Ciencia y Progreso
Publicada en línea: enero 2021, RNPS: 2477, ISSN: 2707-7098
http://cienciayprogreso.cug.co.cu

La preparación en seguridad informática del docente en la Educación Técnica y Profesional
The preparation in Informatics security of the teacher in Technical and Professional Education

Esteban Fernández-Sánchez; Dania Roman-Cruañes

Universidad de Guantánamo

Correo(s) electrónico(s)
estebanfs@cug.co.cu
daniarc@cug.co.cu
ORCID: https: //orcid.org/: 0000-0001-9493-2527
https: //orcid.org/: 0000-0002-6368-9816

Recibido: 20 de septiembre de 2020
Aceptado: 26 de noviembre de 2020

Resumen

Se propone una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática del docente de las instituciones educativas de la ETP del Ministerio de Educación (MINED) en la provincia Guantánamo. Se expone la estructuración de las diferentes fases o etapas a utilizar durante el proceso de preparación en seguridad informática del docente de forma presencial y a distancia con el empleo de entornos virtuales de enseñanza aprendizaje.

Palabras clave: Alternativa metodológica B-learning; Seguridad informática; Entornos virtuales de enseñanza aprendizaje; Moodle

Abstract

A methodological alternative B-learning is proposed to improve the preparation in computer security of the teacher of the education institutions of the ETP del MINED in Guantánamo. It is exposed, the structure of the different phases or stages to be used during the teacher's*informatics*security preparation process is exposed in personal and remotely with the environments.

Keywords: B-Learning Methodological Alternative; Informatics Security; Virtual Surroundings of Teaching Learning; Moodle

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).

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 la sociedad, y 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. (Hurtado, 2015).

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, que provoca, entre otras cuestiones, la pérdida de información y la denegación de servicios.

En correspondencia, González (2008), plantea 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.

En este mismo sentido, Bidot (2012), 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" (p. 21).

Sobre esta misma idea, Rodríguez (2012, p. 4), director de Informática Educativa del Ministerio de Educación, al realizar un análisis sobre la situación relacionada con los usuarios de las TIC y la seguridad informática, destacó:

1- 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.

2- 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.

Otros autores como Borghello (2001), Bisogno (2004), Mayol (2006), Monzón (2009), Peñalver (2010), Hernández (2012), Valdés (2012), han abordado el tema de la preparación en seguridad informática dirigida a profesionales de la especialidad informática como: responsables de seguridad informática, administradores de red, y 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 solo se manifiesta en la formación inicial del técnico medio y de licenciados en educación, especialidad Informática, en las instituciones educativas del Ministerio de Educación (MINED), sino también en la formación de ingenieros informáticos. Por ello, desde el mes de septiembre del año 2008 se han desarrollado cursos de superación por los especialistas de la empresa cubana Desoft perteneciente al Ministerio de la Informática y las Comunicaciones, y a partir del curso escolar 2018 - 2019 se inició en algunas universidades cubanas la formación de especialistas en seguridad informática para contribuir a solucionar la problemática antes planteada.

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 para 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.

Sin embargo, la sistematización que hemos efectuado ha permitido determinar algunos contenidos que, a pesar de su importancia, se han dejado de tratar. Entre estos están: 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 de las carencias antes mencionadas, fue necesaria, la realización de una exploración relacionada con la preparación en seguridad informática de los docentes que laboran en la Educación Técnica y profesional (ETP) de la provincia Guantánamo, en específico aquellos centros educacionales que están destinados a la formación de profesionales de la rama informática, sobre esa base, se tomó como premisas: la observación del desempeño en cuanto al uso de seguro de las TIC, el análisis de seminarios nacionales de preparación para docentes desde el año 2015 hasta el año 2020, así como el intercambio de ideas con los metodólogos de la especialidad Informática de las Direcciones Municipales y Provinciales de Educación de Guantánamo, lo que posibilitó llegar a las situaciones problemáticas siguientes:

-
-
-

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 una 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.

Es por ello, que el presente trabajo tiene como objetivo elaborar una alternativa metodológica B-learning para perfeccionar la preparación en seguridad informática del docente que labora en las instituciones educativas de la ETP del MINED en la provincia Guantánamo.

Desarrollo

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.

Dicha estructura presenta un carácter de sistema, destacándose las funcionabilidad 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 (ver Figura 1).

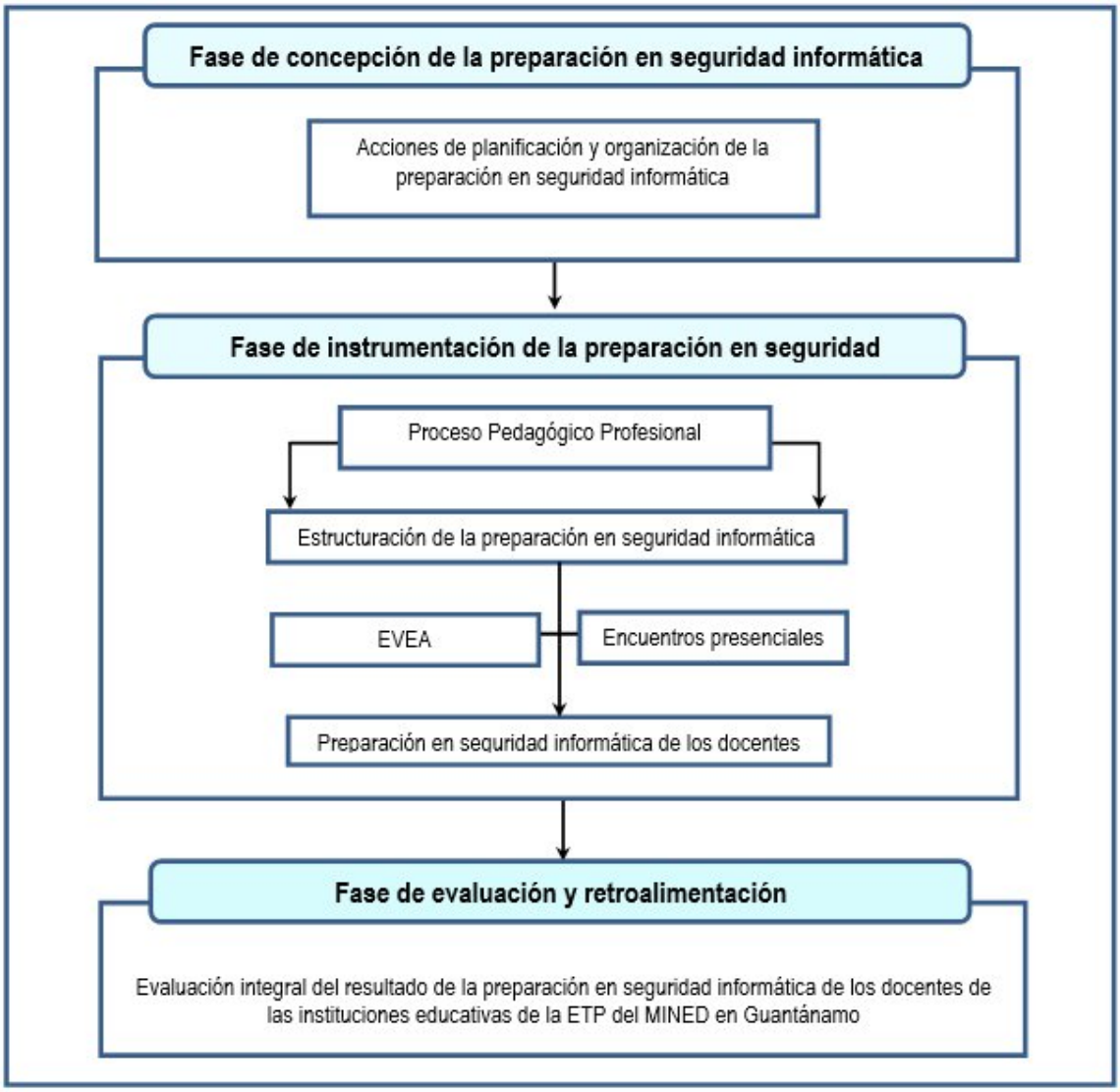

Figura 1. Estructura de la alternativa metodológica B-learning

Fuente: elaboración propia

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.

La primera fase se titula *Concepción de la preparación en seguridad informática*. Esta tiene como finalidad llevar a cabo 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 en la institución educativa.

A consideración de los autores de este trabajo, 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.

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*:*

-
-
-

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 para el desarrollo de cursos a distancia debido a las grandes posibilidades que brinda, tales como:

-
-
-
-
-
-
-

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:

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.

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 de las entidades educativas dándole salida a través de los espacios destinados a la preparación de los docentes desde las actividades de reciclaje.

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.

Desde el punto de vista de los autores de este trabajo, 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 la plataforma Moodle a utilizar, 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 servirá como medio para reforzar todo lo aprendido no de forma aislada sino como un eslabón más de la preparación iniciada en el entorno virtual seleccionado.

Como se ha podido apreciar, para el éxito de la preparación en seguridad informática de los docentes, 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 aprendiz tendrá la posibilidad de exponer sus criterios, ideas, dudas, sugerencias, inquietudes, para así enriquecer las acciones de preparación en seguridad informática desarrolladas.

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.

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.

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.

Por tal razón, la evaluación debe conducir al análisis crítico del desarrollo alcanzado por los docentes 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 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.

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.

Lo expuesto con anterioridad, tiene un sustento en el Reglamento de Seguridad para las Tecnologías de la Información, Ministerio de la Informática y las Comunicaciones. (2019), Resolución 360/2019, donde el artículo 22, se aborda como aspecto importante lo relacionado con la determinación de las responsabilidades que se le atribuye a cada usuario de los diferentes sistemas informáticos.

A su vez, este trabajo tiene como sustento la definición de alternativa dada por Valle (2012), cuando plantea que es:

> 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. (193)

Lo que 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.

Por tal razón, la alternativa propuesta constituye una opción metodológica 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, 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.

Conclusiones

La alternativa metodológica propuesta fue elaborada teniendo en cuenta las condiciones de las instituciones educativas de la ETP en la provincia Guantánamo, y el modo de actuación profesional del docente que aquí labora. Promueve una forma flexible de preparación en seguridad informática, derivada del uso ético, responsable y seguro de las TIC. Brinda desde lo pedagógico la posibilidad de utilizar una herramienta tecnológica multiplataforma que facilita no sólo la inserción y actualización sistemáticamente de la información disponible, sino también el uso de herramientas para la actividad y la comunicación.

La forma en que se proyecta la alternativa elaborada contribuye a la búsqueda de nuevos conocimientos en materia de seguridad informática de una forma colaborativa y reflexiva, y su posterior utilización en los diferentes procesos educacionales.

Referencias bibliográficas

Bidot, J. (2012). *Escenario de la seguridad informática en los inicios del 2013*. Recuperado de http://www.segurmatica.cu

Bisogno, M. V. (2004). *Metodología para el aseguramiento de Entornos Informatizados*. (Tesis de grado). Universidad de Buenos Aires, Argentina.

Borghello, C. F. (2001). *Seguridad Informática. Sus implicancias e implementación*. (Tesis de licenciatura). Universidad Tecnológica Nacional de México.

González, M. (2008). Ética aplicada a la informática: un reto para el desarrollo social. *Revista Cubana de Ciencias Informáticas* Vol. 2. No. 1-2, Enero-Junio, 2008. Recuperado de https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=40&path%%5B%5D=39

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,

Hurtado, F. (2015*). Introducción de las Tecnologías de la Información y las Comunicaciones, su impacto en el aprendizaje de los estudiantes*. La Habana: Pueblo y Educación.

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.

Ministerio de las Comunicaciones (2007). Resolución 127/2007, *Reglamento de Seguridad para las Tecnologías de la Información.* Recuperado de https://www.mincom.gob.cu/es/documento-legal/resolución-127-2007.

Ministerio de la Informática y las Comunicaciones. (2019). Resolución 360/2019, Reglamento de Seguridad para las Tecnologías de la Información. Disponible en: https://www.mincom.gob.cu/es/documento-legal/resolución-360/2019.

Monzón, C. J. (2009). *Auditoría de seguridad de redes inalámbricas de área local.* (Tesis de grado). Universidad Mayor de San Andrés. Bolivia.

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.

Rodríguez, A. M. (2012). *Una concepción teórico-metodológica para la educación en seguridad informática del personal de las instituciones del ministerio de educación*. (Tesis de doctorado). Instituto Pedagógico Latinoamericano y Caribeño (IPLAC).

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.

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