaciones establecidas.

Esta misma autora afirma que el desarrollo de cursos empleando EVEA tiene dos componentes estructurales básicos: uno de naturaleza tecnológica, constituido por las redes y demás recursos que soportan el espacio virtual, lo cual permite el entramado de relaciones entre las personas y la realización de las actividades y otro de naturaleza humana, constituido por las personas, estructuras, funciones, situaciones y actividades, que garantizan el desarrollo de la oferta educativa

En Cuba, se han puesto de manifiesto varias consideraciones según lo anteriormente planteado, desde las cuales juega un papel primordial el uso de las TIC, lo que ha provocado la aparición de nuevas herramientas y estilos de aprendizaje.

Desde este referente básico, Miniguano, M. A. (2014) expone que los cambios ocurridos a partir de la universalización de la Educación Superior, han estado asociados a una concepción pedagógica, didáctica y organizativa novedosa, donde la enseñanza y el aprendizaje dirigidos a la formación de los profesionales, deja de ser bilateral (entre profesor y estudiante), para desarrollarse multilateralmente (entre el profesor, el estudiante y la comunidad) tomando como principal exponente la modalidad semipresencial que responde a nuevas exigencias sociales y formativas.

Desde la modalidad semipresencial, también conocida a nivel internacional como Blended – Learning, B-Learning, aprendizaje mezclado, combinado, híbrido, se trata de superar el modelo pedagógico de enseñanza tradicional centrado en el profesor y en la transmisión de los contenidos por este. Es por ello que se apoya en

brindar un aprendizaje flexible, abierto donde la comunicación va a estar mediada por las TIC (Pompeya, V. E. (2008); Vega, G. M. y Ansola, E. (2013); Andrade, E. M. (2013).

Esta comunicación mediada por las TIC según Sánchez, Y. (2011: 29), se conoce como *mediación pedagógico-instrumental que no es más que el conjunto de acciones, intervenciones y recursos tecnológicos, del sistema articulado de agentes, agencias y medios, como mediadores sociales que intervienen en el hecho educativo en diversos contextos, que facilitan el proceso de intercomunicación pedagógica entre docentes y estudiantes.*

Lo anterior supone, si se consideran los criterios de González, I. y Blanco, L. (2013), realizar cambios en la manera de concebir las actividades de enseñanza y aprendizaje, de manera que posibiliten que docentes y educandos compartan e implementen los recursos educativos y el conocimiento, de ahí la necesidad de implementar nuevas estrategias para que estos puedan construir sus propios aprendizajes.

Desde esta concepción, la estructura de las actividades de enseñanza y aprendizaje adquieren gran connotación, ya que básicamente se desarrollan empleando tanto la modalidad presencial como la educación a distancia.

En este mismo sentido, Martí, J. A. (2009); López, R. (2010), consideran que no es aconsejable hacer una extrapolación directa de los principios de la enseñanza presencial a la educación a distancia, pues deben ser consideradas las particularidades de cada modalidad que repercuten en su didáctica, no se ha de copiar fielmente lo que ocurre en la primera hacia la segunda con respecto a las categorías o componentes personales y no personales, así como el modo en que estos se relacionan.

Lo antes evaluado, desde un enfoque dialéctico, posibilitó al autor de esta tesis llegar a la conclusión de que la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”, debe fundamentarse a partir del análisis y reflexión de la práctica obedeciendo a determinados fines y propósitos del desarrollo y necesidades sociales de los protagonistas, permitiendo su contextualización en correspondencia con el desarrollo pedagógico, tecnológico y los procesos organizativos alcanzados.

Los elementos apuntados revelan la necesidad de una concepción de las acciones para la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”, desde un enfoque sistémico, donde se observe la interrelación de cada uno de sus elementos no de forma aislada sino como parte de un todo; se asume además de este enfoque las cuatro propiedades fundamentales que lo caracterizan abordadas por: Rosell, W. y Más, M. (2003: 3), tales como:

- *Los componentes constituidos por todos los elementos que constituyen el sistema.*
- *Una estructura que comprende las relaciones entre los elementos del sistema, basada en un algoritmo de selección y el ordenamiento lógico de los elementos.*

- *Las funciones determinadas por las acciones que puede desempeñar el sistema, tanto de subordinación vertical, como de coordinación horizontal.*

- *La integración correspondiente a los mecanismos que aseguran la estabilidad del sistema apoyados en las planificación, organización dirección y evaluación del mismo y que permitan la retroalimentación de los resultados alcanzados*.

Por otra parte, resulta importante para esta investigación las consideraciones emitidas por Expósito, C., et al. (2001), en el libro "Algunos elementos de metodología de la enseñanza de la Informática", cuya base está en la implementación de las llamadas formas regulares del proceso de enseñanza - aprendizaje de las asignaturas relacionadas con la familia de esta especialidad, caracterizadas por:

1. Formación de conceptos.
2. Elaboración de procedimientos.
3. Resolución de problemas.

En este trabajo se asume que la formación de conceptos constituye la forma a emplearse en la adquisición y obtención de conocimientos como medios que facilitan el desarrollo del saber a través del tratamiento de los diferentes conceptos relacionados con la seguridad informática, los cuales serán aplicados posteriormente en la elaboración de procedimientos tanto mentales como manuales esencialmente los interactivos, lo cual propicie la descripción de cada uno de los pasos u operaciones a tener en cuenta en el cuidado de las TIC instaladas.

Desde una visión holística hay que precisar que tanto la formación de conceptos como la elaboración de procedimientos van a estar asociados a la adquisición de conocimientos, al desarrollo de hábitos, habilidades y valores, mientras que la resolución de problemas facilitará la fijación de los conocimientos siempre tomando como centro al sujeto que aprende.

De esta manera, la preparación en seguridad informática de los docentes, debe contribuir a la adquisición de conocimientos, valores y actitudes, desde este punto de vista, se pone manifiesto la relación existente entre las formas para alcanzar la educación de los sujetos, las exigencias sociales y las cuestiones derivadas del desarrollo, utilización y sostenibilidad de las TIC.

Viendo esta según las consideraciones realizadas por Lima, S. (2012), como la integración de algunos sistemas como la informática y las telecomunicaciones conformadas por un conjunto de dispositivos dentro de los que se destacan el video interactivo, la Internet, la televisión, las grabadoras, los satélites, el teléfono, las redes de computadoras, las fibras ópticas, el láser, los teléfonos móviles, los nuevos procedimientos de impresión, que

permiten la adquisición, producción, tratamiento, comunicación, registro y presentación de información, datos, voz e imagen.

En sentido similar, diversos autores como Pérez, V. (2006); Lima, S. (2012) y Aranda, R. (2013), añaden que en la actualidad el uso de las TIC se ha acelerado con gran rapidez, debido a la existencia de la convergencia tecnológica cuya base se haya en el desarrollo de algunas ciencias como: la Cibernética, las Telecomunicaciones, la Electrónica, la Microelectrónica, la Automática, la Nanotecnologías y los Nano materiales.

Más recientemente con la aparición de las llamadas tecnologías emergentes, tales como: la computación en la nube, las tecnologías de geolocalización, la Web 2.0 y 3.0, entre otras y, por otro lado, dada la proliferación de los dispositivos móviles y dispositivos inteligentes que según Del Porto, C. (2013) superarán a las computadoras personales como dispositivos más comunes para acceder a la Web a nivel internacional aumenta el número de riesgos y vulnerabilidades relacionadas con el uso de las TIC.

A pesar de que estas tecnologías han incidido positivamente en el surgimiento de dispositivos cada vez más pequeños, aumentando la capacidad de almacenamiento, procesamiento y transmisión de la información a velocidades jamás sospechadas, los aspectos relacionados con la seguridad de las TIC son mucho más críticos y complicados.

Ante esta reflexión, Del Porto, C. (2013), reconoce que con la aparición de los dispositivos móviles que fomentan un estilo de vida digital, surgen nuevas amenazas en lugares inesperados tales como en la televisión u equipos electrodomésticos, afirma además que la seguridad informática ha dejado de ser interés exclusivo de los especialistas convirtiéndose en una necesidad de carácter universal.

Al respecto, Leblanch, I. (2013), al referirse a la utilización de las TIC y a la seguridad informática desde las entidades educativas cubanas expone, que aún se cometen violaciones de las normas éticas de seguridad informática, reafirma además que se observan limitadas influencias educativas que afectan no solo la preparación de docentes sino también restringe su desempeñó diario atendiendo al uso de las TIC en forma integral.

En consecuencia, los siguientes autores (Borghello, C. F. 2001; Mayol, R. N. 2006; Bugarini, F. 2007; Peñalver, N. 2010; Alfonso, A., y Arocha. H. C. 2010; Cáceres, J. A. 2012, y Valdés, M. 2012), al abordar sus criterios sobre qué elementos deben tenerse en cuenta en la preparación en seguridad informática de los sujetos incluyéndose los de la educación plantean que se debe garantizar:

- Que los usuarios tengan conocimientos sobre las terminologías relacionadas con la seguridad informática, los que les posibilitará comprender de forma objetiva las herramientas, tecnologías y, procedimientos asociados a

esta actividad, así como estar al tanto ante la existencia de riesgos o vulnerabilidades que pueden afectar las TIC existentes.

- Abordar temas de carácter teórico, organizativo y educativo que promuevan valores éticos y morales en los usuarios en relación con el uso seguro de las TIC.

- Incorporar contenidos sobre salva y protección de la información, el uso de aplicaciones antivirus destacando sus fortalezas y debilidades.

- Medidas de seguridad para combatir cualquier manifestación engañosa al utilizar las redes sociales de comunicación, el empleo del correo electrónico y equipos móviles de cómputo.

- Introducir temas sobre computación en memoria, la cual ha dado paso a la utilización de gran cantidad de aplicaciones y datos que pueden contener amenazas publicitarias engañosas que pongan en riesgo la seguridad de la información y de las tecnologías existentes.

- La necesidad de actualización de los sistemas operativos y uso de software libre que sean más resistentes a los ataques informáticos.

- Vincular elementos teóricos como prácticos en donde se traten contenidos de auditoría informática, la implementación del plan de seguridad informática y plan de contingencia desde las entidades u organizaciones, abarcando los problemas de seguridad informática existentes.

Sobre esta misma concepción, Hernández, L. (2012), y Bidot, J. (2012), plantean que para lograr la preparación en seguridad informática de los recursos humanos, es necesario además aprovechar las potencialidades que ofrecen las TIC para crear espacios de intercambio y colaboración con vista a mantener de forma sistemática al tanto a los usuarios ante los cambios existentes en relación al desarrollo de la seguridad informática.

Asimismo hay que precisar el nivel de conocimientos sobre seguridad informática que poseen los usuarios con vista a instrumentar las acciones de preparación en relación con las necesidades y con el apoyo de los más aventajados.

Todo lo anterior, se pone de manifiesto en el Artículo 2 de la Resolución Ministerial 127 del año 2007 donde se planta la exigencia de que todos los usuarios de las TIC adquieran la preparación necesaria y los conocimientos de seguridad informática imprescindibles para su posterior utilización en el desempeño de su trabajo.

Por otro lado, se asume en esta investigación el criterio de Rodríguez, A. M. (2012), al plantear que en la preparación en seguridad informática de los sujetos deben ponerse de manifiesto las siguientes dimensiones, las

cuales se ajustan a las condiciones del proceso pedagógico profesional reflejadas desde el Politécnico "Julio Antonio Delgado Reyes":

Dimensión Político – Ideológica: la cual se enmarca en el nivel de preparación que deben alcanzar los sujetos respecto a las bases legales que sustentan la seguridad informática, así como el tratamiento de valores éticos y morales derivados del uso de las TIC.

Dimensión Pedagógica: dada por el uso de las potencialidades pedagógicas de las TIC para llevar a cabo la preparación en seguridad informática de los sujetos teniendo presente la elaboración de programas de preparación, la realización del diagnóstico, la proyección de la planificación, organización, ejecución, control y evaluación de los resultados derivados de las acciones de preparación concebidas.

Dimensión organizativa: que refleja las cuestiones, vías, herramientas y escenarios a emplearse para la instrumentación de la preparación en seguridad informática de los sujetos a partir del análisis de las condiciones existentes.

Dimensión tecnológica: que define el nivel de preparación en cuanto a los temas referidos a la seguridad informática y su posterior aplicación en su actividad profesional, mostrando dominio en cuanto al uso del correo electrónico, navegación en Internet, salva de la información, uso de contraseñas, identificación de incidentes de seguridad informática, virus informáticos, entre otras cuestiones.

Es por ello que tras el análisis realizado, se asume en este trabajo de investigación que un docente tiene preparación en seguridad informática cuando a partir de las necesidades sociales, del rol que desempeña dentro del equipo de trabajo pedagógico y la reflexión de su práctica, es capaz de emplear adecuadamente las técnicas, procedimientos, metodologías, herramientas y normativas establecidas en función de garantizar la disponibilidad, integridad y confidencialidad de la información que se procese, almacene o trasmita a través de las TIC insertadas en las entidades educativas cubanas.

1.3. Diagnóstico del estado actual de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"

El diagnóstico de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes" se realizó con una población de 112 miembros, de la cual se seleccionó como muestra a de 41 docentes que representan un 36,6% del total de la población, con la finalidad de corroborar el problema planteado en la investigación y facilitar la elaboración de la alternativa que se propone para dar solución al mismo. En el (Anexo 1), se muestran las variables, dimensiones e indicadores que fueron empleados en la elaboración de los instrumentos de investigación.

Todo ello permitió la recopilación de información derivada de la aplicación de varias técnicas, métodos e instrumentos de investigación como encuestas, entrevistas y una prueba inicial de desempeño con la finalidad de valorar el estado actual que presenta la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes" (Ver Anexos del 5 al 6).

1. Preparación en seguridad informática alcanzada por los docentes del Politécnico "Julio Antonio Delgado Reyes".

Sobre la base de la valoración de los instrumentos aplicados, se puede inferir que 30 de los docentes de la muestra (73,1%), poseen más de 5 años de experiencia en la ETP y 11 (26, 8%) docentes tienen menos de esa cifra.

Por otro lado el 34, 1% son graduados de Master en Ciencias de la Educación, un 4, 8% alcanzó la categoría docente de asistente y 12, 1% de instructor, lo cual demuestra una sólida preparación del colectivo pedagógico que labora en la entidad educativa.

En este mismo sentido, todos los docentes que conforman la muestra (100%) reconocieron la importancia y necesidad de una preparación en seguridad informática, para hacer un uso adecuado de las TIC.

En consecuencia, la autovaloración realizada por los docentes acerca de su preparación sobre seguridad informática atendiendo a cada uno de los ítems de la dimensión política – ideológica y tecnológica arrojó que 36 (87, 8%) reconoce no poseer preparación en relación con las legislaciones de seguridad informática vigentes, clasificación de programas malignos y uso de software antivirus, los métodos y técnicas para la salva de la información y las metodologías asociadas a la elaboración del Plan de Seguridad Informática y Plan de Contingencias; de igual forma, alcanzaron resultados similares en estos mismos ítems en la prueba inicial realizada, donde 39 docentes (95, 1%) obtuvieron calificaciones de mal y sólo 2 (4, 8%) de regular.

De igual modo, tanto en la autovaloración realizada por los docentes como en la prueba aplicada, se pudo apreciar que el 100% de la muestra seleccionada no posee conocimientos acerca de los llamados sistemas de tierra física, de alarmas contra incendios e intrusos, técnicas de ingeniería social, y las medidas de seguridad a tener en cuenta en el uso de las redes sociales de comunicación.

Atendiendo a las medidas de seguridad a emplearse durante el uso del correo electrónico, se evidenció que entre (el 21, 9% y 65, 8%) de los docentes encuestados reconocieron tener mediana y baja preparación respectivamente y sólo 5 (12, 1%) de ellos consideró haber alcanzado una alta preparación, lo cual demuestra falta de correspondencia con los resultados alcanzados en la prueba de desempeño, en la cual 36 (87, 8%) docentes fueron evaluados de mal y cinco (12, 1%) de regular.

Otra importante información aportada, tanto por la encuesta como por la prueba de desempeño aplicadas, fue que entre el (95, 1% y el 97, 5%) de los docentes mostraron tener pocos conocimientos de las técnicas a utilizar para garantizar la seguridad de la información contenida en fuentes digitales e impresas y de las medidas a tener en cuenta para el uso de equipos móviles de cómputo desde las entidades educativas, sin embargo de los 2 (4, 8%) docentes que manifestaron en la encuesta haber alcanzado una alta preparación al respecto, sólo uno de ellos obtuvo la calificación de regular en la prueba de desempeño ejecutada.

En la propia encuesta, al analizar la preparación lograda por los docentes en la aplicación de auditorías informáticas y la realización del mantenimiento a las TIC, se pudo evidenciar que el 92, 6% de los encuestados declaró falta de dominio en estos temas y sólo tres (7, 3%) manifestaron tener un nivel medio de preparación al respecto.

De igual manera, en los ítems antes mencionados se obtuvo resultado similar en la realización de la prueba de desempeño, al arrojar lo siguiente el 97, 5% de los docentes fueron evaluados de mal al no reconocer las técnicas, procedimientos o métodos de auditorías informáticas que se emplean en su entidad educativa y sólo 1 (2, 4%) alcanzó la categoría de regular.

Al evaluar el dominio de las principales potencialidades que brinda la realización eficiente del mantenimiento a las TIC, al 95, 1% de los docentes se les otorgó la categoría de mal, al resto 4, 8% de regular.

2. Organización y desarrollo de acciones de preparación en seguridad informática, dirigidas a los docentes del Politécnico "Julio Antonio Delgado Reyes".

Por otra parte, en la valoración realizada en cuanto a los ítems de la dimensión pedagógica y organizativa, se corroboró que sólo el 4, 8% y hasta el 7, 3 de los docentes encuestados y entrevistados, habían recibido alguna que otra preparación, dirigida a aquellos docentes responsables de la seguridad informática y de los servicios informáticos que se prestan en las escuelas politécnicas radicadas en el municipio Guantánamo, tratándose específicamente determinados contenidos orientados a la elaboración del Plan de Seguridad Informática y Plan de Contingencias así como la sostenibilidad de la conectividad de las redes informáticas locales con diferentes proveedores de servicios.

Sintetizándose tanto el número de docentes como de contenidos necesarios y pertinentes, los cuales contribuyan verdaderamente a la seguridad de las TIC existentes en las entidades educativas de la ETP, todo ello debido a las complejidades a las cuales está sometido el proceso pedagógico profesional en esta educación donde constantemente el docente se encuentra transitando por diferentes áreas de la producción y los servicios en función del desarrollo de habilidades profesionales en sus educandos.

Otra dificultad enfatizada por el 100% de los docentes encuestados y entrevistados fue el insuficiente acceso a fuentes de información, ya sean digitales o impresas, lo que impide no sólo su preparación sino también la actualización sistemática en aras de los nuevos avances que van alcanzando la ciencia y la técnica en la sociedad contemporánea.

En resumen y completando el diagnóstico del estado actual de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes" se pudieron constatar las siguientes limitaciones:

1. Desconocimiento de las resoluciones y regulaciones fundamentales acerca de la seguridad informática en Cuba y de las cuestiones técnicas, educativas e ideológicas relacionadas con esa actividad.

2. La pobre concepción de la planificación, organización, ejecución, control y evaluación de las actividades de preparación en seguridad informática, sin considerar las características propias y la operatividad de las tareas que se ejecutan en la ETP, lo cual determina el papel que deben asumir los docentes en su desempeño profesional.

3. La carencia de materiales didácticos, destinados a la preparación en seguridad informática, que demuestren una adecuada selección de los contenidos derivados no sólo de las tecnologías emergentes y nuevos equipos móviles de cómputo que van surgiendo sino también desde las TIC existentes en la entidad educativa.

4. El insuficiente uso de métodos y estrategias educativas que desde el contexto de la ETP constituyan verdaderos espacios para el debate y la reflexión sobre temas de seguridad informática.

Conclusiones del capítulo I

La utilización del método histórico y lógico permitió determinar las tendencias que se manifestaron en la evolución de la preparación en seguridad informática de docentes puestas de manifiesto a partir de la determinación de sus tres etapas.

La preparación en seguridad informática de los docentes en Cuba constituye una necesidad para satisfacer las demandas sociales en el uso seguro y ético de las TIC, esta propicia ser tratada no sólo desde lo tecnológico sino también desde lo pedagógico, político - ideológico y organizativo.

Para la instrumentación de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", es necesario tener en cuenta las condiciones en que se desarrolla el proceso pedagógico profesional desde esta entidad educativa, pues condiciona el modo de actuación profesional de este trabajador de la educación.

CAPÍTULO II. LA PREPARACIÓN EN SEGURIDAD INFORMÁTICA DE LOS DOCENTES DEL POLITÉCNICO "JULIO ANTONIO DELGADO REYES"

En este capítulo, se abordarán los rasgos que caracterizan la alternativa metodológica para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", la cual tiene como fundamento el empleo de la modalidad B-learning como forma o vía fundamental para llevar a cabo la estructuración de dicha preparación. Se expone además la valoración de los resultados de la investigación mediante el método criterio de especialistas.

2.1. Fundamentación de la alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"

Al estudiar el término alterativa se apreció que el Diccionario de la Real Academia Española (DRAE), destaca que la palabra alternativa "*proviene del latín alternătus que significa: opción entre dos o más cosas*" (DRAE, 2004).

Valle, A. (2012: 193), a su vez, define la alternativa como "*una opción o vía para dar solución a un problema que se contrapone a otras ya existentes, asumiendo un carácter específico, pues las soluciones existentes no se presentan sistemáticamente en la práctica de ahí que no alcancen un alto grado de generalidad*".

Lo expuesto implica elegir de forma objetiva aquella opción que resulte más beneficiosa, adecuada o pertinente en correspondencia con los intereses, necesidades y posibilidades reales del contexto donde será implementada.

Este propio autor destaca que las alternativas tienen como componentes fundamentales los que se muestran a continuación, aspectos que se asume en esta investigación:

- Objetivos
- Recomendaciones
- Ejemplos
- Formas de implementación
- Formas de evaluación

En tal sentido, la alternativa que se propone constituye una opción metodológica semipresencial conformada por secuencias de acciones distintivas e integradas que orientan la planificación, organización, ejecución, y evaluación de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", a partir de las potencialidades y necesidades sociales e individuales de los implicados en

correspondencia con las condiciones de su entorno, determinadas por las características del proceso pedagógico profesional, el establecimiento de relaciones profesionales de forma presencial y a distancia desde EVEA.

A partir de los anteriores referentes, el autor de esta tesis, advierte la necesidad de analizar determinadas consideraciones relacionadas con la modalidad B-learning, las cuales sirven de sustento para la elaboración de la propuesta de preparación en seguridad informática de docentes.

En consecuencia con lo anterior, la mayoría de los autores consultados Pompeya, V. E. (2008); Martí, J. A. (2009); González, M. y Spenger, I. (2010); Guevara, J. (2014) coinciden en que la modalidad B-learning constituye un modelo educativo donde se combina la enseñanza presencial o tradicional con la enseñanza virtual, haciendo uso de las TIC.

Según estos autores, ello se debe a la necesidad de cambiar la forma de pensar y de incorporar nuevas ideas que ubiquen al aprendiz como responsable de su autonomía intelectual en la gestión del conocimiento que necesita para construir su aprendizaje.

Lo anterior exige la determinación de qué contenidos o parte de un curso ha de ser presencial y cual parte virtual; qué sección debe ser de autoaprendizaje y cuál tutorada; qué parte sincrónica y qué parte asincrónica, qué papel debe jugar el profesor o facilitador presencial y el profesor o tutor virtual, así como la selección de las tecnologías que servirán de base para la elaboración y acceso a los recursos o materiales didácticos de apoyo a las actividades de enseñanza y aprendizaje.

En ese orden de ideas, González, M., y Spenger, I. (2010); Bauta, R. M. (2011), plantean que para poner en marcha una eficiente utilización de la modalidad B-learning, se necesita integrar estrategias, modelos y herramientas, tanto en lo virtual como en lo presencial, que varían en dependencia de cada necesidad específica y del modelo pedagógico adoptado, el cual deberá estar centrado en la actividad del estudiante. Concepciones que son asumidas totalmente en esta investigación.

En ese mismo orden de pensamiento, se tuvo en cuenta las exigencias del proceso pedagógico profesional que responde al modelo pedagógico destinado a la formación del técnico medio u obrero calificado desde los Institutos Politécnicos en Cuba el cual constituye el proceso de educación como respuesta a una demanda social, que tiene lugar bajo las condiciones de una institución docente y la empresa para la formación y preparación de un profesional competente.

Dicho proceso determina, además, el modo de actuación profesional de este personal de la educación. Hay que destacar que el desempeño de este docente, no sólo se lleva a cabo desde la institución educativa donde labora, sino también desde las entidades de la producción y los servicios de la provincia Guantánamo, para acompañar a

los estudiantes en la formación y desarrollo de habilidades profesionales, ya sea a través de clases prácticas o mediante las actividades de inserción laboral.

Tal situación se pone de manifiesto durante todo el curso escolar, lo cual obstaculiza la sistematicidad en la asistencia de los docentes a las actividades de preparación planificadas y desarrolladas desde el ámbito de su centro de trabajo y en otros niveles de dirección de la ETP en la provincia Guantánamo.

Lo anterior condicionó la selección de la modalidad B-learning como alternativa para perfeccionar la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”.

Port tal razón, la alternativa metodológica B-learning tiene como finalidad crear las condiciones básicas para garantizar la preparación en seguridad informática de los docentes del Politécnico Julio Antonio Delgado Reyes atendiendo a las características puestas de manifiesto desde el proceso pedagógico profesional y así poder realizar un uso eficiente y seguro de las TIC existentes en dicha entidad educativa.

Precisamente la alternativa metodológica B-learning propuesta, se compone de tres fases las cuales constituyen actividades concatenadas entre sí a través de cuya ejecución se puede constatar un sistema de acciones y operaciones que definen las vías o métodos que determinan la instrumentación de la dirección de la preparación en seguridad informática de los docentes.

A su vez, cada fase persigue una meta conscientemente planificada que dependerá no sólo de las vías o métodos a utilizar sino también de los medios, instrumentos y condiciones en que se emplearán, considerando además que para la ejecución de estas fases derivadas en acción se necesita haber comprendido previamente con qué objetivo se van a realizar, en qué consisten, cómo hay que ejecutarlas, cuáles son los procedimientos a seguir, en qué condiciones se deben utilizar, qué recursos se van a emplear, constituyendo todo esto una guía de orientación para su posterior ejecución y control.

De igual modo en esta investigación para llevar a cabo la elaboración del programa de preparación, se toma como premisa la determinación de las unidades didácticas o temas como vía fundamental para organizar los contenidos en seguridad informática destinados a la preparación de los docentes del Politécnico “Julio Antonio Delgado Reyes”.

Es por ello que las unidades didácticas constituyen una representación de trabajo articulado que contiene la planificación de las situaciones de enseñanza y aprendizaje alrededor de un elemento de contenido que se convierte en eje integrador aportando consistencia y significatividad a las acciones de preparación en seguridad informática desarrollar.

En correspondencia, las unidades didácticas dan respuesta a todas las cuestiones curriculares en relación con la descripción, objetivos didácticos, contenidos, actividades, recursos materiales, organización del espacio y el tiempo y la evaluación.

En la descripción se puntualiza el tema o nombre de la unidad, los contenidos previos que debe poseer el estudiante, así como las actividades de motivación para el desarrollo de los mismos.

En los objetivos didácticos se expresa cuál es la parte del contenido que se necesita que el alumno adquiera durante el desarrollo de la unidad didáctica.

Los contenidos, están representados por los objetos de aprendizajes (learning - objects) necesarios, con los cuales interactuará el aprendiz, incluyéndose entre otros aspectos: conceptos, definiciones, procedimientos, etc.

Las secuencias de actividades, establecen el conjunto de acciones y operaciones interrelacionadas que se ajustarán en consecuencia con las necesidades existentes; en los recursos materiales se identificarán los materiales básicos y complementarios que contribuirán al desarrollo de la unidad.

Por otro lado, en lo que respecta a la organización del espacio y el tiempo se preverá todo lo concerniente a su planificación para el desarrollo de los contenidos y por último la evaluación definirá las actividades y vías que se instrumentarán para valorar los niveles de desarrollo alcanzados por los aprendices.

En tanto las unidades didácticas están integradas, además, por objetos de aprendizajes, que constituyen la parte más pequeña de un curso, suelen además dar respuesta a las preguntas: qué, para qué, cómo y dónde; además su conformación presenta tres elementos básicos, estando en correspondencia los criterios de Valdés, M. (2012):

Contenidos: los cuales transmiten información como: datos, conceptos, leyes, principios, procedimientos, procesos complejos, valores y normas.

Interactividad: orientada al trabajo de los aprendices hacia el cumplimiento de los objetivos que se pretenden alcanzar a través de diversas actividades de aprendizaje integradas por:

Actividades sencillas que suelen contener preguntas y ejercicios para su posterior ejecución y corrección respondiendo a un único objetivo.

Actividades complejas caracterizadas por una mayor duración y requieren la división en formas secuenciales dirigidas al cumplimiento de más de un objetivo formativo desde el trabajo grupal o individual.

Evaluación: la cual se realiza mediante contenidos que tienen como finalidad principal evaluar el nivel alcanzado por los estudiantes respecto a la adquisición de los conocimientos.

2.2. Estructura de la alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes"

La estructura de la alternativa metodológica B-learning, se conforma tomando como premisas tres fases fundamentales, las cuales en su conjunto tienen como finalidad la dirección de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes".

Dicha estructura presenta un carácter de sistema, donde se destaca la funcionabilidad de cada una de sus partes existiendo una relación de coordinación, subordinación e interdependencia entre las mismas, desde las que se determinarán las peculiaridades de las acciones a desarrollar para la preparación en seguridad informática de los docentes, tomando como punto de partida la articulación entre lo político e ideológico, lo pedagógico, lo organizativo y lo tecnológico.

Desde esta perspectiva y a partir de la valoración realizada, se asumen los rasgos a tenerse en la dirección de la preparación de docentes tales como:

- Poseer objetivos precisos que estén en correspondencia con las potencialidades y necesidades detectadas en el diagnóstico inicial.
- Revelar flexibilidad ante los cambios que van surgiendo en el uso de las TIC en relación a las demandas sociales y las condiciones de la entidad educativa.
- Facilitar la participación de todos los factores y actores implicados desde la concepción, ejecución y evaluación.
- Poseer una estructura organizativa que muestre una lógica para la puesta en marcha en la práctica, estableciéndose un sistema de acciones estructuradas por fases, etapas o momentos muy estrechamente relacionados entre sí y funcionar de forma armónica.
- Debe avizorarse desde su concepción el liderazgo coordinado y comprometido entre todos los factores de la entidad educativa.

A partir de ello, la primera fase se titula "Concepción de la preparación en seguridad informática". Esta tiene como finalidad llevar acabo las acciones de planificación y organización que permitan crear las condiciones necesarias para el desarrollo exitoso de la preparación.

Para ello, se necesita el establecimiento de vínculos no sólo entre los sujetos participantes y protagonistas de la preparación en seguridad informática sino también con los demás factores responsables de la dirección del proceso pedagógico profesional desde el Politécnico "Julio Antonio Delgado Reyes".

A consideración del autor de esta tesis, lo planteado con anterioridad es de gran importancia por cuanto se trata de poner de manifiesto las acciones de preparación no de forma aislada, sino a partir de las planificación anual, mensual e individual de la institución educativa, con lo que se propicia el establecimiento de relaciones sistémicas de coordinación y cooperación para la toma de conciencia de las necesidades y de las metas a alcanzar.

En este mismo sentido, en la fase número uno se analizará:

- La pertinencia de las necesidades de preparación en seguridad informática de los docentes.
- La determinación de los protagonistas de dicha preparación.
- La selección de la fecha de inicio y culminación de la misma.
- Los posibles recursos materiales a utilizar.
- Los aspectos tenidos en cuenta en la elaboración del programa de preparación, así como en el diseño de sus respectivas unidades didácticas, valorando cuáles se van a impartir de forma presencial y cuáles de forma no presencial.
- La selección del EVEA a utilizar.

Todo ello sobre la base, de los objetivos trazados, de los contenidos en seguridad informática a tratar, del papel a desempeñar por los aprendices, el grupo y el equipo docente, para los cual se necesita:

Modelar el sistema de actividades y tareas de enseñanza y aprendizaje, a través de las cuales se desarrollará la preparación en seguridad informática, tomando en consideración las particularidades de los servicios, herramientas de actividad y comunicación tales como: foro, Wiki, chat, cuestionarios, talleres, consultas, etc., que ofrece el entorno virtual y su relación con los encuentros presenciales.

La selección del sistema de materiales didácticos a elaborar atendiendo a las potencialidades pedagógicas y tecnológicas que poseen, favoreciendo la flexibilidad en el manejo del espacio y el tiempo superando la barrera de los horarios rígidos, brindando al aprendiz la posibilidad de acceder al contenido y a las diferentes actividades de enseñanza aprendizaje de forma dinámica en correspondencia con sus propias necesidades.

Determinar las formas de organización a emplearse tanto de forma presencial como no presencial, así como los métodos, medios, procedimientos y formas de evaluación y control, acordes con las condiciones generales y específicas del contexto donde se desarrollarán las acciones de preparación en seguridad informática.

De esta manera se tiene en cuenta en el diseño de las actividades de enseñanza – aprendizaje para la preparación en seguridad informática de los docentes no sólo los aspectos didácticos sino también los tecnológicos, reconociendo además las diferencias que existen entre estos dos aspectos.

Atendiendo a los aspectos antes planteados, se aprecia cómo se ha cumplido con los referentes asumidos en el capítulo número uno, dándole salida a la concepción a tener en cuenta en la elaboración de un curso donde se empleen los EVEA.

La fase número dos: "Fase de instrumentación de la preparación en seguridad informática", tiene como finalidad implementar las actividades de preparación en seguridad informática concebidas en la fase anterior.

En este sentido, la implementación de las acciones de preparación en seguridad informática, se propone que se realicen desde las condiciones del Politécnico "Julio Antonio Delgado Reyes" dándole salida a través de los espacios destinados a la preparación de los docentes desde las actividades de reciclaje.

Se propone además que las cuatros primeras unidades didácticas se desarrollen en las ocho primeras semanas del curso escolar en un total de 36 horas, 32 horas destinadas al autoaprendizaje en relación al estudio de los contenidos previstos en la unidad uno, dos y tres desde EVEA y las cuatro horas restantes a los contenidos a desarrollarse desde encuentros presenciales empleando el espacio para el control de las actividades de reciclaje prevista desde la entidad educativa y a desarrollarse los segundos sábados laborables de cada mes.

De esta misma forma, y desde las próximas ocho semanas se realizarán las actividades de preparación en seguridad informática concebidas desde la unidad cinco a la ocho, para un tiempo total de duración de 72 horas.

Se hace necesario además, utilizar el plan de capacitación y desarrollo como documento rector que facilita dar tratamiento a las necesidades de preparación de los docentes durante un curso escolar, teniéndose la oportunidad de planificar y establecer de forma flexible los momentos que éste empleará para acceder y participar en las actividades de preparación en seguridad informática de forma presencial y desde EVEA.

Lo anterior tiene su sustento en las premisas y las condiciones del proceso pedagógico profesional que se gesta desde esta entidad educativa. Ello puede determinar además, el modo de actuación profesional de este personal de la educación, tal como se había explicado con anterioridad.

En esta misma dirección, la estructuración de los contenidos en seguridad informática para la preparación de los docentes, se organizará desde la propia concepción del programa de preparación mediante la determinación de diferentes unidades didácticas.

Por esta razón, las unidades didácticas estarán compuestas por unidades didácticas de preparación básica y unidades didácticas de preparación complementaria, las de preparación básica estarán dirigidas al desarrollo de

actividades de familiarización, colaboración y reflexión sobre temas de seguridad informática y las de preparación complementaria a la contextualización de los contenidos en seguridad informática a las condiciones reales y concretas de la entidad educativa.

En ese orden, las unidades didácticas quedarán estructuradas según se ilustra en el siguiente esquema:

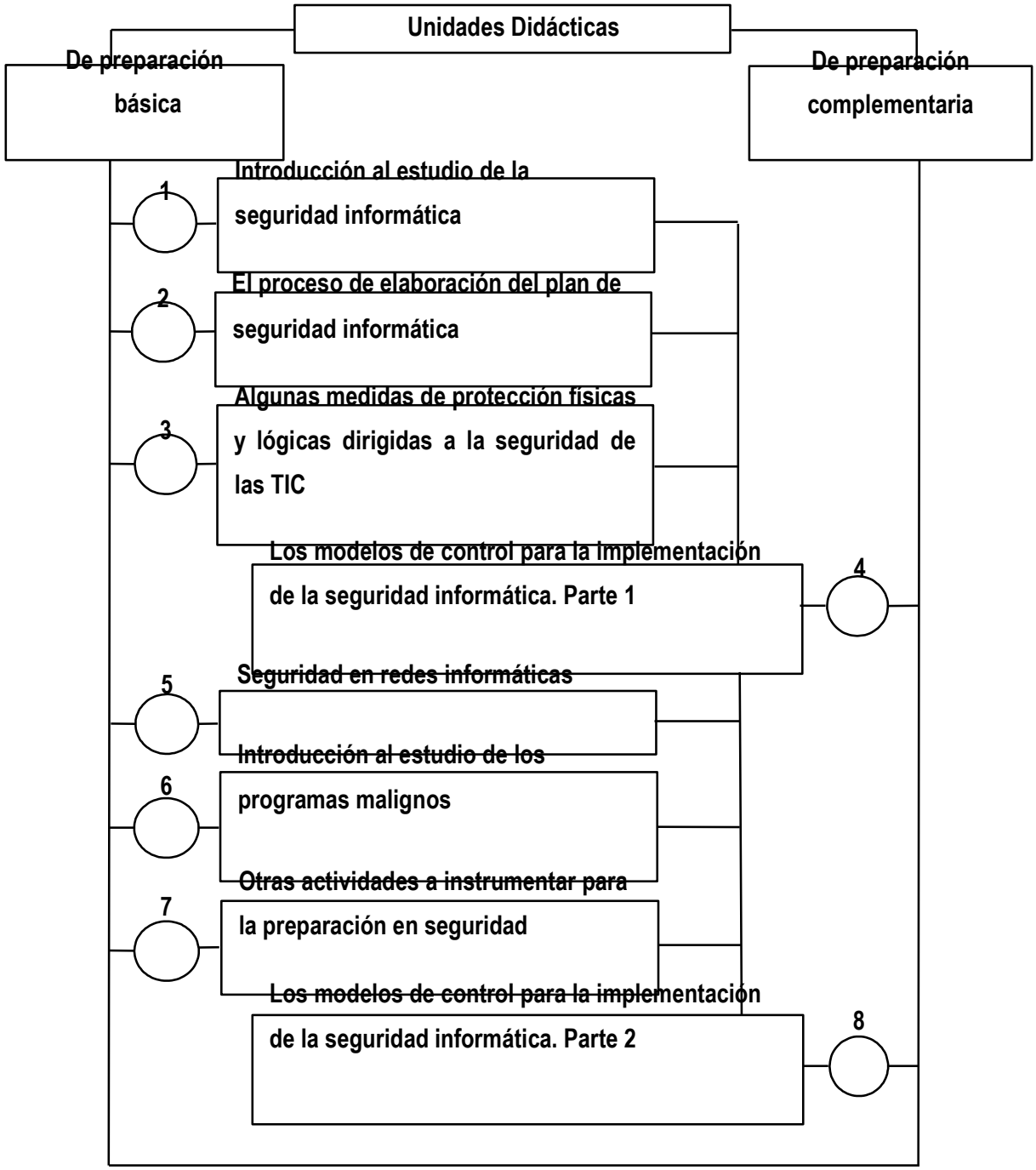

Figura 1: Estructura de las unidades didácticas.

Contenidos que forman parte de la estructuración de cada una de las unidades didácticas.

Unidad 1: Introducción al estudio de la seguridad informática.

Objetivo: Caracterizar el concepto de seguridad informática, seguridad de la información y sistema informático, haciendo énfasis en las legislaciones y contenidos relacionados con la seguridad informática en Cuba y a nivel internacional.

Sistema de conocimientos

Concepto de seguridad informática, de seguridad de la información y de sistema informático. Estudio de las legislaciones cubanas relacionadas con la seguridad informática.

Unidad 2: El proceso de elaboración del plan de seguridad informática.

Objetivo: Explicar los aspectos a tener en cuenta en la elaboración del Plan de Seguridad Informática, a través del estudio de las metodologías destinadas para su creación.

Sistema de conocimientos

El plan de seguridad informática. Metodología para su elaboración. Importancia de la realización e implementación del análisis de riesgos y del código de ética para el uso de las TIC desde las entidades educativas cubanas.

Unidad 3: Algunas medidas de protección físicas y lógicas dirigidas a la seguridad de las TIC.

Objetivo: Valorar la importancia de la implementación de las políticas de protección físicas y lógicas para la protección de los bienes informáticos y de comunicaciones.

Sistema de conocimientos

Los sistemas de tierra física, contra fluctuaciones eléctricas y de alarma contra incendios e intrusos. La información contenida en fuentes digitales e impresas, principios para su seguridad y conservación. El uso de memorias flash USB. Introducción al mantenimiento de las TIC existentes en la entidad educativa.

Unidad 4: Los modelos de control para la implementación de la seguridad informática. Parte 1.

Objetivo: Identificar y evaluar las debilidades, riesgos y vulnerabilidades existentes en la entidad educativa mediante la implementación de los modelos de control de la seguridad informática.

Sistema de conocimientos

Estudio de las medidas de control de la seguridad informática: libro de incidencias, modelo de control usuario de las TIC, modelo de control memorias USB, aspectos a tener en cuenta para el control del sistema de tierra física.

Unidad 5: Seguridad en redes informáticas.

Objetivo: Valorar la necesidad del uso responsable de las redes informáticas mediante el estudio de los aspectos vinculados con el diseño de redes informáticas, el empleo de firewall, de las políticas de seguridad a implementarse en servidores de redes informáticas, la utilización del correo electrónico, las redes sociales de comunicación, la actualización de sistemas operativos, así como contrarrestar los efectos de las técnicas de ingeniería social.

Sistema de conocimientos

Concepto de red informática. El diseño de redes informáticas (Proyecto de red informática). El uso de firewall para proteger las redes informáticas. Políticas de seguridad a implementarse en los servidores de redes informáticas. Recomendaciones para el uso del correo electrónico. Medidas a tener en cuenta para el uso seguro de las redes sociales de comunicación. Importancia de la actualización de los sistemas operativos. Medidas para contrarrestar los efectos de las técnicas de ingeniería social.

Unidad 6: Introducción al estudio de los programas malignos.

Objetivos: Caracterizar los conceptos de programas malignos, virus informáticos, a través de los aspectos más esenciales que los identifican.

Valorar la importancia de protegerse de los virus informáticos y otros programas malignos para minimizar los riesgos de contaminación y sus posibles efectos colaterales.

Sistema de conocimientos

Concepto de programas malignos y de virus informáticos. Daños que ocasionan los virus, estrategias y métodos de contaminación. Acciones a ejecutar en caso de infección por virus informático. Medidas de seguridad para no infectarse. Uso de programas antivirus. Sistemas Operativos resistentes y sistemas débiles ante el ataque de programas malignos.

Unidad 7: Otras actividades a instrumentar para la preparación en seguridad informática.

Objetivos: Explicar la necesidad de realización de la salva de información, de auditorías informáticas y la disminución de riesgos asociados con la pérdida de información o de bienes informáticos o de comunicaciones.

Caracterizar el concepto de equipos móviles de cómputo y explicar la importancia de su control desde las entidades educativas.

Valorar la necesidad de implementar medidas que garanticen la seguridad y salud ante el trabajo y su relación con la seguridad informática.

Sistema de conocimientos

La salva de la información, responsabilidad de los usuarios. Las auditorías informáticas, propuesta de guía para su ejecución. El uso de equipos móviles de cómputo desde las entidades educativas. Sugerencias para la implementación de medidas de seguridad y salud ante el trabajo y su relación con la seguridad informática.

Unidad 8: Los modelos de control para la implementación de la seguridad informática. Parte 2.

Objetivo: Identificar y evaluar las debilidades, riesgos y vulnerabilidades existentes en la entidad educativa por medio de la implementación de los modelos de control de la seguridad informática.

Sistema de conocimientos

Estudio de las medidas de control de la seguridad informática: modelo registro de sistemas operativos, modelo para el control de usuarios con acceso al correo electrónico, modelo de control salva de la información, de las auditorías informáticas, de equipos móviles de cómputo. Cumplimiento de las medidas de seguridad y salud ante el trabajo a tener en cuenta al interactuar con las TIC.

Por otro lado, se hace necesario destacar que las condiciones y potencialidades tecnológicas de los EVEA que por sí solas no contribuyen al logro de la calidad de la preparación en seguridad informática bajo estas condiciones, de ahí la necesidad de convertirlas en potencialidades pedagógicas.

Desde el punto de vista del autor de esta tesis, lo expresado se puede lograr a partir de la estructuración y la eficiente orientación pedagógica de las tareas de aprendizaje en estrecha relación con los diferentes objetos de aprendizaje que incluyen el empleo de las herramientas para la actividad y comunicación disponibles, sólo así se pondrá de manifiesto la flexibilidad, la motivación, el trabajo colaborativo, el aprendizaje significativo, la atención a las diferencias individuales, entre otros aspectos.

En esta misma dirección, si bien los EVEA facilitarán la adquisición de los conocimientos mediante el tratamiento de los diferentes conceptos y la elaboración de procedimientos en seguridad informática, la realización de actividades presenciales servirán como medio para reforzar todo lo aprendido no de forma aislada sino como un eslabón más de la preparación iniciada en los EVEA.

De esta manera, el aprendizaje adquiere un sentido especial y una connotación trascendental para las personas involucradas, al poder aplicar los nuevos conocimientos en su entorno laboral y en situaciones reales al reconocer además el origen, esencia y naturaleza de los problemas vinculados con la seguridad informática.

Brindando la posibilidad a los docentes de participar en las acciones de preparación en seguridad informática, así como en las tareas cotidianas aledañas a su desempeño profesional.

Sin embargo, el valor de esta idea no sólo depende de lo planteado con anterioridad sino de los diferentes niveles de ayuda que el profesor, tutor o moderador sean capaces de establecer en la estructuración de los contenidos en seguridad informática.

Al considerar los aspectos señalados, se crean espacios de coordinación y orientación sistemática para el debate y la reflexión por parte del profesor, tutor, moderador, estudiantes o el grupo, en cuanto a la aplicación de los conocimientos derivados de la preparación en seguridad informática que serán adquiridos paulatinamente, dando posibilidad al intercambio con especialistas de otras instituciones educativas y de la producción y los servicios.
Tal reflexión se corresponde con los aspectos tenidos en cuenta para la implementación de la alternativa metodológica B-learning propuestas basada en tres aspectos fundamentales*:*

- Conocimiento de las características esenciales del contexto donde será implementada.
- El uso de herramientas e-learning cuyo diseño sea capaz de soportar las condiciones del contexto seleccionado.
- Contar con el apoyo de profesionales para contemplar y optimizar la alternativa propuesta.

Desde este punto de vista, se seleccionó como vía fundamental para llevar a cabo la estructuración de la preparación en seguridad informática de los docentes, la plataforma Moodle, la cual fue diseñada por Martin Dougiamas en la década de los años noventa, esta plataforma se sustenta según su creador en las ideas del constructivismo social, potenciando el trabajo grupal y el aprendizaje colaborativo.

Moodle, significa en inglés (Modular Object - Oriented Dynamic Learning Environment) y en español (Entorno Modular de Aprendizaje Dinámico Orientado a Objetos). Esta puede ser utilizada desde diferentes sistemas operativos como: Windows, Linux, Unix, etc., siempre y cuando soporten tecnologías para el trabajo en la web como Apache, PHP, y una base de datos MySQL, entre otros.

La utilización de esta plataforma ha sido muy difundida en todo el mundo incluyendo Cuba para el desarrollo de cursos a distancia debido a las grandes posibilidades que brinda tales como:

❖ Es una plataforma de distribución libre, debido a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar y modificarla para ser implementada desde otras condiciones.

❖ Presenta una interfaz sencilla atendiendo a una concepción modular que brinda flexibilidad para insertar y cambiar sus diferentes componentes.

❖ A través de esta, se combinan diferentes materiales didácticos en variados formatos tales como: la multimedia: texto, imágenes, animación, sonido y video, etc., así como la estructuración no lineal de la información.

❖ En los cursos montados bajo esta plataforma se pueden combinar elementos en línea (online) y fuera de esta (offline) respaldados en variadas formas de comunicación ya sea sincrónica y asincrónica teniendo presente además la ejecución de encuentros presenciales.

❖ Favorece la creación de espacios para la realización de consultas, plantear inquietudes, dudas a partir de la interacción entre los estudiantes, docentes y grupo, promoviendo el intercambio, la colaboración, el trabajo en grupo con vista a la adquisición de los nuevos conocimientos.

❖ Le ofrece al docente un registro completo con informaciones sobre las actividades que van realizando los estudiantes al interactuar con la plataforma facilitando los procesos de control y evaluación.

❖ Está disponible en varios idiomas y versiones mejorando su rendimiento y empleo desde cualquier parte del mundo.

Por otro lado, para el diseño didáctico del curso para la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", se tuvo en cuenta aunque adaptados a las condiciones y preparación de los docentes antes mencionado otros elementos con vista a la organización de los materiales y las diferentes actividades de comunicación.

Se propone que el inicio de la preparación, se realice mediante las herramientas de actividad y comunicación creadas desde la plataforma Moodle, para ello, los profesores utilizando el correo electrónico informarán a los aprendices matriculados la fecha de inicio y orientarán los aspectos básicos a tener en cuenta tales como: participar en las diferentes actividades, leer las orientaciones, las guías de estudio emitidas, el programa de preparación en seguridad informática, plantear dudas, sugerencias mediante los espacios de reflexión y colaboración implementados.

Desde los bloques de implementación se le indicará al aprendiz la necesidad de iniciar su participación dando lectura primeramente a la guía de estudio para así informarse de los objetivos a alcanzar, las tareas a desarrollar y las formas de evaluación que se utilizarán.

En este sentido, desde el bloque inicial del curso de preparación en seguridad informática se ofrecen las orientaciones preliminares para dar comienzo a las actividades de aprendizaje mezclándose diversas herramientas para la actividad y la comunicación que posee la plataforma Moodle, a continuación se muestran los aspectos seleccionados para este fin:

❖ Presentación: se ejecuta a través de una actividad de foro, dándole la bienvenida a los aprendices así como motivarlos a insertar sus expectativas y solicitándole insertar sus datos personales para el llenado de su perfil como usuarios del curso de preparación en seguridad informática.

❖ Novedades: constituye un foro para la comunicación creado para ofrecerle a los aprendices lo novedoso del curso, al darle informaciones que provoquen una serie de sensaciones e incertidumbres estimulando la necesidad y búsqueda de nuevos conocimientos relacionados con la seguridad informática.

❖ Orientaciones preliminares para la realización de las actividades de aprendizaje: como su nombre lo indica es la guía preliminar con la que cuentan los participantes de la preparación en seguridad informática, en esta se muestra una vez más la importancia del curso, la modalidad que se empleará, cómo se ejecutarán las tareas de aprendizaje, cómo se puede acceder y obtener las informaciones desde la plataforma seleccionada, las formas de evaluación, los requisitos necesarios para matricular en el curso, el objetivo general del mismo y sugerencias para el uso de algunas herramientas de actividad y comunicación.

❖ Programa general del curso: brinda informaciones generales como la fundamentación del curso, objetivos generales y específicos, organización de las unidades didácticas con sus respectivos sistemas de conocimientos, el sistema de habilidades a desarrollar, los valores a los que se tributa, el sistema de evaluación, sugerencias metodológicas, las bibliografías básicas y complementarias, entre otros aspectos.

❖ Glosario de términos: constituye una actividad de carácter general, desde la cual los protagonistas de la preparación en seguridad informática, tienen la posibilidad de insertar conceptos, definiciones elaboradas por estos o sencillamente derivadas de las actividades de estudio.

❖ Actividad de comunicación para la familiarización de los aprendices con la estructura del curso: esta actividad devenida en un chat para familiarizar a los participantes con la interfaz de comunicación de la plataforma Moodle, así como un medio de intercambio y ayuda según lo tratado en las actividades iniciales del curso.

❖ Diagnóstico inicial: presenta la secuencia de preguntas para determinar el nivel de preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes” lo cual contribuye a la estructuración de los contenidos y de los niveles de ayudas necesarios.

❖ Actividad de comunicación para la socialización y orientación sistemática**:** constituye un espacio de preparación, socialización y orientación sistemática para ser utilizado durante las acciones de preparación en seguridad informática, desde este contexto todos los participantes del curso podrán insertar informaciones novedosas que obtengan al interactuar con los contenidos del curso, visitando otros sitios web o a través del intercambio con especialistas en seguridad informática.

Por medio de las siguientes figuras se muestra la interfaz de la plataforma Moodle y los aspectos tenidos en cuenta en el inicio del curso de preparación en seguridad informática:

Figura 2. Interfaz plataforma Moodle.

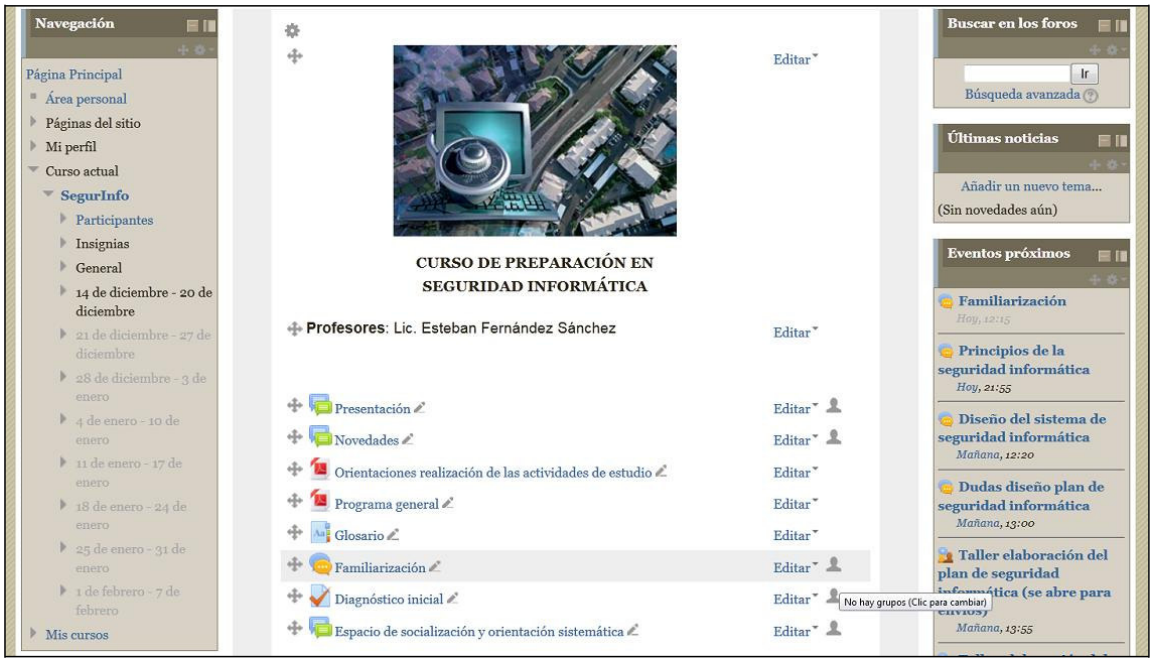

Figura 3. Interfaz inicial curso seguridad informática.

Para el desarrollo de los bloques para la instrumentación de las actividades de aprendizaje, fueron tomados en cuenta los referentes considerados en el capítulo uno de esta investigación, desde esta perspectiva se utilizan diferentes indicadores del diseño didáctico de cursos para la preparación a distancia de docentes en entornos virtuales. Los cuales constituyen una guía de orientación para la estructuración de los contenidos en seguridad informática bajo estas condiciones, dentro de estos indicadores se muestran:

1. Los concernientes al rol del profesor*:* desde este contexto el profesor constituye el ente socializador que está presente y accesible empleando las diferentes vías de actividad y comunicación existentes, tales como el foro, el

chat, wiki, el taller etc., con vista a orientar la búsqueda del nuevo conocimiento devenido de los aspectos básicos y esenciales de la seguridad informática, brindando atención individualizada y promoviendo el aprendizaje grupal de los aprendices.

2. Los concernientes al rol del estudiante: dirigida a la participación consciente, activa, y creadora de los mismos, tratando de lograr la motivación hacia los nuevos contenidos de seguridad informática vinculando las actividades de aprendizaje con situaciones reales del contexto donde se desarrolla.

Para ello debe transitar por situaciones de aprendizaje que van desde lo particular a lo general (vía inductiva) o desde lo general a lo particular (vía deductiva), haciéndose necesario una revisión detallada de los materiales didácticos que se les brinda para el cumplimiento de los objetivos planificados.

Se enfatiza en el tratamiento de los diferentes conceptos y elaboración de procedimientos de seguridad informática a través de la realización de las diversas tareas de aprendizaje, se debe hacer una descripción e identificación de sus características esenciales teniendo en cuanta las experiencias previas y desarrollo alcanzado por los participantes en el curso de preparación en seguridad informática según el resultado del diagnóstico inicial, dándole la posibilidad a estos de exponer sus criterios, hacer valoraciones críticas e insertar nuevas ideas desde las herramientas de actividad y comunicación de la plataforma Moodle, según las conclusiones a las cuales llegaban.

De esta misma forma, fue necesario diseñar espacios de socialización y orientación sistemática ya sea para tratar temas generales o particulares de cada unidad de aprendizaje desde los cuales los aprendices pudieran introducir inquietudes, dudas o sencillamente aportar criterios, informaciones, sugerencias y aportes a problemas vinculados con las temáticas estudiadas, promoviendo la independencia cognoscitiva y estimular el desarrollo del valor responsabilidad.

3. Los concernientes al rol del grupo**:** para el trabajo en grupo, se emplearon como formas organizativas fundamentales el taller, seminario, el debate y determinadas herramientas de actividad y comunicación que posee la plataforma seleccionada.

Dentro de las herramientas de actividad y comunicación seleccionada para el trabajo colaborativo y socialización grupal se empleó el foro, el cual constituye una herramienta de comunicación asíncrona que permite originar conversaciones o debates en tiempo diferido sobre temas de seguridad informática de interés común.

Esta herramienta facilita el desarrollo de actividades tales como talleres y seminarios y de esta manera el que aprende tiene la posibilidad de acceder, buscar y reflexionar sobre la información pertinente en función de poder emitir su criterio, aspecto que se asume en esta investigación.

En tal sentido, a los aprendices se les posibilitó desde los foros insertados como actividad de trabajo grupal observar los nuevos temas añadidos por otros compañeros del grupo, de esta forma se generan debates, reflexiones grupales, se aportan ideas, y sobre todo se garantiza que cada uno de los miembros del grupo se sientan acompañados y orientados en la búsqueda de los nuevos conocimientos.

Otras herramientas utilizadas para el trabajo grupal fue el wiki y taller, que si bien para su realización desde entornos virtuales en especial la plataforma Moodle se hace necesaria la implicación individual de los estudiantes, el resultado final puede ser socializado con los demás miembros del grupo y así emitir una evaluación y solución colectiva ante las tareas de aprendizajes planteadas.

Ejemplo de lo anterior lo constituye el taller creado desde la plataforma Moodle con vista a la elaboración de un plan de seguridad informática por cada miembro del grupo luego de haber revisado y estudiado cada uno de los materiales de estudio incluyendo metodologías para su creación y el análisis de riesgos de seguridad informática, debiendo subir el trabajo realizado y entre todos valorar el resultado final emitiendo sus opiniones y un criterio de evaluación final.

Las acciones de preparación en seguridad informática realizadas a partir del taller antes mencionado, se complementa con el desarrollo de encuentros presenciales, que si bien se sale de este entorno, el estudiante tiene la posibilidad de continuar accediendo a las diferentes herramientas de actividad y comunicación.

Por tal razón desde el entorno virtual, primero se tratan los conceptos relacionados con la elaboración del plan de seguridad informática para el caso que se analiza, luego se determina la sucesión de indicaciones con vista a dar salida a cada paso para garantizar la realización de este documento y luego se fija y evalúa el resultado alcanzado desde el encuentro presencial.

El chat de igual forma fue otras de las herramientas utilizadas para el trabajo grupal, que genera además acciones de intercambio, colaboración para alcanzar metas comunes, facilitando la realización de ayudas, consultas, el esclarecimiento de dudas e inquietudes simultáneamente en tiempo real.

En el curso desde Moodle se puede acceder a un conjunto de sesiones de chat con diferentes objetivos que van desde la familiarización de los participantes con las actividades de aprendizaje y la interfaz del curso así como para establecer niveles de ayuda y análisis de temas derivados de los contenidos en seguridad informática.

Puntualizar que, aun cuando esta actividad se realiza de manera simultánea y en tiempo real, siempre estuvo vinculada a una actividad de estudio anterior (tarea) que debió realizar cada miembro del grupo. De ahí que el chat se utilizara para el desarrollo de los contenidos de seguridad informática por los cuales transitaban los aprendices paulatinamente y para la atención diferenciada con ayuda de los demás participantes.

Es importante destacar que tanto para el uso de los foros como del chat, al inicio del curso en el documento titulado “Orientaciones para la realización de las actividades de estudio” se ofrecen sugerencias para establecer una buena comunicación al emplear las mismas, de esta manera se fomenta los buenos valores, formas de comunicación y de cortesía entre los protagonistas de la preparación en seguridad informática.

4. Los concernientes a los objetivos y al contenido de enseñanza - aprendizaje: lo analizado hasta el momento en esta tesis se sustenta en la correcta determinación de los objetivos y de los contenidos de aprendizaje, los primeros se orientan desde el inicio del curso a través del programa general de preparación en seguridad informática y desde cada unidad didáctica, con vista a que los implicados en las acciones de preparación conozcan la esencia del conocimiento que deben adquirir.

Para la determinación y orientación de los objetivos se prevé como aspecto fundamental la presencia de la habilidad a desarrollar, el nivel de profundidad de los contenidos y el nivel de asimilación con que se tratarán los mismos, tales como la familiarización y la aplicación de los conocimientos, así como la intencionalidad política según lo requiera.

La selección de los contenidos, fue realizada según los criterios aportados por los diferentes autores estudiados, aunque algunos de estos contenidos fueron previstos por el autor de esta tesis a partir del análisis de la guía de inspección que utilizan los especialistas de la Oficina de Seguridad de Redes Informática (OSRI) de Cuba y la experiencia de este autor desde el año 2011 al 2013 como administrador de red y responsable de seguridad informática en una de las empresas (PROVARI del MININT), en la provincia de Guantánamo.

Se tuvo presente además, que a través del programa de preparación en seguridad informática mostrar una adecuada organización y dosificación de los contenidos, estando en correspondencia con el tiempo que disponen los docentes que está muy ligado al modo de actuación profesional según las condiciones que genera el proceso pedagógico profesional que se implementa en el Politécnico “Julio Antonio Delgado Reyes” y su posterior aplicación a situaciones reales concretas que promuevan el uso eficiente, responsable y ético de las TIC.

5. Los concernientes a la calidad de los materiales didácticos en estrecha relación con otros recursos: desde este punto de vista, existe gran relación entre la selección de los contenidos en seguridad informática y la determinación de los materiales didácticos empleados para su distribución, evaluación y control.

El acceso a los materiales didácticos se puede hacer, desde la plataforma Moodle mediante las carpetas materiales básicos o complementarios creada para este fin y disponible en cada una de las unidades didácticas del curso de preparación en seguridad informática.

En la de materiales básicos, se hallan los objetos de aprendizaje esenciales a los cuales deben acceder los aprendices para gestionar los contenidos en seguridad informática y en la de materiales complementarios se encuentran los recursos de apoyo y de profundización de los conocimientos que irán alcanzando los participantes en la preparación en seguridad informática.

Estos materiales, fueron seleccionados teniendo en cuenta tanto su actualidad en relación a los nuevos avances derivados del desarrollo y uso de las TIC los cuales provocan la necesidad de implementar nuevas vías para la protección y seguridad de estas así como la posibilidad de accesibilidad de los usuarios del curso de preparación en seguridad informática a las mismas.

Es por ello, que se pueden encontrar materiales en varios formatos como documentos Word, PDF, así como imágenes, videos y materiales multimedia confeccionados en flash que muestran eventualidades vinculadas con la seguridad informática, los cuales pueden ser descargados para ser utilizados desde otros contextos.

Destacar la presencia de otros materiales que si bien no ofrecen acceso directo a los contenidos de aprendizaje, si facilitan la orientación para la realización y evaluación de estos, ejemplo de ello lo constituyen las guías de estudio que son documentos que brindan sugerencias a los aprendices para que accedan de manera más fácil a los contenidos en seguridad informática.

Para la elaboración de las guías de estudio se hizo énfasis en cuatro elementos fundamentales:

- Los objetivos que debe alcanzar el aprendiz redactados en forma clara y precisa.
- La determinación de los contenidos esenciales de cada unidad didáctica, desde el punto de vista conceptual y procedimental, integrando las acciones de enseñanza aprendizaje desde lo virtual con apoyo de lo presencial.
- EL empleo de un lenguaje, claro, accesible y utilizando el dialogo en la exposición de los contenidos, para propiciar una adecuada comunicación y lograr que el estudiante durante la lectura, sienta como si el profesor estuviera saliendo de la guía de estudio.

Destacar además, que desde la guía de estudio se facilita:

- ❖ La orientación hacia el autoaprendizaje.
- ❖ Motivar el estudio, favorecer la autonomía.
- ❖ Mantener la atención, despertar curiosidad científica.
- ❖ Facilitar el logro de los objetivos propuestos en el curso.
- ❖ Presentar la información adecuada y de forma amena.

- ❖ Propiciar la solución de problemas, la creatividad y el trabajo colaborativo.

Por otro lado, existen otros materiales que se integran como apoyo al desarrollo de la preparación en seguridad informática, los mismo se muestran en formato digital (videos) poniéndose de manifiesto la conferencia como forma de organización y otros en formato impreso (revistas y libros).

A estos se puede acceder desde el laboratorio de computación o desde la biblioteca del Politécnico "Julio Antonio Delgado Reyes"; todos estos materiales, se articulan tanto para su utilización desde EVEA como para los encuentros presenciales teniendo para estos últimos la clase práctica como forma de organización fundamental.

6. Los relacionados con la evaluación de los resultados alcanzados: en este sentido, la forma fundamental para la evaluación de los resultados alcanzados en la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes" es la sistemática vinculada con la realización de actividades para la autoevaluación.

De esa manera, desde el propio inicio del curso desde el entorno virtual seleccionado, se orientan las formas de evaluación que se implementarán, tomando como punto de partida el desempeño y participación de los protagonistas durante toda la preparación en seguridad informática al participar en las diferentes actividades planificadas.

En consecuencia, desde las guías de estudio de igual manera se especifica cómo se pondrá de manifiesto la actividad de evaluación, al proporcionarse sugerencias para que los aprendices puedan una vez terminada la unidad valoren los niveles de desarrollo alcanzados en materia de seguridad informática.

Para la realización de las evaluaciones, se emplearon situaciones reales o creadas por los profesores del curso de preparación en seguridad informática, lo cual genera debates, análisis críticos sustentado en la contradicciones que se dan respecto al uso seguro y ético de las TIC desde el Politécnico "Julio Antonio Delgado Reyes" estimulando el estudio y la búsqueda de información respecto a los temas de seguridad informática planteados.

En correspondencia, se llevó a cabo la creación de un banco de preguntas vinculadas con los contenidos tratados en cada unidad didáctica planificada, dentro de los tipos de preguntas creadas se encuentran preguntas de respuestas cortas desde las cuales el aprendiz responde empleando un pequeño número de palabras que son comparadas con respuestas matrices previamente creadas por el profesor.

Preguntas de verdadero o falso, donde se les solicita a los aprendices después de planteada una determinada situación escoger la respuesta correcta, aunque esta es un tipo de pregunta sencilla de opción múltiple, es

necesario desde el punto de vista de la preparación en seguridad informática que los aprendices realicen previamente un estudio de cada uno de los materiales orientados ya sea básicos o complementarios.

Preguntas de opción múltiple, desde las cuales se hace necesario sobre la base de varias opciones mostradas seleccionar una o varias en dependencia del objetivo para la cual fue programada la misma.

En todos los casos, las preguntas fueron proyectadas atendiendo a los siguientes contenidos: conceptuales al analizar los conceptos y definiciones de seguridad informática, procedimentales valorando los pasos, acciones a recurrir para dar solución a un problema vinculado con la seguridad informática y desde lo axiológico estimulando el análisis de formas de actuación donde se reflejen actitudes éticas y responsables en el uso de las TIC.

En general, otro aspecto que destaca la evaluación desde la plataforma Moodle es la utilización de los distintos registros de actividad y trazas a las cuales se puede acceder para constatar el nivel de participación de todos los usuarios en las actividades de preparación en seguridad informática, favoreciendo el seguimiento y atención a las diferencias individuales.

Lo anterior, se integra a las formas de estructurar los contenidos en seguridad informática desde encuentros presenciales si se tiene en cuenta que estos complementan los conocimientos adquiridos desde EVEA.

En las siguientes imágenes, se presentan ejemplos de varios tipos de preguntas diseñadas a partir de las posibilidades que brinda la plataforma de educación a distancia Moodle:

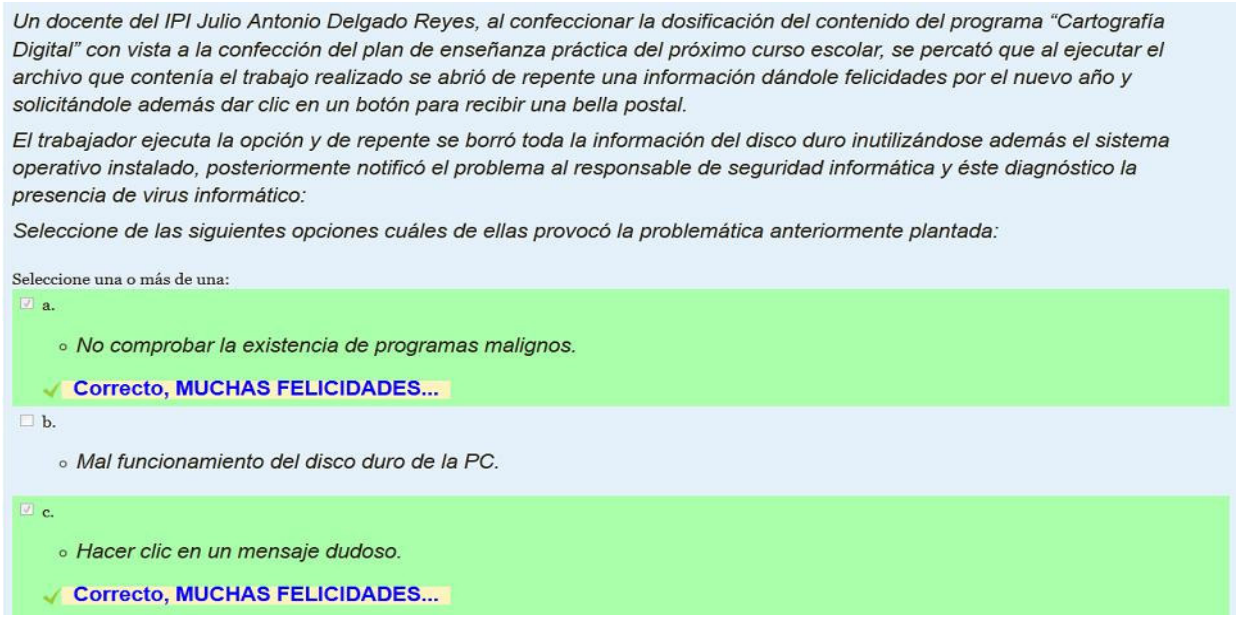

Figura 4. Ejemplo de pregunta de selección múltiple con retroalimentación.

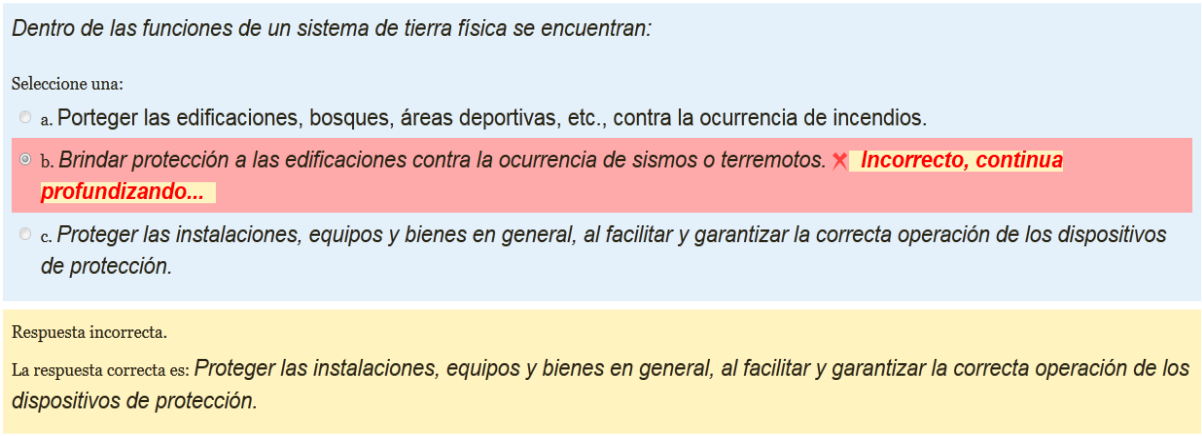

Figura 5. Ejemplo forma simple de pregunta de opción múltiple con retroalimentación.

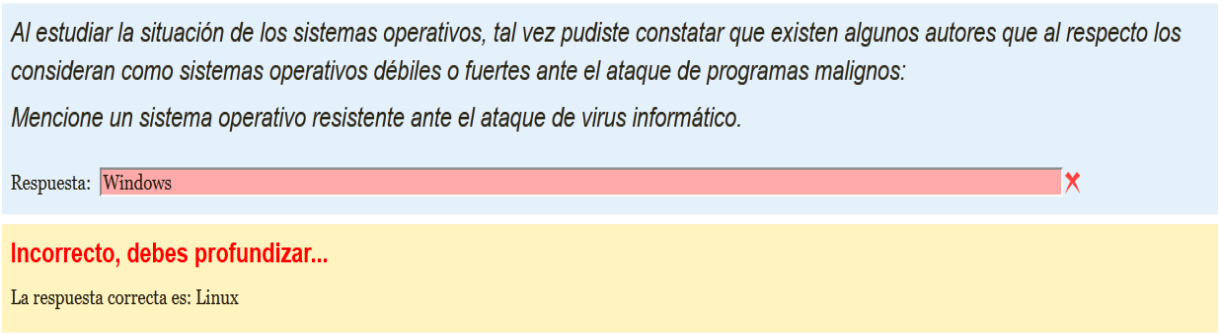

Figura 6. Ejemplo de pregunta de respuesta corta con retroalimentación.

7. Los relativos a las formas de organización del proceso de enseñanza - aprendizaje: las formas de organización fundamentales empleadas para el desarrollo de la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”, se han ido mencionando con anterioridad en correspondencia con el empleo de las herramientas de actividad y comunicación desde la plataforma Moodle, los objetivos, contenidos, métodos y posibilidades reales que presentan los aprendices según los resultados y seguimiento al diagnóstico inicial.

En esencia, para el uso de las herramientas de actividad y comunicación se hace necesario tener presente el objetivo que determina para qué se emplearán dichas herramientas, cómo se utilizarán (sistema de tareas de aprendizaje) y qué materiales ya sean básicos o complementarios servirán de apoyo para el debate y reflexión atendiendo al tratamiento de los contenidos de preparación en seguridad informática.

La implementación de la plataforma Moodle se sustentó, no sólo a partir de la preparación de los docentes desde el punto de vista del uso de las TIC sino también teniendo en cuenta los requerimientos tecnológicos existentes desde las propias condiciones del contexto del Politécnico “Julio Antonio Delgado Reyes”.

Este centro cuenta con un laboratorio de computación con quince computadoras personales conectadas a la red nacional con el apoyo de los servidores de RIMED, teniéndose además la posibilidad de acceder a los servicios de navegación y correo electrónico nacional facilitando así de igual forma el acceso a otros sitios vinculados con la seguridad informática.

Por otro lado, la escuela posee un servidor Web, desde el cual se utiliza la versión 2.6 de la plataforma Moodle, recurriendo además a una versión portable que puede ser utilizada por los aprendices desde otros contexto que no sea del Politécnico antes mencionado.

Como se ha podido apreciar, para el éxito de la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", se deben relacionar tanto la estructuración de los contenidos desde EVEA como de forma presencial.

Los contenidos tratados de forma presencial conforman un complemento de los conocimientos adquiridos por los aprendices desde el entorno virtual, de ahí que estos encuentros tengan por finalidad aplicar los nuevos saberes relacionados con la seguridad informática, asimismo, contribuyen al control y evaluación de la calidad de los avances alcanzados por estos en las actividades de preparación en seguridad informática ejecutadas.

En tal sentido cada unidad didáctica a desarrollarse de forma presencial, culmina con la presentación de un trabajo final el cual será presentado por los equipos seleccionados, de esta forma se emitirá una evaluación final al respecto.

Desde este contexto, cada estudiante tendrá la posibilidad de exponer sus criterios, ideas, dudas, sugerencias, inquietudes, para así enriquecer las acciones de preparación en seguridad informática desarrolladas.

Es por ello que resulta importante tener en cuenta para el desarrollo de los contenidos en seguridad informática para la preparación de docentes de forma presencial es la utilización del método de las instrucciones que tiene una amplia utilización en la ETP.

Pues posibilita combinar las formas de dirección y orientación para el trabajo independiente de los aprendices, ajustándose además a las exigencias de la Resolución 254/2013 que constituye el actual Reglamento para la planificación, organización, desarrollo y control de la enseñanza práctica en los centros docentes de la ETP y en las entidades de la producción o los servicios.

Durante todo el desarrollo de la clase práctica, dirigida a la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", se empleará el método de las instrucciones que estará compuesto además por:

La instrucción inicial: tiene como componente principal contribuir a la educación formal, reflexiva y ética en cuanto al tratamiento de los temas de seguridad informática, a partir de las guías de estudio a emplear, precisando las condiciones de realización de las actividades prácticas, las características de las tareas de aprendizaje a ejecutar el análisis de forma colaborativa de algunas dudas que puedan estar presentes en los aprendices.

Todo ello, a partir de los conocimientos que han ido adquiriendo estos, para lo cual se prepararon preguntas de intercambio, análisis y reflexión que permitan la sistematización de los contenidos en seguridad informática tratados anteriormente a través de EVEA.

La instrucción para la ejercitación práctica de los contenidos en seguridad informática: desde este contexto, se les da cumplimiento a las exigencias plasmadas en las guías de estudio, por tanto, es donde se desarrollarán las habilidades prácticas plasmadas en el objetivo de la clase atendiendo al trabajo colaborativo, la creatividad y autonomía que deben mostrar los aprendices en la realización de las actividades de aprendizaje previstas.

Y por último, la instrucción final, que es aquella que teniendo en cuenta la participación de todos los protagonistas de la preparación en seguridad informática, garantiza la discusión, valoración, comunicación y evaluación de las tareas de aprendizaje realizadas por los aprendices.

La fase número tres: “Fase de evaluación y retroalimentación” tiene como finalidad, valorar las acciones planificadas e instrumentadas en la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”.

En ella se pone de manifiesto de forma integral acciones de control, y/o evaluación que revelen los resultados que se van obteniendo respecto al cumplimiento de los objetivos planificados y el desarrollo mostrado por cada uno de los docentes inmersos en la preparación en seguridad informática.

Se hace necesario, además alcanzar un carácter consciente de todos los factores de la entidad educativa con vista a las deficiencias y avances que se van alcanzando. De esta manera se contribuirá si es necesario a la realización de los ajustes pertinentes en cada una de las fases al darles verdadero sentido de flexibilidad y pertinencia a las acciones ejecutadas.

En correspondencia con lo anterior, se sugiere sistemáticamente que los miembros del consejo de dirección de la entidad educativa, apliquen encuestas, entrevistas, valoren los distintos registros de actividad para de esta forma evaluar el nivel de satisfacción que van mostrando, en sentido general los protagonistas de la preparación en seguridad informática a medida que van transcurriendo las diferentes fases previstas en la alternativa metodológica B-learning.

Por tal razón, la evaluación debe conducir al análisis crítico del desarrollo de la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes” al ponerse de manifiesto desde el propio modo de actuación del docente en lo concerniente a la seguridad informática, vista desde el dominio que posea en relación con las legislaciones vigentes, procedimientos, metodologías existentes y en la posibilidad de insertar los temas de seguridad informática en las diferentes actividades curriculares planificadas y ejecutadas en función del aprendizaje de los estudiantes.

Es por ello, que la evaluación de la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes” no debe verse como un componente a proyectarse sólo desde las acciones propias de dicha preparación, sino desde el propio funcionamiento integral del proceso pedagógico y profesional.

Es importante que el control y la evaluación, se mantengan durante todas las fases destinadas a la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”, y de esta manera, crear un clima agradable, donde impere en todo momento la buena comunicación manteniendo así una motivación estable ante los contenidos a tratar.

Lo antes abordado garantizará mantener en todo momento, y cuando se requiera el acceso de los docentes al laboratorio de computación y la biblioteca escolar, asimismo se propiciará el buen estado técnico del sistema informático instalado, la sistematicidad de los servicios de navegación nacional y buen funcionamiento de la red informática. Para el desarrollo de las actividades práctica se hará necesario por parte de los profesores del curso, realizar coordinaciones para garantizar la disponibilidad de los locales y recursos necesarios.

Es preciso que los docentes seleccionados posean una preparación básica para el trabajo con el Sistema Operativo Windows pues es el que se encuentra instalado en la entidad educativa antes mencionada así como poseer habilidades para la navegación en la Web y el procesador de texto Microsoft Word pues estos contribuirán a la realización de las distintas actividades de aprendizaje.

En caso de alguna interrupción, se deberá informar de inmediato a los profesores del curso o algún miembro del consejo de dirección del centro escolar para llevar a cabo la toma de decisiones que den continuidad a las actividades de preparación en seguridad informática.

Se recomienda, para el seguimiento de las acciones de preparación en seguridad informática analizar su evolución desde los temas a valorar en los diferentes órganos de dirección que se ponen de manifiesto desde el Politécnico “Julio Antonio Delgado Reyes”.

Y por último, se debe, siempre que sea posible y fundamentalmente para el desarrollo de los contenidos en seguridad informática de forma presencial, la participación de especialistas en temas de seguridad informática

para que aborden sus opiniones respecto a los contenidos estudiados y aportar sus experiencias para así contribuir al perfeccionamiento del sistema de preparación en seguridad informática implementado.

En la figura que se muestra a continuación se realiza un resumen de los aspectos abordados con anterioridad.

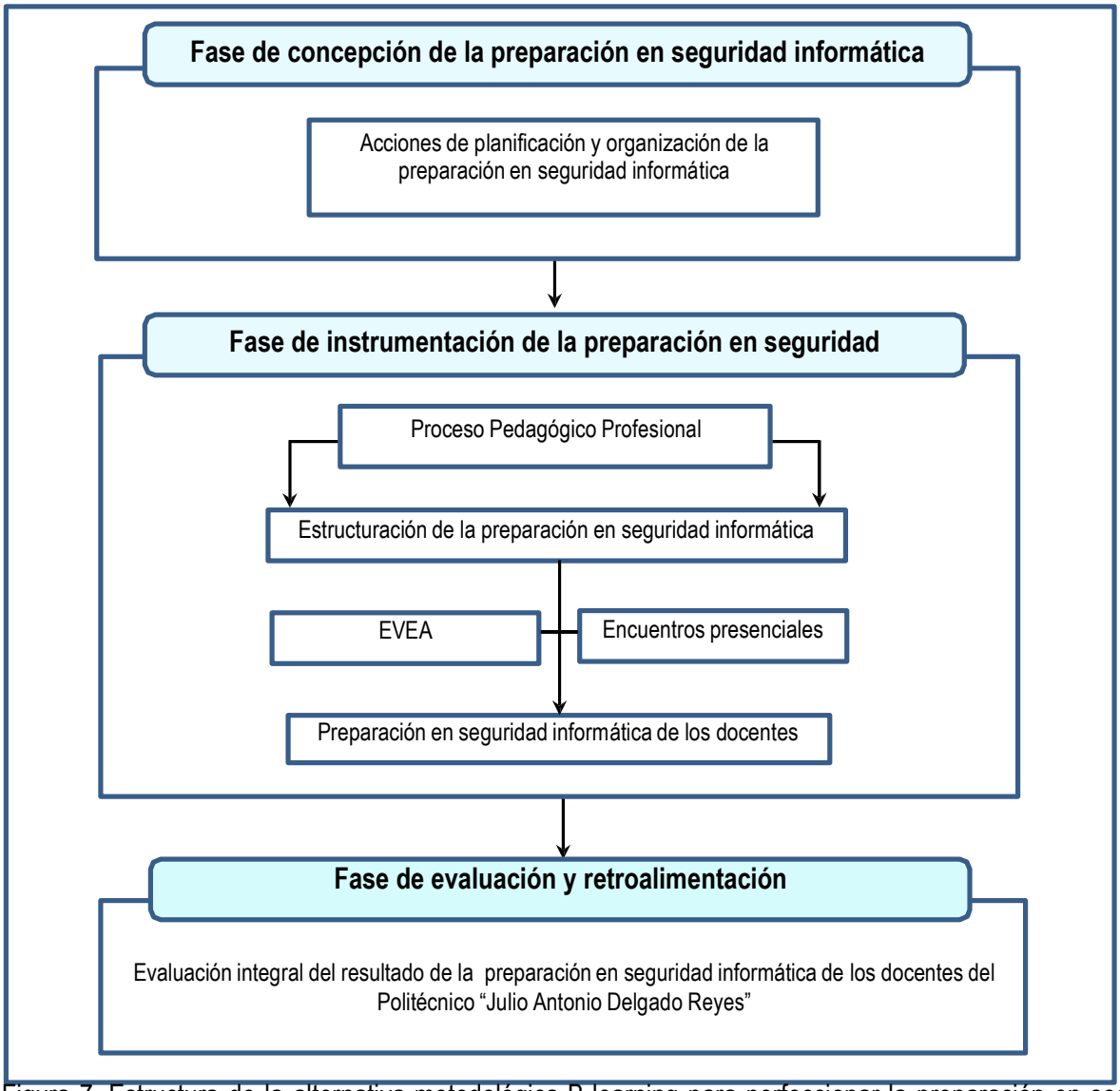

Figura 7. Estructura de la alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes.

2.3. Valoración de la factibilidad de la alternativa metodológica B-learning propuesta para dar solución al problema planteado en la investigación

La alternativa metodológica B-learning propuesta para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes" fue sometida a criterio de especialistas con el objetivo de evaluar, su estructura, la propuesta de programa para la preparación en seguridad informática y la concepción

puesta en macha para la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes” de forma presencial y desde EVEA.

Fueron considerados como especialistas profesionales de especialidades informáticas de nivel superior con conocimientos y experiencia en temas de seguridad informática. Asimismo, pedagogos con experiencia de trabajo tanto en la informática como en la ETP ya sea desde el nivel superior o desde la Enseñanza General Politécnica y Laboral. Todos ellos fueron capaces de ofrecer sus opiniones, valoraciones y recomendaciones en relación a la alternativa que se propone.

Dentro de los profesionales que aceptaron desempeñarse como especialistas para valorar los resultados de la propuesta realizada se encuentran: dos que han desarrollo cursos preparación en seguridad informática, los cuales laboran en la actualidad en la empresa DESOFT y en la Jefatura del MININT, dos de los Joven Club de Computación y Electrónica, cinco pedagogos de la Universidad de Guantánamo con experiencia en la formación de profesionales de perfil informático, cinco metodólogos de la Dirección Provincial y Municipal de Educación; de ellos uno de la rama informática y cuatro de la ETP, todos pertenecientes a la provincia Guantánamo, para un total de 14 especialistas.

A continuación se muestra la cantidad de especialistas, el nivel científico y categoría docente que poseen:

Nivel científico y categoría docente	**Cantidad**
Titular y Doctor	1
Auxiliar y Doctor.	1
Asistente y Doctor.	2
Master y Auxiliar.	2
Master y Asistente.	2
Master e Instructor.	4
Licenciado, Ingeniero o Instructor.	2
Total	14

Tabla 1**:** Caracterización de los especialistas.

A estos, se les ofreció las siguientes informaciones en relación con la propuesta de alternativa metodológica B-learning teniendo en cuenta los siguientes argumentos:

1. Estructura de la alternativa metodológica B-learning.

2. Propuesta de programa para la preparación en seguridad informática.

3. Concepción de la preparación en seguridad informática desde EVEA.

4. Concepción de la preparación en seguridad informática desde encuentros presenciales.

Para conocer la valoración de las especialistas en función de los argumentos antes expuestos, fue aplicada una encuesta (Anexo 7). Se garantizó el trabajo solicitado desde el anonimato y de forma independiente.

Desde los resultados de la valoración realizada, mostrados en el Anexo 8 y el Gráfico 1, se pudo evidenciar en relación con los argumentos revelados, que la mayor parte de los especialistas los caracterizó de muy adecuado (5), bastante adecuado (4) y adecuado (3).

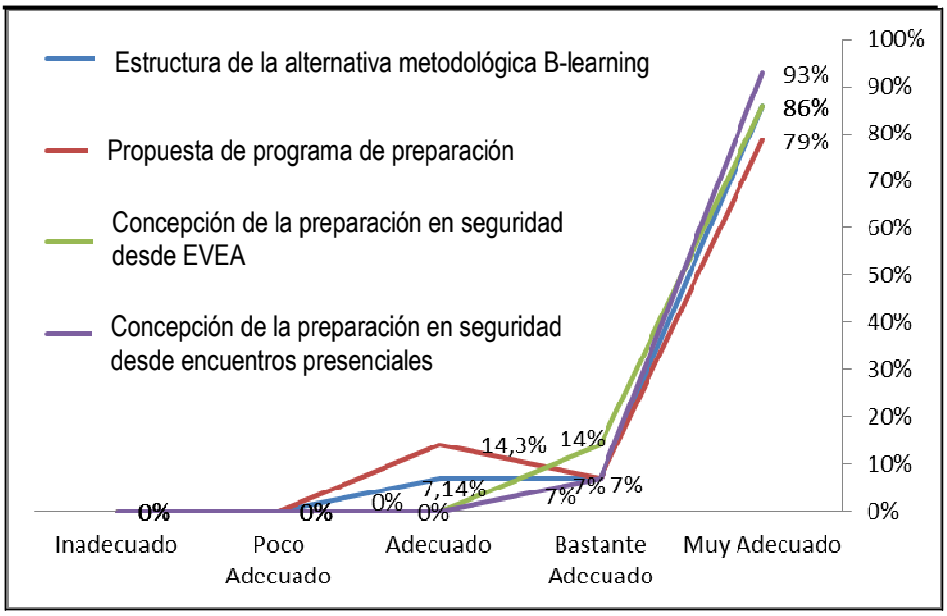

Gráfico 1. Resultados de la valoración realizada por los especialistas en relación a la propuesta de alternativa metodológica B-learning según argumentos mostrados.

En cuanto a la estructura de la alternativa metodológica B-learning, la consideraron muy positiva, pues cada una de sus fases se enfocan en forma de sistema materializándose el conjunto de actividades a ejecutar en correspondencia a las necesidades y condiciones existentes en el Politécnico "Julio Antonio Delgado Reyes" tomando como base el modelo de actuación profesional del docente.

Por otro lado y respecto a lo anterior, destacaron lo positivo de incluir a los demás factores responsables de la dirección del proceso pedagógico profesional del Politécnico, para que de esta manera contribuyan y apoyen cada una de las acciones que garantizarán finalmente el éxito de la preparación en seguridad informática dirigida al docente de esta entidad educativa.

El programa de preparación en seguridad informática, como se había mencionado con anterioridad, fue ubicado en las categorías de muy adecuado, bastante adecuado y adecuado, exponiendo por parte de los especialista que responde a las aspiraciones proyectadas para la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”, vinculando además lo político e ideológico, lo pedagógico, lo organizativo y lo tecnológico.

Destacaron la gama de informaciones existentes, que sirven de apoyo, guía y orientación a los protagonistas de las acciones de preparación en seguridad informática, ya sea para ser ejecutado desde EVEA o de manera presencial, sugirieron además planificar de forma objetiva el tiempo que se le dedicará al desarrollo de cada unidad didáctica, aspecto asumido por el autor de esta tesis.

Enfatizaron por otro lado, lo importante que fue llevar a cabo la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes”, tomando como base fundamental los EVEA y apoyado con encuentros presenciales en estrecha relación.

Además valoraron de positivo el uso de las herramientas de comunicación desde los entornos virtuales contribuyendo al intercambio, el análisis y colaboración atendiendo a los temas tratados y por otro lado la contextualización respecto a la estructuración didáctica de los contenidos de seguridad informática tomando como premisas las fases de la estructura didáctica de la clase práctica desde la ETP.

En fin, los resultados obtenidos en la entrevista realizada a los especialistas evidencia la aceptación de alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico “Julio Antonio Delgado Reyes” pues responde a las condiciones y características del mencionado centro escolar.

Conclusiones del capítulo II

La alternativa propuesta, se elaboró relacionando tres fases para su instrumentación, las cuales fueron necesarias para poder perfeccionar la preparación en seguridad informática contextualizada al proceso pedagógico profesional y condiciones del Politécnico “Julio Antonio Delgado Reyes”.

Según el criterio de especialistas, la concepción de la preparación diseñada, es válida pues facilita el tratamiento de los contenidos en seguridad informática de forma presencial y a distancia, al facilitar el intercambio, la colaboración no sólo entre los protagonistas de la preparación sino también con los demás miembros del consejo de dirección.

CONCLUSIONES

1. El análisis de las tendencias históricas permitieron constatar que la preparación en seguridad informática de los docentes constituye una necesidad en las condiciones actuales en función de garantizar el uso ético, responsable y seguro de las TIC en el marco de la Revolución Cubana.

2. La sistematización realizada, permitió sentar las bases para obtener los referentes teóricos necesarios para comprender las necesidades de preparación en materia de seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", en correspondencia con el desarrollo experimentado por las TIC y las exigencias que demanda la sociedad actual.

3. El diagnóstico de la preparación en seguridad informática, evidenció el estado actual del problema planteado en la investigación, por tal razón, fue necesario implementar una alternativa metodológica B-learning ajustándola a las condiciones del proceso pedagógico profesional de la institución educativa antes mencionada.

4. La alternativa se estructuró tomando como base las concepciones teóricas emitidas por los diferentes autores estudiados para el uso de EVEA en estrecha relación con las exigencias puestas de manifiesto para el desarrollo de las clases prácticas desde la ETP en Cuba, lo cual sirvió de sustento para el tratamiento de los contenidos en seguridad informática a distancia y de forma presencial.

5. Los resultados obtenidos en la valoración de la factibilidad de la alternativa metodológica B-learning por criterio de especialistas, permitieron corroborar que esta es factible y aplicable, en correspondencia con los fines que guiaron su elaboración.

RECOMENDACIONES

1. Proponer a la Dirección Provincial de Educación de la provincia Guantánamo la posibilidad de poner en marcha la valoración de los resultados de la alternativa elaborada de forma experimental con vista a ser perfeccionada y llevar a cabo su generalización en otras instituciones de la ETP.

2. Socializar los resultados de la alternativa metodológica B-learning propuesta para la preparación en seguridad informática de docentes, sirviendo de material de consulta para estructurar otras formas de preparación desde la ETP en la provincia Guantánamo.

3. Continuar sistematizando la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", atendiendo a los cambios sistemáticos que se dan en las TIC y la integración de estas según las nuevas formas de utilización.

BIBLIOGRAFÍA

1. Alfonso, A., y Arocha. H. C. (2010). La seguridad informática un componente de la seguridad nacional. Revista Mendive. ISSN: 1815 – 7696. Extraído el 2 de diciembre de 2012 desde http://www.revistamendive.rimed.cu.
2. Alemañy, C. (2009). Blended Learning y sus aplicaciones en entornos educativos. Revista de Docencia Universitaria. ISSN: 1887- 4592. Extraído el 2 de mayo 2012 desde http://red-u.net/redu/index.php/REDU/article/view/536
3. Álvarez, C. (1999). La escuela con la vida. (pp. 1 - 13). Ciudad Habana: Pueblo y Educación.
4. Andrade, E. M. (2013). Propuesta Blended – Learning de educación estética dirigida a docentes para la enseñanza a niñas de 8 – 10 años. Tesis de Maestría. Universidad tecnológica de Israel. Ecuador.
5. Andrés, J., Chappe, A. y López, C. (2012). Blended – Learning y estilos de aprendizajes en estudiantes universitarios del área de salud. Revista Scielo. ISSN: 0758 - 5936. Extraído el 2 de diciembre de 2012 desde http://scielo.sld.cu.
6. Aranda, R. (2013). Estudio de sistemas de seguridad basados en la detección de intruso físico y tecnológico. Tesis de Maestría. Universidad de Cantabria. Extraído el 12 de Noviembre de 2014 desde http://bucserver01.unican.es/xmlui/handle/10902/4531.
7. Baptista, M. J., Díaz, F. G. (2015). Diagnóstico para a implementação do ensino a distancia (ead) no isced do Huambo. CD-ROM: Congreso Internacional Pedagogía 2015. ISBN: 978-959-18-1099-1.
8. Barrera, A. (2010). Diseño didáctico de entorno virtual de aprendizaje para la capacitación de directivos del Poder Popular. Tesis de Maestría. Instituto Superior Politécnico José Antonio Echeverría.
9. Batista, A. Y. (2015). Estrategia pedagógica para desarrollar la cultura informática en la formación inicial del profesional de la educación.CD-ROM. Congreso Internacional Pedagogía 2015. ISBN: 978-959-18-1099-1.
10. Bauta, R. M. (2011). B-learning, alternativa educacional para la Universidad de Ciencias Informáticas a través de Entornos Virtuales. Revista Series Científica. ISSN: 2206 – 2495. Extraído el 2 de mayo 2012 desde http://publicaciones.uci.cu/index.php/article/view/23.
11. 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.
12. Bermúdez, R., y Pérez, L. M. (2004). Aprendizaje formativo y crecimiento personal. MINED. p. 35. Ciudad Habana: Pueblo y Educación. ISBN: 959-11547-5.
13. Bidot, J. (2012). Escenario de la seguridad informática en los inicios del 2013. Extraído el 11 Octubre de 2012 desde http://www.segurmatica.cu.
14. Bisogno, M. V. (2004). Metodología para el aseguramiento de Entornos Informatizados. Tesis de Grado. Universidad de Buenos Aires. Argentina.

15. Blanco, A. (2001). Introducción a la sociología de la educación. Ciudad Habana. Pueblo y Educación. ISBN: 959-13-0931-7.
16. Blanco, L. (2004). Apuntes para una historia de la informática en Cuba. Extraído el 11 Octubre de 2012 desde http://www.sld.cu/galerías/doc/infodir/apuntes.doc.
17. Borghello, C. F. (2001). Seguridad Informática. Sus implicancias e implementación. Tesis de Licenciatura en Sistemas. Universidad Tecnológica Nacional de México.
18. Bravo, J. L. y Chacón, C. M. Diccionario Latinoamericano de Educación. Universidad Central de Venezuela. Fundación Gran Mariscal de Ayacucho. ISBN: 980-00-2099-3.
19. Bugarini, F. (2007).Una propuesta de seguridad en la información: Caso Systematics de México, SA. Tesis de Maestría. Politécnico Nacional. México.
20. Cáceres, J. A. (2012). Virus informáticos. ¿Cómo protegernos? Ciudad Habana: Ciencia y Técnica. ISBN: 978-959-05-0668.
21. Calderón, I. L. (2012). Desarrollo de una metodología para la creación de objetos de aprendizaje en el modelo B-learning. Tesis de Grado. Escuela Superior Politécnica Chimborazo. Ecuador.
22. Cifuentes, G. (2006). Análisis de seguridad en BD: aplicación Oracle Versión 116. Tesis de Maestría. Universidad de las Fuerza Armadas. Ecuador.
23. Collazo, D. B. y Puentes, A. M (2004). La orientación en la actividad pedagógica. Ciudad Habana: Pueblo y Educación. ISBN: 959-13-0749-7.
24. Cruz, R. M. (2007). Procesamiento de la información en las investigaciones educacionales. Ciudad Habana: Ciencia y Técnica. ISBN: 978-959-18-0354-2.
25. De Armas, R. A y Valle, L. A. (2011). Resultados científicos en la investigación educativa. Ciudad Habana: Pueblo y Educación. ISBN: 978-959-13-2124-4.
26. De la Caridad, P. (2013). Dinámica socio – laboral –profesional de la semipresencialidad en la universidad. Revista Didascalia. Universidad de Oriente. ISSN: 2224-2643. Extraído el 5 de Octubre 2014 desde http://ojs.uo.edu.cu/index.php/Didascalia/article/view/3852/3233.
27. De los Ángeles, N. (2010). Sistemas de recursos educativos de apoyo al estudio de la seguridad informática en los Joven Club de Computación y Electrónica. Tesis de Maestría. Instituto Superior Politécnico José Antonio Echeverría.
28. Del Porto, C. (2013). Tendencia en el 2013, para tener en cuenta. Revista de Computación (GIGA). ISSN: 1028 – 270X.
29. Díaz, R. C, y Del Carmen, E. (2010). Experiencia y modalidad B-learning para la formación y evaluación en competencias genéricas en ingeniería. Revista La Cuestión Universitaria. Universidad de Madrid. Extraído el 21 de Noviembre de 2014 desde. http://www.upm.es.

30. Díaz, R. Y., y Pérez, C. Y. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Extraído el 7 de Septiembre 2014 desde http://www.ciencias.holguin.cu/index.php/cienciasholguin/article/view/827/879.
31. DRAE, (2014). Diccionario de la Lengua Española de la lengua. Disponible en http://rae. es, (consultado el 7 de Septiembre 2014 desde
32. Eugenia, M. (2011). La preparación del docente para el uso de las TIC. Revista IPLAC. Instituto Latinoamericano y Caribeño. Extraído el 7 de Septiembre 2014 desde http://revista.iplac.rimed.cu/index.php.
33. Expósito, C., et al. (2001). Algunos elementos de la metodología de la enseñanza de la informática. Instituto Superior Pedagógico Enrique José Varona. (pp. 1-13). Ciudad Habana.
34. Fuentes, H., Montoya, J., y González, N. (2012). La universalización de la universidad y la evaluación de la calidad en la semipresencialidad: Un reto en su dimensión. Revista Colegio Universitario. Universidad de Oriente. ISSN: 2307-7522. Extraído el 7 de Septiembre 2014 desde http://ojs.uo.edu.cu/index.php/rcu/article/View/4303/3661.
35. García, O. (2010). Concepción pedagógica de un entorno virtual de enseñanza aprendizaje desarrollador para la formación de profesores. Tesis Doctoral. Universidad de Ciencias Pedagógicas Frank País García. Santiago de Cuba.
36. González, M. y Spenger, I. (2010). Curso semipresencial. La reacción química, un acercamiento hacia la educación digital. Revista Universitaria. Universidad de la Habana. ISSN: 1609-4808.
37. González, I. y Blanco, L. (2013). La evolución de los sistemas virtuales en la educación. Revista Cubana de Computación (GIGA). ISSN: 1028-270.
38. González, O. M. (2013). Evaluación de la calidad en la semipresencialidad: un reto en su dinámica. Revista Con Luz Propia. SNTECD. ISNN: 1029-6123.
39. Guevara, J. (2014). El Blended – Learning en el proceso de refuerzo académico de programación de aplicaciones de cuarta generación en la unidad educativa Fronieska Montalvo. Tesis de Maestría. Universidad Técnica de Ambato. Ecuador.
40. Hernández, A. Y., y Pérez, A. (2013).Propuesta metodológica para una periodización de las contribuciones de las telecomunicaciones al desarrollo sostenible de Pinar del Rio. Revista Científica Avances. ISSN: 1562 – 3297. Universidad de Pinar del Rio. Extraído el 7 de Junio de 2015 desde http://www. Ciget.pinar.cu/Revista/NP2013/artículos/rap09414.doc
41. Hernández, G. A., y Ansola, H. E. (2014). La clase encuentro en la modalidad semipresencial para las carreras de Ingeniería Informática e Ingeniería Industrial. Revista Referencia Pedagógica. Politécnico José Antonio Echeverría. ISSN: 2308-3042. Extraído el 7 de febrero 2014 desde http://rrp.cujae.edu.cu.

42. Hernández, L. (2012). Un modelo de implementación de la seguridad en una aplicación Web con el uso de Programación Orientada a Aspectos. Tesis de Maestría. Instituto Superior Politécnico José Antonio Echeverría.
43. Herradón, R., Blando J. y Sánchez, J. A. (2009). Experiencia y modalidad B-learning para la formación y evaluación en competencias genéricas en ingeniería. Revista La Cuestión Universitaria. Universidad de Madrid. Extraído el 21 de Noviembre de 2014 desde. http://www.upm.es.
44. 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 Doctoral. Instituto Superior Pedagógico Enrique José Varona.
45. Horruitiner, P. (2006). La universidad cubana: el modelo de formación. La Habana. Editorial Félix Varela, (material digital).
46. Hurtado, F. (2007). Introducción de las Tecnologías de la Información y las Comunicaciones su impacto en el aprendizaje de los estudiantes. MINED. p. 35. Ciudad Habana: Pueblo y Educación. ISBN: 958-18-0305-2.
47. Leblanch, I. (2013). Sitio Web educativo para desarrollar una cultura en seguridad informática en los estudiantes de los institutos politécnicos de informática. Extraído el 11 Octubre de 2012 desde http://revista.iplac.rimed.cu/index.php.
48. Leiva, A. (2007). Estrategia de superación semipresencial en la microuniversidad para los docentes de la educación especial que atienden a escolares con baja visión. Tesis Doctoral. Instituto Superior Pedagógico Félix Varela Villa Clara.
49. Lima, S. (2012). Estrategia de superación profesional de los docentes en contenidos de Educación a Distancia. Instituto Latinoamericano y Caribeño (IPLAC).Material Digital.
50. Lineamientos estratégicos para la Informatización de la Sociedad Cubana. Resumen ejecutivo. Material mecanografiado. La Habana: junio, 1997.
51. López, J. (2013). Propuesta de una estrategia metodológica para perfeccionar la funcionabilidad de plataformas virtuales de aprendizaje. Revista Series Científicas. Universidad de Ciencias Informáticas. ISSN: 2206-2495. Extraído el 7 de Septiembre 2014 desde http://publicaciones.uci.cu/index.php/article/view/1957.
52. López, R. (2010). Componentes para la estructura didáctica de cursos de Educación a Distancia usando como herramientas las plataformas gestoras. Tesis Doctoral. Universidad de Cienfuegos Carlos Rafael Rodríguez, Cienfuegos.
53. Martí, J. A. (2009). Aprendizaje B-learning. Modalidad de formación de profesionales. En Revista Universidad EAFIT. ISSN: 0120 – 341X. Extraído el 21 de Noviembre de 2014 desde. http://redalyc.uaemex.mx/src/inicio/artpdf.red.jspCve=21512252006.

54. Martín, E. A., y Botello, G. I. (2008). Seguridad en redes inalámbricas. Revista de Computación (GIGA). ISSN: 1028 – 270X.
55. Martínez, J. (2012). El uso de la informática y la Cibernética en las guerras modernas. En Revista Series Científicas. Universidad de Ciencias Informáticas. ISSN: 2206-2495. Extraído el 21 de Noviembre de 2014 desde http://publicaciones.uci.cu/index.php/article/view/190.
56. Martínez, M., y Rodríguez, J. (2002). Filosofía de la Educación. Instituto Superior Pedagógico Enrique José Varona. Ciudad Habana, (material digital).
57. Martínez, O. L. (2014). Las TIC y su integración en la Educación Universitaria. Una medida del futuro. Revista Didascalia. Universidad de Oriente. Cuba. ISSN: 2224-2643. Extraído el 21 de Noviembre de 2014 desde. http://ojs.uo.edu.cu/index.php/Didascalia/view/96/4039/3417.
58. Mayol, R. N. (2006). Modelo para la auditoría de la seguridad informática en la red de datos de la Universidad de los Andes. Tesis de Maestría. Universidad de los Andes.
59. Mayorga, C. (2014). Seguridad informática y la relación en la utilización de Internet como herramienta de apoyo en la formación de niñas, niños y adolescentes en educación inicial y básica del Centro Educativo Pradera. Tesis de Maestría. Universidad Técnica de Ambato. Ecuador.
60. Méndez, G. M. (2011). Virus infectores de cavidad. Revista de Computación (GIGA). ISSN: 1028 – 270X.
61. MIC. (2007). *Resolución 127/2007, Reglamento de Seguridad para las Tecnologías de la Información*. Ciudad Habana, (material digital).
62. MINED. (2010). *Resolución 17/2010, Políticas para la conexión de los centros educacionales del Sistema Nacional de Educación*. La Habana, (material digital).
63. MINED. (2014). Seminario Nacional de Preparación del Curso Escolar 2014 – 2015. La Habana, (material digital).
64. MINED. (2005). VI Seminario Nacional para Educadores. La Habana, (material digital).
65. Miniguano, M. A. (2014). El Blended – Learning como herramienta de apoyo docente en el proceso de enseñanza aprendizaje del Módulo de NTIC. Tesis de Maestría. Universidad Técnica de Ambato. Ecuador.
66. MININT. (1996). Resolución 6/2004, Reglamento de Seguridad Informática. La Habana, (material digital).
67. MININT. (2000). *Resolución 1/2000. Reglamento de Seguridad y Protección de la Información Oficial*. La Habana, (material digital).
68. MININT. (2012). *Orden 35/2012, Reglamento de seguridad de las infocomunicaciones*. La Habana, (material digital).
69. Monzón, C. J. (2009). Auditoría de seguridad de redes inalámbricas de área local. Tesis de Grado. Universidad Mayor de San Andrés. Bolivia.

70. Morejón, A. y Arocha, H. C. (2011). La seguridad informática un componente de la seguridad nacional. Revista Mendive. Universidad de Ciencias Pedagógicas Rafael María Mendive. ISSN: 1815-7696. Extraído el 7 de Septiembre 2014 desde http://www.revistamediive.rimed.cu.
71. Muñoz, A. y Aguirre, J. R. (2013). Criptografía y redes telemáticas orientadas a la educación global. Revista Docencia Universitaria. ISSN: 1887 – 4592.
72. Nacer, O. y Bello, S. (2013). Tecnologías del milenio, el poder del futuro. Ciudad Habana. Científico – Técnica. ISBN: 978-959-05-0679-6.
73. Norde, R., Valdés, M. N. y Díaz, S. (2014). Una alternativa didáctica para la práctica profesional en los ISP. Revista Referencia Pedagógica No. 2. ISSN: 2308 – 3042. Extraído el 7 de Septiembre 2014 desde http://rrp.cujae.edu.cu/index.php/rrp/article/view/62/72.
74. Oceguera, M. S., y De los Ángeles, N. M. (2015). Implementación de un curso a distancia para la sistematización de los elementos de seguridad informática a nivel de usuario común. CD-ROM: Congreso Internacional Pedagogía 2015. ISBN: 978-959-18-1099-1.
75. Pallas, M. G. (2009). Metodología de implantación de un SGSI en un grupo empresarial jerárquico. Tesis de Maestría. Instituto de Computación, Uruguay.
76. Pardo, M. E. y Izquierdo, J. M. (2014). La formación de profesionales universitarios en EVEA: experiencia en la Universidad de Oriente. Revista Colegio Universitario. ISSN: 2307 – 7522. Extraído el 2 de mayo año 2012 desde http://ojs.uo.edu.cu/index.php/rcu/article/View/4303/3660.
77. PCC. (1986). Informe Central al Tercer Congreso del Partido Comunista de Cuba, Departamento de Orientación Revolucionaria del CC del PCC. Material impreso.
78. PCC. (2011). Lineamientos de la Política Económica y Social del Partido y la Revolución, aprobados en el 6to Congreso del Partido Comunista de Cuba. Material impreso.
79. Pedraza, C. L. (2011). Guías prácticas para uso de técnicas de ingeniería social con herramientas SET incluida en la distribución Backtaclgr2. Tesis de Grado. Corporación Universitaria Bogotá. Colombia.
80. Peláez, R. (2012). Elementos de seguridad aplicada a las TIC. Tesis de Maestría. Universidad Autónoma del Estado de Hidalgo. México.
81. Peñalver, N. (2010). Libro electrónico como medio de enseñanza en los Cursos de Operador de Microcomputadoras y Seguridad Informática para los estudiantes de los Joven Club de Computación y Electrónica del municipio San Cristóbal. Tesis de Maestría. Instituto Superior Politécnico José Antonio Echeverría.
82. Pérez, A. (2013). Aplicación del modelo KOTTER para la gestión del cambio en la incorporación de TIC en el proceso de innovación académica con el uso de un B-learning para el C. E. Jahibé. Tesis de Maestría. Universidad Católica de Ecuador. Ecuador.

83. Pérez, V. (2006). La preparación informática del docente para la educación a distancia en entornos virtuales de enseñanza-aprendizaje. Tesis Doctoral. Instituto Pedagógico Latino Americano y Caribeño, Ciudad de La Habana.
84. Pérez, Y. (2012). Estándares para minimizar ataques de seguridad informática. Revista Series Científicas. Universidad de Ciencias Informáticas. ISSN: 2206-2495. Extraído el 7 de Septiembre 2014 desde http://publicaciones.uci.cu/index.php/article/view/965.
85. Pompeya, V. E. (2008). Blended – Learning. La importancia de la utilidad de diferentes medios en el proceso educativo. Tesis de Maestría. Universidad de la Plata. Argentina.
86. Quesada, R., Ceballos, C. y Miranda, E. H. (2007). Texto para el curso de preparación básica en Defensa Nacional para la Maestría en Dirección. Diplomado I. MES. Departamento Independiente de Enseñanza Militar. (Material digital).
87. Ramírez, S. (2008). Sistema de cursos a distancia para superar en materia de seguridad informática a los profesores de computación que atienden esta actividad en la provincia Guantánamo. Tesis de Maestría. Instituto Central de Ciencias Pedagógicas. Cuba.
88. Ramiro, J. (2006). Libro Electrónico de Seguridad Informática y Criptografía. Universidad Politécnica de Madrid. España. (Material digital).
89. Ripoll, I. J. (2012). Seguridad en los sistemas informáticos. Universidad Politécnica de Valencia. . Extraído el 2 de mayo 2012 desde http://www.segu-info.com.ar.
90. Rodríguez, A. M. (1998). Proyecto de Informática Educativa en Cuba. Tesis de Maestría. Instituto Superior Pedagógico Enrique José Varona.
91. Rodríguez, A. M. (2010). La seguridad informática en la docencia universitaria. Extraído el 2 de mayo 2012 desde http://revista.iplac.rimed.cu/index.php.
92. Rodríguez, A. M. (2011). ¿Qué hacer con los usuarios de las TIC y la seguridad informática? Extraído el 16 de Octubre de 2013 desde http://blog.rimed.cu/seguridadinformatica.
93. Rodríguez, A. M. (2012). Una concepción teórico-metodológica para la educación en seguridad informática del personal de las instituciones del ministerio de educación. Tesis Doctoral. Instituto Pedagógico Latinoamericano y Caribeño (IPLAC).
94. Rodríguez, H. M. (2013). Filosofía de la educación cubana. Transformación de los modos de actuación de los educadores. Revista Con Luz Propia. SNTECD. ISNN: 1029-6123.
95. Rodríguez, M. F., y Quintana, V. A. (2007). Introducción a la estadística descriptiva. MINED. Ciudad Habana: Pueblo y Educación. ISBN: 959-13-1529-8.
96. Rodríguez, M. I., et al. (2007). El proceso profesional y el proceso pedagógico profesional: leyes y principios, elementos constituyentes. MINED. Ciudad Habana: Pueblo y Educación. ISBN: 978-959-13-1504-5.

97. Rosell, W. y Más, M. (2003). Enfoque sistémico en el contenido de la enseñanza. Revista Educación Médica Superior. ISSN: 0864 – 2411. Extraído el 2 de mayo 2012 desde http://scielo.sld.cu/scielo.php?scrip=sci_atextpid=50864-2141260300020402.

98. Sánchez, Y. (2011). Concepción teórico – metodológica del uso pedagógico de las herramientas de comunicación de los entornos virtuales en la superación profesional de docentes. Tesis Doctoral. Universidad de Ciencias Pedagógicas Enrique José Varona.

99. Seguridad informática, conceptos generales. Extraído el 2 de diciembre de 2012 desde http://www.Redyseguridad.firp.unam.mx.

100. Sosa, M., Vialart, N. y Vidal, M. (2012). Problemas éticos de seguridad asociados al uso de las tecnologías. Revista Scielo. ISSN: 0758 - 5936. Extraído el 2 de diciembre de 2012 desde http://bvs.sld.cu/revistas/n909/infd130910.htm.

101. Valdés, M. (2012). Diseño didáctico de cursos en línea para la capacitación de cuadros y funcionarios del Ministerio de la Informática y las Comunicaciones en temas de código abierto. Tesis de Maestría. Instituto Superior Politécnico José Antonio Echeverría.

102. Valle, A. (2012). La investigación pedagógica. Otra mirada. Ciudad Habana: Pueblo y Educación. ISBN: 978-959-13-2263-0.

103. Vidiaux, L., Madrigal, E. y Henry, J. (2013). Seguridad informática en la formación de profesionales. Revista Series Científicas. Universidad de Ciencias Informáticas. ISSN: 2206-2495. Extraído el 7 de Septiembre 2014 desde http://publicaciones.uci.cu/index.php/article/view/1163.

104. Vigotsky, L. S., Leontiev, A. y Luria, A. (1989). El proceso de formación de la Psicología Marxista. Editorial Progreso, Moscú.

Anexo 1. Variables e indicadores para la realización del diagnóstico.

Variables	Dimensiones	Indicadores
1. Preparación en seguridad informática alcanzada por los docentes del Politécnico "Julio Antonio Delgado Reyes"	1.1. Política – ideológica	1.1.1. Conocimientos de los principales aspectos contenidos en la legislación vigente sobre seguridad informática y los valores éticos y morales relacionados con el uso de las TIC.
	1.2. Tecnológica	1.2.1. Conocimientos sobre la aplicación de sistemas tierra física y contra fluctuaciones eléctricas. 1.2.2. Conocimientos sobre la aplicación de sistemas de alarmas contra intrusos y contra incendios. 1.2.3. Comprensión de la importancia del mantenimiento de las TIC. 1.2.4. Dominio de las metodologías para la elaboración del Plan de Seguridad Informática y Plan de Contingencias. 1.2.5. Conocimientos de los aspectos esenciales a tener en cuenta en la realización de auditorías informáticas.
		1.3.1. Conocimientos de los métodos y procedimientos dirigidos a la salva de la información.
		1.3.2. Dominio de las técnicas para la seguridad de la información contenidas en soportes digitales e impresos.
		1.3.3. Comprensión de las medidas de seguridad a tener en cuenta para el uso de equipos móviles de cómputo desde las entidades educativas.
		1.4. Conocimientos de las medidas de seguridad a emplearse para el uso del correo electrónico. 1.4.1. Preparación para el uso de programas antivirus.
		1.4.2. Conocimientos de las técnicas de ingeniería social dirigidas al uso de las TIC.
		1.4.3. Reconocimientos de las medidas de seguridad a emplearse en el uso de las redes sociales de comunicación.
2. Organización y desarrollo de acciones de preparación en seguridad informática, dirigidas a los docentes del Politécnico "Julio Antonio Delgado Reyes"	2.1. Pedagógica	2.1.1. Contenidos tratados en las actividades de preparación en seguridad informática. 2.1.2. Recursos digitales e impresos empleados en el desarrollo de las actividades de preparación en seguridad informática, dirigidas a los docentes del Politécnico "Julio Antonio Delgado Reyes". 2.1.3. Formas utilizadas para el control de la preparación.

	2.2. Organizativa	2.2.2. Principales actividades que se realizan para contribuir con la preparación en seguridad informática de los docentes. 2.2.3. Docentes seleccionados para participar en las actividades de preparación en seguridad informática.

Anexo 2. Cuestionario de encuesta.

Instrucciones: Estimado docente, se necesita de su colaboración en una investigación dirigida a la preparación que usted posee sobre seguridad informática. Agradecemos sus criterios atendiendo a la información que en el orden siguiente se solicita:

Años de experiencia_____

Grado científico_____

Categoría docente_____

1. ¿Considera importante tener preparación en seguridad informática, la cual garantice salvaguardar la información y las tecnologías empleadas en su creación? Sí_____ NO_____

2. Evalúe sus conocimientos sobre seguridad informática marcando con una (X) en las casillas según corresponda.

Aspectos	Bajo	Medio	Alto
Legislación dirigida a la seguridad informática.			
Clasificación de programas malignos y uso de programas antivirus.			
Sistemas de tierra física, alarmas contra incendios e intrusos.			
Medidas de seguridad para el uso del correo electrónico.			
Métodos para la salva de la información.			
Técnicas para la seguridad de la información digital e impresa.			
Técnicas de ingeniería social y redes sociales de comunicación dirigidas al uso de las TIC.			
Medidas de seguridad en el uso de equipos móviles de cómputo.			
Metodologías para la elaboración del Plan de Seguridad Informática y de Contingencias.			
Aspectos esenciales a tener en cuenta en la realización de auditorías informáticas y su relación con el mantenimiento de las TIC.			

3. Marque con una (X) las variantes que usted ha utilizado para adquirir preparación en seguridad informática:

Pregrado_____ Actividades metodológicas_____

Postgrado_____ Autodidacta_____

Autopreparación desde el puesto de trabajo_____

4. A continuación, se muestran determinados recursos digitales e impresos, marque con una (X) aquellos que usted ha empleado para adquirir preparación en seguridad informática:

Revistas impresas _____

Revistas digitales _____

Páginas o Sitios Web _____

Multimedia _____

Libros electrónicos _____

Libros impresos _____

Software educativos _____

Publicaciones científicas _____

Bibliotecas digitales _____

Cursos Virtuales _____

Anexo 3. Entrevista grupal.

Estimados docentes, se necesita de su colaboración con vista al desarrollo de una investigación la cual tiene como finalidad dotarlos a ustedes de una preparación en seguridad informática. Gracias.

1. ¿Cuántos años de experiencia posees en la Educación Técnica Profesional?

2. Narre brevemente los momentos más importantes de la introducción de las TIC en la ETP y cómo se ha trabajado en la preparación de los docentes en relación a la seguridad informática.

3. ¿Consideras importante que un docente tenga preparación en seguridad informática?

4. ¿Qué tipos de actividades se han desarrollado desde el Politécnico "Julio Antonio Delgado Reyes", con vista a la preparación en seguridad informática de los docentes que laboran en esta entidad educativa?

5. ¿Cómo se ha controlado y evaluado el nivel de preparación en seguridad informática alcanzado por los docentes?

6. ¿Cuáles contenidos han sido tratados?

7. ¿Cuáles son los aspectos positivos y negativos que consideras se han puesto de manifiesto en las actividades de preparación en seguridad informática dirigidas a los docentes del Politécnico "Julio Antonio Delgado Reyes"?

Culminación y agradecimientos

Anexo 4. Prueba inicial de desempeño.

Estimado docente, esta prueba nos permitirá diagnosticar el grado de preparación que usted posee sobre seguridad informática, favor de contestar las siguientes preguntas:

1. Mencione tres de las legislaciones que se emplean en la actualidad en Cuba para dar tratamiento a la seguridad informática.

_____

2. Realice una clasificación de los programas malignos y programas antivirus que usted conoce, explique brevemente en qué consisten dos de ellos.

_____

3. ¿Qué medidas usted empelaría para garantizar la seguridad de las informaciones contenidas en fuentes digitales e impresas?

_____

4. ¿Conoce usted qué es un sistema de tierra física, de alarma contra incendios o intrusos? Mencione dos de las ventajas que muestran estos para proteger las TIC instaladas en los centros educacionales cubanos.

_____

5. ¿Qué medidas de seguridad usted tendría en cuanta al utilizar las redes sociales de comunicación y contrarrestar los efectos de las técnicas de ingeniería social?

_____

6. ¿Qué medidas de seguridad usted emplearía para garantizar el uso correcto del correo electrónico?

_____

7. ¿Cuáles métodos o procedimientos se utilizan desde tu centro escolar para el logro eficiente de la salva de la información?

_____

8. Mencione dos de las medidas de seguridad que se emplean en tu escuela en relación al uso de equipos móviles de cómputo.

_____

9. Aborde tres aspectos que se tienen en cuenta en tu centro escolar para la elaboración del Plan de Seguridad Informática y el Plan de Contingencias.

_____

10. Mencione tres de las técnicas, métodos o procedimientos de auditorías informáticas que se explotan en tu entidad educativa y su relación con el mantenimiento de las TIC.

_____

Anexo 5. Tablas con los resultados de la encuesta aplicada a los docentes del Politécnico "Julio Antonio Delgado Reyes" para valorar la preparación en seguridad informática que poseen.

Años de experiencia como docentes en la Educación Técnica y Profesional.

Rangos	Cantidad	%
Menos de 5 años	11	26, 8
Más de 5 años	30	73, 1

Grado científico

Grado	Cantidad	%
Doctor	0	0
Master	14	34, 1

Categoría docente

Rangos	Cantidad	%
Titular	0	0
Auxiliar	0	0
Asistente	2	4, 8
Instructor	5	12, 1
Sin categoría	34	82, 9

Autovaloración de los docentes del Politécnico "Julio Antonio Delgado Reyes" en relación a la importancia que le concede a la preparación en seguridad informática.

Variante	Cantidad	%
Sí	41	100
No	0	0

Autovaloración de los docentes del Politécnico “Julio Antonio Delgado Reyes” acerca de los conocimientos que poseen sobre seguridad informática.

Aspectos	Bajo		Medio		Alto	
	Cantidad	%	Cantidad	%	Cantidad	%
Legislación dirigida a la seguridad informática.	36	87, 8	3	7, 3	2	4, 8
Clasificación de programas malignos y uso de programas antivirus.	36	87, 8	3	7, 3	2	4, 8
Sistemas de tierra física, alarmas contra incendios e intrusos.	41	100	0	0	0	0
Métodos de seguridad para el uso del correo electrónico.	27	65, 8	9	21,9	5	12,1
Métodos para la salva de la información.	36	87, 8	3	7, 3	2	4, 8
Técnicas para la seguridad de la información digital e impresa.	39	95, 1	0	0	2	4, 8
Técnicas de ingeniería social y redes sociales de comunicación dirigidas al uso de las TIC.	41	100	0	0	0	0
Medidas de seguridad en el uso de equipos móviles de cómputo.	39	95, 1	0	0	2	4, 8
Metodologías para la elaboración del Plan de Seguridad Informática y de Contingencias.	36	87, 8	3	7, 3	2	4, 8
Técnicas de auditorías de seguridad informática y su relación con el mantenimiento de las TIC.	38	92, 6	3	7, 3	0	0

Variantes utilizadas por los docentes del Politécnico “Julio Antonio Delgado Reyes” para adquirir preparación en seguridad informática.

Variantes	Cantidad	%
Pregrado	3	7, 3
Postgrado	0	0
Autodidacta	0	0
Actividades metodológicas	0	0
Autopreparación desde el puesto de trabajo	0	0
Dirigidas por la Dirección Municipal o Provincial de Educación u otras entidades	2	4, 8

Autovaloración sobre los recursos digitales e impresos empleados por los docentes del Politécnico “Julio Antonio Delgado Reyes” para adquirir preparación en seguridad informática.

Recursos	Cantidad	%
Revistas impresas	2	4, 8
Revistas digitales	2	4, 8
Páginas o Sitios Web	5	12, 1
Multimedia	0	0
Libros electrónicos	0	0
Libros impresos	0	0
Software educativos	0	0
Publicaciones científicas	0	0
Bibliotecas digitales	0	0
Cursos virtuales	0	0

Anexo 6. Resultados de la aplicación de la prueba inicial de desempeño aplicada para constatar el grado de preparación seguridad informática que poseen los docentes del Politécnico "Julio Antonio Delgado Reyes".

Resultado de aplicación de prueba inicial de desempeño.

Aspectos	Mal		Regular		Bien	
	Cantidad	%	Cantidad	%	Cantidad	%
Dominio de la legislación vigente sobre seguridad informática.	39	95, 1	2	4, 8	0	0
Clasificación de programas malignos y uso de programas antivirus.	38	92, 6	3	7, 3	0	0
Dominio de las medidas a tener en cuenta para la seguridad de la información contenida en fuentes digitales e impresas.	40	97, 5	1	2, 4	0	0
Sistemas de tierra física, alarmas contra incendios e intrusos.	41	100	0	0	0	0
Medidas de seguridad a tener en cuenta al emplear las redes sociales de comunicación y técnicas de ingeniería social.	41	100	0	0	0	0
Medidas de protección a emplearse al utilizar el correo electrónico.	36	87, 8	5	12, 1	0	0
Métodos y procedimientos para la salva de la información.	39	95, 1	2	4, 8	0	0
Medidas de seguridad para el uso de equipos móviles de cómputo.	40	97, 5	1	2, 4	0	0
Aspectos a tener en cuenta en la elaboración del Plan de Seguridad Informática y de Contingencias.	39	95, 1	2	4, 8	0	0
Técnicas de auditorías informáticas y su relación con el mantenimiento de las TIC.	40	97, 5	1	2, 4	0	0

Anexo 7. Encuesta a especialistas.

Estimado (a) compañero (a):

Con el propósito de evaluar una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática de los docentes del Politécnico "Julio Antonio Delgado Reyes", se solicita su valoración, dada su experiencia al respecto.

De forma anticipada se agradece su colaboración.

Gracias.

Evalúe los aspectos mostrados a continuación atendiendo a las categorías:

5 4 3 2 1

Muy adecuado, Bastante adecuado, Adecuado, Poco adecuado, Inadecuado.

Documentos a evaluar	1	2	3	4	5
1. Estructura de la alternativa metodológica B-learning.					
2. Propuesta de programa para la preparación en seguridad informática de los docentes.					
3. Concepción de la preparación en seguridad informática desde EVEA.					
4. Concepción de la preparación en seguridad informática desde encuentros presenciales.					

¿Cómo valora usted la relación existente entre las fases previstas en la estructuración de la alternativa metodológica B-learning? ¿Qué sugiere transformar?

_____

_____

¿Cómo valora usted los aspectos asumidos para la elaboración del programa de preparación en seguridad informática y su relación con el diseño de las unidades didácticas previstas? ¿Qué sugiere modificar?

_____

_____

¿Cuál es su criterio en relación a los aspectos tenidos en consideración en el diseño del proceso de preparación en seguridad informática desde EVEA y de forma presencial?

_____

_____

Otras valoraciones y sugerencias que desee realizar:

_____

_____

_____

Anexo 8. Encuesta aplicada a especialistas.

Procesamiento de los datos.

Encuestados	Documentos			
	D1	D2	D3	D4
Especialista 1	5	5	5	5
Especialista 2	5	5	5	5
Especialista 3	5	5	4	4
Especialista 4	5	4	5	5
Especialista 5	5	5	5	5
Especialista 6	5	3	5	5
Especialista 7	5	5	5	5
Especialista 8	5	5	5	5
Especialista 9	5	5	5	5
Especialista 10	4	5	5	5
Especialista 11	5	3	5	5
Especialista 12	5	5	5	5
Especialista 13	5	5	5	5
Especialista 14	3	5	4	5
Media	**4,79**	**4,64**	**4,86**	**4,93**

Tabla de frecuencias.

Documentos	Categorías				
	C1	C2	C3	C4	C5
D1	0	0	1	1	12
D2	0	0	2	1	11
D3	0	0	0	2	12
D4	0	0	0	2	13

Tabla de por ciento.

Documentos	Categorías				
	C1	C2	C3	C4	C5
D1	0%	0%	7%	7%	86%
D2	0%	0%	14%	7%	79%
D3	0%	0%	0%	14%	86%
D4	0%	0%	0%	14%	93%