UNIVERSIDAD DE SANCTI SPÍRITUS
José Martí Pérez

FACULTAD: CIENCIAS TÉCNICAS Y EMPRESARIALES

CARRERA: EDUCACIÓN LABORAL INFORMÁTICA

TRABAJO DE DIPLOMA

TÍTULO: TAREAS DOCENTES PARA EL APRENDIZAJE DE LA SEGURIDAD INFORMÁTICA EN LOS ESTUDIANTES DE 7MO GRADO.

Autor: Angel Miguel Gutiérrez Valdivia

Tutora: Profesor Auxiliar, Lic. Niurka de las Mercedes González Acosta, Dr. C.

Sancti Spíritus

2019

PENSAMIENTO

“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: las personas que usan y administran los ordenadores”. (Mitnick, 1990)

DEDICATORIA

Le dedico este trabajo en primer lugar a Dios, Él con su infinita misericordia ha puesto su mano en todos los aspectos de mi vida, y ha hecho posible que yo llegue hasta aquí, a pesar de las adversidades y los contratiempos.

A mi madre la Virgen María, que con su manto fraterno me ha acogido siempre, me ha ayudado y me ha cuidado para que pueda terminar este trabajo. Ella que siempre vela por mí y los míos para que nada les falte, a Ella mi amor.

A mis padres, los que se han sacrificado junto a mí por esta carrera, por sus noches de desvelo, sus empujes, sus fuerzas, por el ánimo necesario en los momentos de cansancio, sus palabras de aliento, porque son el sentir de mi vida y porque les debo mi vida.

A mi familia, a los que viven, porque han sido fuente de inspiración, y me han ayudado a consolidar aspiraciones, deseos y me han mostrado el camino cuando la luz ha faltado, y a los que no viven, porque sé que desde el cielo me cuidan y rezan por mí, en especial mi abuela que se hubiera sentido muy orgullosa de este título.

A mi esposa que me ha acompañado en el último tramo del camino, a ella que ha sufrido los largos viajes entre provincias, que ha tenido que batallar con la casa en muchas ocasiones sola, a ella que me ha dado fuerzas y ánimos, todo mi amor, también le dedico este trabajo.

AGRADECIMIENTOS

Agradezco una y mil veces la realización de este trabajo, a mi tutora la profesora Niurka, que ha tenido que cargar conmigo, y hacer magia para que de una idea nazcan tantas cosas buenas, como esta, le agradezco porque se ha sobrepuesto de situaciones muy difíciles y no ha dejado en ningún momento de estar a mi lado, acompañarme y guiarme por este camino, mi gratitud eterna.

A mis profesores, los cuales mencionar sería interminable y correría el riesgo de olvidar alguno, ellos que con su sabiduría y su paciencia han moldeado nuestra inteligencia y han obtenido lo mejor de nosotros.

A mis amigos, que me han apoyado siempre, ellos, son uno de los motores que han movido este mecanismo y han ayudado a que fuera una mejor persona a ellos, gracias.

No puede faltar una persona muy especial para mí, que como segunda madre ha luchado conmigo, ha cargado conmigo en mis momentos de flaqueza, me ha felicitado y me ha corregido desde el cariño y el amor fraterno, es el único nombre que mencionaré, Mercedes Polanco Prado, a ella le debo parte del profesor que soy, a ella le debo mi carrera, ella me motivó cuando me hacía falta redirigir el curso de mi vida, ella me aconsejó como ser una mejor persona y un buen educador, ella me dio aliento y me guió por este camino de la docencia, gracias Merce.

Para concluir no puedo dejar de mencionar a las Religiosas del Sagrado Corazón de Jesús. Esas maestras de la mente y el alma, que han forjado en mi el amor por los niños, el amor que hay que tener para educar, ellas con su sabiduría y ejemplo han impregnado en mi toda la obra evangelizadora y educativa de su comunidad que he tratado de transmitir a mis alumnos, a ustedes que Dios les bendiga, muchas gracias.

RESUMEN

Las instituciones educativas tienen la tarea de preparar a los estudiantes para que sean usuarios responsables de las tecnologías que se encuentran a su disposición y dominen las medidas necesarias para dar cumplimiento a la política de Seguridad Informática, que permitan la protección y cuidado al hardware y el software. La principal causa que condujo a la realización de esta investigación lo constituyó la existencia de un insuficiente aprendizaje de los estudiantes de 7mo grado en los temas relacionados a los riesgos, amenazas y agresiones existentes a la seguridad informática. Para resolver esta problemática se planteó como objetivo: proponer tareas docentes para contribuir con el aprendizaje de los contenidos sobre Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea. En la realización de este trabajo se emplearon varios métodos de la investigación educacional, del nivel teórico: el analítico y sintético, el inductivo y deductivo y el histórico y lógico; del nivel empírico: la observación, la entrevista a estudiantes, el análisis documental y la prueba pedagógica. Además se utilizó la estadística descriptiva y como procedimiento el cálculo porcentual.

ABSTRACT

Educational institutions have the task to prepare students to be responsible users of the available technologies at their disposal and in this way they can master the required measures to fulfill the politics of Informatic Safety that allow the care and protection of the hardware and software. The main reason for the realization of this research was the insufficient knowledge on the 7th grade students according to themes regarding the risks, threads and aggressions in relation to Informatic Safety. In order to solve this issue, the following problem was stated: to propose teaching tasks to contribute with the learning of the contents about the Informatic

Safety in 7th grade students of Ramón Leocadio Bonachea high school. From the theoretical level, some methods were used in this educational investigation: the analytical and synthetic, the inductive and deductive and the historical and logical; and from the empirical level: the observation, the interview to the students, the documental analysis and the pedagogical test. Besides the methods previously mentioned, the descriptive statistic and the percentual calculus as the procedure were conveyed.

ÍNDICE

Contenido

Introducción

En la escuela cubana actual se encuentra los llamados “nativos informáticos”, generación caracterizada por hacer un uso excesivo de las tecnologías y permanecer conectados a las redes en busca de contenidos diversos y de otros usuarios para compartir diferentes tipos de datos.

En ocasiones, los jóvenes no se percatan de los riesgos a los que están expuestos cuando se encuentran conectados, fundamentalmente aquellos que afectan la integridad de los datos. Por lo antes expuesto es necesario tener conocimiento sobre los temas relacionados con la Seguridad Informática, para mantener un control estricto sobre la información, los medios donde se almacenan y los dispositivos usados para trabajar.

La Seguridad Informática en Cuba, es un factor crucial, dentro de todas las políticas del Estado, y fundamentalmente de las Instituciones Estatales, debido a que regula el uso adecuado de las tecnologías y qué hacer en caso de detectarse una infracción.Tener conocimiento sobre la misma ha sido una preocupación por parte del Ministerio de Educación (MINED) es por esto que en los planes de estudio de la asignatura de Informática aparece con el objetivo de insistir en la necesidad de ser conscientes, cuidadosos y precavidos a la hora de utilizar las tecnologías.

En Secundaria Básica, los contenidos referentes a la Seguridad Informática solo se trabajan en el Programa de Informática en 7mo grado particularmente en la Unidad 2: Controlando la computadora, dónde se centra en conocer las precauciones que se deben tener en cuenta al utilizar dispositivos de almacenamiento externos (disquete, memoria USB, entre otros) para evitar infecciones por virus y aplicar un programa antivirus a dispositivos de almacenamiento (Fuerte, Labañino y Galán, 2016). Estos contenidos no se encuentran actualizados a partir de los adelantos que hoy se encuentran en la sociedad tales como: el uso de los correos electrónico, la búsqueda y navegación internacional por la Wi-Fi de ETECSA, o la navegación nacional, a la que los estudiantes tienen acceso desde la escuela.

La experiencia del autor como docente en la Escuela Secundaria Básica Urbana (ESBU) Ramón Leocadio Bonachea le ha permitido constatar como los estudiantes aunque muestran, en pocas ocasiones, cuidado con la información que tienen en las memorias, en sentido general no realizan el chequeo al colocar una memoria en la PC, no mantienen sus puestos de trabajo limpios, ingieren alimentos en los laboratorios, introducen material audiovisual, música y juegos a las estaciones de trabajo, cambian parámetros establecidos en los escritorios de las computadoras y desconocen las políticas de la Seguridad Informática para los centros docentes, además en los laboratorios no se exige el cumplimiento de las acciones contenidas en el Plan de Seguridad Informática.

Por otra parte, en el análisis realizado al programa de estudio de este nivel de enseñanza se constató que los contenidos están dirigidos básicamente al conocimiento de los programas malignos y los softwares que permiten la protección, de allí que se presente la siguiente problemática:

Existe insuficiente conocimiento en los temas relacionados con la Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea

Por la necesidad de minimizar la situación anterior se formula el siguiente problema científico: ¿Cómo contribuir con el aprendizaje de los contenidos sobre Seguridad Informática en la secundaria básica?

Por lo antes expuesto se plantea el siguiente objetivo: Proponer tareas docentes para contribuir con el aprendizaje de los contenidos sobre Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea

El proceso de resolución del problema de investigación llevó al planteamiento de las siguientes preguntas científicas:

1. ¿Cuáles son los fundamentos teóricos que sustentan el aprendizaje de la Seguridad Informática en secundaria básica a través de tareas docentes?
2. ¿Cuál es la situación actual de los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea acerca del aprendizaje de la Seguridad Informática?

3. ¿Qué tareas docentes se podrán elaborar para contribuir con el aprendizaje sobre Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea?
4. ¿Qué resultados se obtuvieron al aplicar las tareas docentes para contribuir con el aprendizaje sobre Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea?

Para darle cumplimiento al objetivo del trabajo y respuesta a las preguntas formuladas, se tienen en cuenta las siguientes tareas de la investigación:

1. Determinación de los fundamentos teóricos que sustentan el aprendizaje de la Seguridad Informática en secundaria básica a través de tareas docentes.
2. Diagnóstico de la situación actual que tienen los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea en el aprendizaje sobre la Seguridad Informática.
3. Elaboración de tareas docentes para contribuir con el aprendizaje sobre Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea.
4. Constatación de los resultados de la aplicación de las tareas docentes para contribuir con el aprendizaje sobre Seguridad Informática en los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea.

Para la realización de esta investigación se emplearon los siguientes métodos de nivel teórico:

Histórico y lógico: permitió estudiar los principales fundamentos teóricos que sustentan el aprendizaje de la asignatura Informática, así como los temas relacionados con la Seguridad Informática.

Analítico y sintético: facilitará realizar el análisis de los datos e informaciones obtenido durante el diagnóstico del aprendizaje a los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea.

Inducción y deducción: permitirá hacer inferencias sobre los cambios que se producirán en el aprendizaje de la asignatura Informática en los temas relacionados con la Seguridad Informática, a partir de las insuficiencias diagnosticadas.

Los métodos del nivel empírico utilizados permiten comprobar en la práctica pedagógica cómo se manifiesta el objeto de la investigación, así como la constatación de los resultados alcanzados después de aplicada la propuesta, para ello se utilizó:

La observación pedagógica: permitió constatar cómo se manifiestan y el nivel de aprendizaje de los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea sobre la Seguridad Informática. Además, posibilitó determinar cómo se conciben acciones para lograr que los estudiantes se apropien de las principales normas sobre Seguridad Informática. (Anexo 1)

La entrevista a estudiantes: para la recogida de información empírica que afianzó la constatación inicial del problema. (Anexo 2)

El análisis documental: para constatar los aspectos esenciales del programa de estudio de Informática en 7mo grado, especialmente lo referido a la temática de Seguridad Informática y los documentos normativos, orientaciones metodológicas y los planes de clases preparadas por el colectivo de trabajadores.(Anexo 3)

El experimento: Se empleó en su variante de pre-experimento en el registro y comparación del nivel de aprendizaje sobre la Seguridad Informática en el pre-test y pos-test para evaluar la aplicación de la propuesta. (Anexos 4 y 5)

Los métodos del nivel matemático y/o estadístico permitieron tener una tabulación de datos que mostraron la línea base de cómo estaba el desarrollo del proceso antes de iniciar y luego de aplicar las tareas docentes.

El cálculo porcentual: permite mediante la utilización de tablas el análisis de los resultados y el procesamiento de datos.

La estadística descriptiva: se emplea para determinar la media; además, para la confección de tablas de frecuencias y en la representación gráfica de los resultados. Unidad de estudio y decisión muestral.

Se tomará como población la matrícula 7mo grado de la ESBU Ramón Leocadio Bonachea consistente en 200 estudiantes y la muestra los 40 estudiantes del grupo de 7mo 1. Se toma como muestra este grupo pues mediante la utilización de instrumentos pedagógicos se ha detectado que existe un insuficiente conocimiento sobre la Seguridad Informática ya que los estudiantes aunque en su

mayoría son asiduos al uso de las tecnologías informáticas desconocen lo que son los virus informáticos, como estos pueden afectarles a ellos y a su familia en el ámbito económico, no pasan el antivirus en las computadoras, introducen memorias con contenidos que no están permitidos en un centro educativo y no tienen cuidado al dejar abiertas las secciones de trabajo en la computadora.

Importancia del trabajo: está en la elaboración de tareas docentes para perfeccionar el proceso de enseñanza aprendizaje de la Seguridad Informática. Estas tareas posibilitarán la concientización de los estudiantes sobre la importancia de la Seguridad Informática y posterior puesta en práctica de la misma. Esta investigación también aportará al maestro herramientas y técnicas para trabajar la Seguridad Informática en las clases ya que las tareas al ser flexibles así lo permiten.

La actualidad está dada en la incorporación en el proceso de enseñanza aprendizaje de Informática del nivel de secundaria básica de contenidos actualizados de Seguridad Informática a tono con los adelantes tecnológicos que se han producido en los últimos tiempos.

Desarrollo

1.1 Antecedentes históricos de la Seguridad Informática.

Uno de los pioneros en el tema de la Seguridad Informática fue James Anderson quien, en el año 1980 solicitado por el gobierno de Estados Unidos, produjo uno de los primeros escritos relacionados con el tema, y desde entonces, se sientan las bases de palabras que hoy se asumen como naturales en este ámbito de la Seguridad Informática, pero que por aquella época parecían ciencia ficción.

Hasta finales de 1988 en el mundo muy pocas personas tomaban en serio el tema de la seguridad en redes de computadores de propósito general. Mientras que por una parte Internet iba creciendo exponencialmente con redes importantes que se adherían a ella, como bitnet o hepnet, por otra el auge de la informática de consumo unido a factores menos técnicos iba produciendo un aumento espectacular en el número de piratas informáticos.

El 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la Seguridad Informática: uno de sus programas se convirtió en el famoso Worm o gusano de Internet. Miles de ordenadores conectados a la red se vieron inutilizados durante días y las pérdidas se estimaron en millones de dólares. (Villalón, 2002).

Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. Poco después de este incidente, y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos estadounidenses (en general, a los sistemas de cualquier país) la agencia DARPA (Defense Advanced Research Projects Agency) creó el CERT (Computer Emergency Response Team), un grupo formado en su mayor parte por voluntarios cualificados de la comunidad informática, con el objetivo principal de facilitar una respuesta rápida a los problemas de seguridad que afecten a hosts de Internet.

Para tener un acercamiento a este tema el autor considera necesario examinar algunas de las definiciones concebidas por varios investigadores sobre Seguridad Informática. En la EcuRed (2010) se define que la Seguridad Informática es:

> (…) un estado de cualquier tipo de información (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

Por su parte Ávila (2009) fundamenta que la Seguridad Informática tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información. Además, expresan que es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias:

1. Confidencialidad: Protege los Activos de Información contra accesos o divulgación no autorizados.
2. Integridad: Garantiza la exactitud de los Activos de Información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
3. Disponibilidad: Asegura que los Recursos Informáticos y los Activos de Información pueden ser utilizados en la forma y tiempo requeridos. Bajo el punto de vista de seguridad, la disponibilidad se refiere a su posible recuperación en caso de desastre (Recuperabilidad). Estos aspectos llevan implícitos los conceptos de Propiedad, Depósito y Uso, de los Recursos Informáticos y Activos de Información.

El investigador Urbina (2016) plantea que:

> (…) es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenaza, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.

En estos estudios se coincide en la importancia de la protección de la información y los sistemas informáticos y la necesidad de poseer una cultura informática que garantice la integridad y privacidad de la información. A criterio del autor la Seguridad Informática, es una serie de métodos y estrategias desarrolladas para prevenir y proteger los equipos informáticos o de información individual y

conectada en una red frente a daños accidentales o intencionados ocurridos ya sea por la acción del hombre o de la naturaleza.

El investigador Aneiro (2001) al profundizar en lo concerniente a la Seguridad Informática expresa que esta se divide, para su estudio, en dos grandes grupos: la seguridad física y seguridad lógica. Entendiendo la seguridad física aquella que se relaciona normalmente con temas de políticas de seguridad, normativas, planes de contingencia, la protección física de los datos, gestión de la seguridad, accesos, auditoria, leyes. Y, la seguridad lógica orientada hacia la protección de la información en su mismo medio, ya sea generación, almacenamiento y transmisión; usando en este caso por lo general herramientas, técnicas y esquemas propios de la criptografía. Ambas formas de Seguridad Informática se complementan, una no puede plantearse sin la otra, siendo esta una especialidad emergente donde convergen un alto número de disciplinas y temas muy específicos.

1.2 La Seguridad Informática en Cuba

En Cuba cuando apenas se contaba con una tecnología incipiente se le prestó especial atención al tema de la Seguridad Informática. A principio de los 90 debido a la crisis de la caída del Campo Socialista, Cuba se quedó sin un proveedor confiable que pudiera ayudarlo en la lucha contra las amenazas informáticas que sobre la Isla se cernían. No es hasta 1995 que nace Segurmática Antivirus, una empresa de consultoría y seguridad informática, con el objetivo de comercializar productos antivirus, brindar asesoría, así como otros servicios relacionados con la Seguridad Informática.

Sin embargo, años antes del surgimiento de Segurmática ya había sido aislado en Cuba en 1988 el primer virus internacional, nombrado Vienna.648. En 1991 se detectó el TerminatorA, primero desarrollado en el archipiélago cubano.

Hoy se habla de unos 200 programas creados en Cuba o para ella, aunque ninguno de estos se ha considerado más destructivo que el W32.vrbat, un caballo de Troya (programa aparentemente legítimo e inofensivo, hasta que activa su ataque) aislado en agosto de 2011.

Unido al surgimiento de Segurmática se establecieron textos legales como el Reglamento de Seguridad Informática, emitido por el Ministerio del Interior en 1996, el cual estipula que todos los ministerios y organismos centrales de la Administración Central del Estado, así como empresas y otras instituciones de Educación deben analizar, confeccionar, aplicar planes de Seguridad Informática y de contingencia; para reducir el riesgo de afectaciones a los recursos informativos, por la acción de catástrofes naturales o artificiales, de fraudes, de errores humanos, de los propios programas malignos o de otra naturaleza.

Los avances tecnológicos han hecho necesario la actualización de las políticas sobre Seguridad Informática estableciéndose la Resolución 127 de 2007 en la que el Ministro de la Informática y las Comunicaciones, resolvió aprobar y poner en vigor el Reglamento para las tecnologías de la información, que regulariza el funcionamiento del sistema informático en el país.

En el caso del Ministerio de Educación fue en el año 1999 que se establece el primer Plan de Seguridad Informática (con el inicio del funcionamiento de la red del Organismo Central), donde se precisaron las medidas técnicas, físicas y lógicas para proteger la información y todos los activos informáticos, no solo para el organismo sino para todos los centros educacionales y empresas. De acuerdo a lo anterior, el Ministerio de Educación, dictó la Resolución 176/07 que no es más que el Reglamento que trata sobre la Seguridad Informática en el Ministerio la cual está actualmente vigente, la misma tiene como objetivo establecer los principios que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

Hoy día, no existen sistemas completamente seguros, por lo que se hace necesarios buscar los aspectos vulnerables; por tanto, crear conciencia a los directores, docentes y alumnos de la necesidad de la seguridad, puesto que la mayor cantidad de ataques se produce por usuarios de las propias instituciones. Los usuarios deben conocer las políticas de seguridad con el fin de interiorizar las implicaciones que su desconocimiento ocasionaría.

1.3 El aprendizaje sobre Seguridad Informática.

Para profundizar en el término aprendizaje sobre la Seguridad Informática se hizo necesario considerar los estudios realizados respecto al proceso de enseñanza aprendizaje por varios investigadores como Álvarez, (1999); Zilberstein, (2004); Addine, (2004) y otros.

Para la investigadora Silvestre el proceso de enseñanza aprendizaje:

> (…) tiene lugar en el transcurso de las asignaturas y tiene como propósito esencial contribuir a la formación integral de la personalidad del estudiante, constituyendo la vía mediatizadora fundamental para la adquisición por éste de los conocimientos, estrategias de aprendizaje, normas de comportamiento, valores, es decir, la apropiación de la experiencia histórico social acumulada por las generaciones precedentes. (2001)

Para Addine (2004) el proceso de enseñanza aprendizaje:

> (…) se concreta en una situación creada para que el estudiante aprenda a aprender. Se constituyen en un proceso dialéctico donde se crean situaciones para que el sujeto se apropie de las herramientas que le permitan operar con la realidad y enfrentar al mundo con una actitud científica, personalizada y creadora.

Estos autores reflejan la misión esencial de este proceso, donde los estudiantes se apropian de los diferentes elementos del conocimiento y de procedimientos para su actuación de acuerdo a las normas y valores de la sociedad en que vive, expresado en el contenido de enseñanza, en estrecho vínculo con el resto de las actividades docentes, sin descuidar el papel del docente para estimularlo, dirigirlo y controlarlo.

En el proceso de enseñanza aprendizaje se potencia el aprendizaje cuando se creen situaciones en las que el sujeto se apropie de las herramientas que le permitan operar con la realidad y enfrentar al mundo con una actitud científica, personalizada y creadora.

La investigadora Talizina (1988) expresa que el aprendizaje es un proceso en el que participa activamente el alumno, dirigido por el docente, apropiándose el primero de conocimientos, habilidades y capacidades, en comunicación con los otros, en un proceso de socialización que favorece la formación de valores,

socialización que favorece la formación de valores, "es la actividad de asimilación de un proceso especialmente organizado con ese fin, la enseñanza."

La autora Fernández (1997) al profundizar en el tema define que el aprendizaje es:

> (…) la actividad que desarrolla el estudiante para aprender, para asimilar la materia de estudio, y además, es el resultado y el proceso que dirige el profesor, es la enseñanza, que tiene en la materia de estudio el medio mediante el cual se aprende.

En la escuela cubana se trabaja para lograr que este aprendizaje conduzca a que el estudiante sea el gestor de su conocimiento y participe activamente y de forma consciente en él. La investigadora Castellano (2002) lo define como

> (…) el proceso dialéctico de apropiación individual de los contenidos y formas de conocer, hacer, convivir y ser, construidos en la experiencia socio histórica, en el cual se producen, como resultado de la actividad del individuo y de la interacción con otras personas, cambios relativamente duraderos y generalizables, que le permiten adaptarse a la realidad, transformarla y crecer como personalidad.

Estas definiciones incluyen los cuatro pilares básicos que aparecendefinidos en el informe de la (UNESCO 1996: 4) sobrela educación hacia el siglo XXI: aprender a conocer, aprender ahacer, aprender a convivir y aprender a ser.

El aprendizaje se logra en la medida en que se promueve el desarrollo de los estudiantes, para que puedan pasar de un nivel de desarrollo a otro superior. En tal sentido se concibe el aprendizaje como un proceso dialéctico, individualizado, vinculado estrechamente con al contexto histórico-cultural, con las experiencias y las necesidades de los individuos, así como con su crecimiento humano, con el desarrollo de su personalidad.

Tomando en consideración lo antes expuesto el aprendizaje sobre Seguridad Informática debe distinguirse por ser activo y regulado. Esto requiere que el estudiante sea protagonista de su propio aprendizaje, ser consciente y comprender por qué aprende, hasta dónde llegar, el qué y cómo aprende. Para ello se debe propiciar un proceso de aprendizaje con análisis críticos, problémico, con un pensamiento alternativo, flexible y original. Además, se debe propiciar que

lo que el estudiante aprende posea sentido, valor y utilidad para el proceso de socialización e individualización de los estudiantes.

A continuación, se hace referencia a los contenidos principales abordados en el grado que forman parte de la Seguridad Informática, tomado del Programa de Computación para la Educación Secundaria Básica:

- Entre los objetivos se persigue que cuiden y conserven de forma organizada su puesto de trabajo.
- Los virus informáticos. Nociones de Seguridad Informática, medidas básicas para la protección de la información y cuidado del equipamiento. Los virus informáticos, programas para proteger la información: antivirus. Aplicando un programa antivirus

El aprendizaje de estos contenidos debe caracterizarse por:

- Potenciar en los estudiantes la apropiación activa y creadora de la cultura informática y de seguridad.
- Representar aquella manera de aprender y de implicarse en el propio aprendizaje que garantice el tránsito del control del proceso por parte del docente al control por parte de los estudiantes
- Conducir al desarrollo de actitudes, motivaciones y herramientas necesarias para el dominio de los contenidos sobre Seguridad Informática de manera creativa e independiente.

Para contribuir conel aprendizaje de estos contenidos se precisa de un cambio esencial en la concepción y forma de la tarea docente en el proceso de enseñanza aprendizaje porque es en este tipo de actividad donde se concretan las acciones y operaciones a realizar por el estudiante.

2. Tareas docentes para contribuir con el aprendizaje sobre Seguridad Informática en los estudiantes de 7mo1 en la ESBU Ramón Leocadio Bonachea.

Con el diagnóstico del estado inicial de los estudiantes del 7mo1 en la ESBU Ramón Leocadio Bonachea, en cuanto a la Seguridad Informática, se fundamenta las tareas docentes desde el punto de vista pedagógico, se manifiestan sus

características, desde el planteamiento del objetivo general, la descripción de cada una de las tareas docentes y la forma de implementación que se sugiere.

2.1 Diagnóstico de los estudiantes del 7mo1 en la ESBU Ramón Leocadio Bonacheasobre Seguridad Informática.

Como paso previo, en el diseño de las tareas docentes sobre la Seguridad Informática de los estudiantes del 7mo1 de la ESBU Ramón Leocadio Bonachea, se realizó un diagnóstico para conocer el estado real que presentan los estudiantes en relación con el aprendizaje sobre la Seguridad Informática.

El diagnóstico abarcó a 40 estudiantes del 7mo1. Los instrumentos aplicados fueron los siguientes:

- Guía de observación. (Anexo 1)
- Entrevista a estudiantes. (Anexo 2)
- Pre- Test (Anexo 4)

Se observaron 15 actividades docentes con el objetivo de determinar cómo se manifiestan y el nivel de aprendizaje de los estudiantes de 7mo grado de la ESBU Ramón Leocadio Bonachea sobre la Seguridad Informática. Además, posibilitó determinar cómo se conciben acciones para lograr que los estudiantes se apropien de las principales normas sobre Seguridad Informática, arrojando los siguientes resultados:

En la guía de observación pedagógica se pudo determinar que: la frecuencia con la que los estudiantes asisten al laboratorio es bastante poca para un 57.50 % de asistencia a los laboratorios fuera del horario de clases. Además, se pudo constatar que cuando están en el laboratorio fuera del horario de clases utilizan las tecnologías para la recreación en un 60.00 % de las 15 veces que se observó. Se pudo detectar asimismo, que solo el 85.00 % de los estudiantes no pasan el antivirus al colocar un dispositivo USB en la estación de trabajo. Por otra parte, se pudo evidenciar que el 67.50 % de los estudiantes ingieren alimentos, así como toman agua en las estaciones de trabajo y en algunos casos usan indebidamente los periféricos de los clientes ligeros. Se pudo comprobar que el 59.50 % de los estudiantes no conocen el Registro de acceso a la tecnología, el 25.00 % lo llena frecuentemente pero solo el 30.00 % de los estudiantes saben cuál es su utilidad.

Se pudo observar que solo el 17.50% de los estudiantes conocen del Plan de Seguridad Informática de la escuela y el 28.57 % de ellos saben cuándo están infringiendo dicho Plan de Seguridad Informática.

En la entrevista a estudiantes con el objetivo de determinar los conocimientos que poseen acerca de la Seguridad Informática se pudo determinar que: el 62.50 % de la muestra solo tienen alguna noción sobre Seguridad Informática. El 72.50 % no conoce que son los virus informáticos y el 5.00 % conoce elementos para caracterizarlos. El 82.50 % de los estudiantes del 7mo 1 no conocen que deben hacer para evitar infectarse en sus dispositivos con algún virus informático y el 15.00% conoce como contribuir a que exista una buena Seguridad Informática en el centro.

El resultado del instrumento aplicado demuestra que existen insuficiencias en los estudiantes sobre la Seguridad Informática. Se corrobora que los estudiantes presentan limitaciones en el conocimiento de lo que es la Seguridad Informática y la forma que pueden contribuir a ella.

En la prueba pedagógica inicial (pre-test) aplicada con el objetivo de determinar el nivel de conocimientos que presentan los estudiantes se constató que el 70.00 % de ellos desconocen de grados anteriores que deben pasar el antivirus a los dispositivos de almacenamiento que se inserten, mientras que un 51.50 % afirman que consumen alimentos en el laboratorio. El 59.50 % de la muestra no conoce ni utiliza el Registro de la tecnología en ningún momento; mientras que un 78.60 % de las veces los estudiantes introducen contenidos multimedia en el laboratorio que no son materiales didácticos. (Anexo 6)

Se realizó el análisis documental con el objetivo de constatar los aspectos esenciales del programa de estudio de Informática en 7mo grado, especialmente lo referido a la temática de Seguridad Informática y los documentos normativos, orientaciones metodológicas y los planes de clases, esta constatación arrojó que, si bien lo referente a la Seguridad Informática está implícito en el Programa de 7mo grado, en sus objetivos generales de la disciplina en el nivel y en los objetivos generales de la asignatura en el grado; en la dosificación solo se le conceden dos horas clases al estudio de la Seguridad Informática en la Unidad# 2, enfocada en

el concepto de Seguridad Informática, virus y antivirus informáticos y las medidas para evitar infectarse en con un virus informático. En el caso de los planes de estudio se detecta una mayor deficiencia en el trabajo de la Seguridad Informática donde solo se trabaja en estas dos horas clases, el resto de tiempo no se hace alusión en ninguna otra unidad al tema.

Estos elementos, fundamentan la necesidad de establecer tareas docentes para potenciar la Seguridad Informática en los estudiantes de 7mo 1 en la ESBU Ramón Leocadio Bonachea, que les permita motivarlos y obtener conocimientos sobre la Seguridad Informática.

2.2 Tareas docentes para contribuir con el aprendizaje sobre Seguridad Informática de los alumnos del 7mo1 de la ESBU Ramón Leocadio Bonachea.

Se han detectado dificultades en la preparación sobre la Seguridad Informática en los estudiantes del 7mo 1 de la ESBU Ramón Leocadio Bonachea relacionada con la falta de dominio del tema y el qué hacer para contribuir a su buen funcionamiento, que se manifiesta en las limitaciones en cuanto a los conocimientos para su desempeño en la labor como alumno.

Para resolver esta problemática se escogen las tareas docentes porque estas son una herramienta práctica de apropiación y ejercitación de conocimientos por parte del alumno guiada y orientada por el docente.

Son varios los pedagogos que han definido qué son tareas docentes. El investigador Álvarez de Zayas (1999), plantea que la tarea docente: “es la acción que atendiendo a ciertos objetivos se desarrolla en determinadas condiciones (…) es la acción del profesor y los estudiantes dentro del proceso, que se realiza en ciertas circunstancias pedagógicas, con el fin de alcanzar un objetivo (…) resolver el problema planteado a estudiar por el profesor” (p.101).

Para Sivestre y Zilberstein (2000) la tarea docente son “(…) aquellas que se conciben para realizar por el estudiante en clases y fuera de ésta, vinculadas a la búsqueda y adquisición de los conocimientos y al desarrollo de habilidades.”

En esta investigación se asume esta definición al reafirmar que las tareas docentes son acciones para reforzar la apropiación de conocimientos y promover el desarrollo de los estudiantes orientados, guiados y controlados por el docente.

Para las tareas docentes propuestas se seguirá la siguiente estructura:

- Título de la tarea
- Objetivo
- Actividad
- Evaluación
- Conclusiones

La tareas docentes se ejecutaron fundamentalmente en dos momentos del proceso de enseñanza aprendizaje, durante la clase de Informática (2 horas clases y en los turnos de Tiempo de Máquina, para lograr una asimilación gradual y sistemáticade estos contenidos. Se realizarán en turnos de 45 minutos y estará orientada, motivada, guiada y supervisada por el docente en todos los casos.

Teniendo en cuenta la estructura propuesta se precisan las siguientes tareas docentes para el aprendizaje de la Seguridad Informática de los estudiantes del 7mo 1 en la ESBU Ramón Leocadio Bonachea:

Tarea docente 1.

Título: ¿Qué es la Seguridad Informática?

Objetivo: Caracterizar la Seguridad Informática como una vía para la prevención de delitos informáticos en las escuelas cubanas.

Actividades

Para la formación de un concepto, se necesita investigar en la bibliografía científica que se ha escrito sobre el tema. Anteriormente solo podíamos conformarnos con algunos libros de texto; hoy se pone a nuestra disposición un sitio web con publicaciones científicas diversas y actualizadas a las que podemos acceder gracias al internet, siendo el sitio google académico.

En la dirección URL de google académico que ustedes conocen (https://scholar.google.com.cu/) hoy les propongo investigar sobre la Seguridad Informática:

- ¿Qué es la Seguridad Informática?

- ¿Quiénes están sujetos a la Seguridad Informática?
- ¿Para qué usar la Seguridad Informática?

Una vez investigado sobre estos temas en google académico construiremos juntos el concepto de Seguridad Informática para ello realice las siguientes tareas:

- Escriba en su libreta las palabras que consideres imprescindibles para decir que estamos en presencia de la Seguridad Informática
- Elabore un cuadro resumen con las principales similitudes y diferencias.

Evaluación

1 Se evaluará a los estudiantes de acuerdo a:

- Extracción de las principales palabras claves
- Determinación de las semejanzas y diferencias esenciales

2 Participación de manera destacada en la conformación del concepto de Seguridad Informática.

Conclusiones

Una vez conformado el concepto de Seguridad Informática, se pasa a reforzar los contenidos claves de la investigación realizada como: quienes estamos sujetos a la Seguridad Informática y por qué es necesaria la Seguridad Informática.

Tarea docente 2

Título: ¿Cómo tener mi PC segura?

Objetivo: Evaluarla importancia de la seguridad en las computadoras.

Actividades

Como ustedes saben, tener una computadora que funcione bien, no es cosa fácil, se necesitan tener dos aspectos fundamentales bien asegurados el Hardware y el Software, uno por la necesidad de potenciar el rendimiento, y el otro por tener programas que garantices el funcionamiento óptimo de la unidad.

Nos enfocaremos en el Software, y para ello unas preguntas de marcar:

¿Cómo hacer más segura una computadora?

___ Tener contraseña en las carpetas de películas

___ Tener un antivirus instalado

___ Llenar el Disco Duro de programas innecesarios

___ Actualizar periódicamente el Antivirus.

___ Poner contraseñas de inicio de sección

¿Crear carpetas en la partición donde se encuentra el Sistema Operativos, es seguro?

____ Si ____ No

¿Cuáles son los requerimientos necesarios para una contraseña segura en tu computadora?

_____ Tener hasta 5 caracteres.

_____ Tener más de 8 caracteres.

_____ Tener más de 5 caracteres u poseer mayúsculas y caracteres especiales.

_____ Ser el día de tu cumpleaños o 1234

Generalmente guardamos en nuestras computadoras información valiosa para nosotros, el hacerlas seguras para que no perdamos información o se la roben, es requisito fundamental para todos, por eso hay que asegurarse de tener los programas indispensables para su correcto funcionamiento.

A continuación te dejo una lista de programas que deben tener las computadoras para hacerlas más segura:

- Segurmática Antivirus
- CCleaner
- Winrar
- AdvancedSystemCare

Expresa brevemente cuál es la función de cada uno de estos programas, utilizando la Enciclopedia EcuRed.

Evaluación

Se evaluará a los estudiantes de acuerdo a la participación al responder las interrogantes, y luego a los estudiantes que participen de manera más destacada en la búsqueda de información relacionada a los programas propuestos.

Conclusión

Tener una PC saludable es una necesidad vital hoy en día, y no solo las computadoras si no también los celulares, estos programas sobre los que ustedes buscaron información en el día de hoy también están disponibles para los teléfonos inteligentes, por lo que les recomiendo que estas acciones que vimos

hoy necesarias para proteger una PC también las tengan en cuenta y las tomen para proteger sus celulares y sobre todo profundicen más sobre estos programas y sus utilidades para sacarles un mayor provecho para la protección de su información y sus teléfonos.

Tarea docente 3

Título: ¿Qué no se debe hacer en un Laboratorio de Computación?

Objetivo: Identificar lo que no se puede hacer en el laboratorio de Computación.

Actividades

Como pueden ver el Laboratorio docente es un lugar en el que se localizan varias estaciones de trabajo, para que ustedes puedan hacer uso de ellas. Para mantener funcionando estas máquinas es necesario cumplir con medidas de seguridad. ¿Estas medidas creen ustedes que solo sean medidas informáticas? Pues también existen medidas físicas que se deben tener en cuenta para la protección de las máquinas y el cuidado que deben tener los usuarios de las mismas.

A continuación se relacionarán algunas medidas de protección y ustedes deben marcar con una (X) ¿cuáles son las que deben cumplirse en un laboratorio de computación?

___ Usar cascos al entrar al laboratorio.

___ Llenar el registro de uso de las computadoras.

___ Pasar el antivirus a las memorias que se insertan.

___ Tener un pararrayos en el techo

___ No comer ni tomar agua en las estaciones de trabajo.

___ No cambiar el fondo de escritorio o papel tapiz.

___ Golpear los teclados.

___ Ver material audiovisual prohibido en centros de enseñanza.

___ Tener protegido el laboratorio con rejas y candado.

¿Creen ustedes que estas son las únicas medidas que se pueden tomar para proteger un laboratorio de computación? Mencionen al menos 5 medidas que no se hayan expresado anteriormente.

Evaluación

Evaluar a los estudiantes a través de preguntas cuáles son a su parecer las medidas más importantes que se deben tomar para la protección de los laboratorios.

Conclusiones

El cuidado y protección de los laboratorios es una tarea que todos debemos concientizar, para lograr que perduren en el tiempo y cumplan sus funciones. Además que los laboratorios se rigen por las normas y políticas de la Seguridad Informática, infringirlas supone un delito informático que puede tener serias consecuencias.

Tarea docente 4

Título: Los Virus Informáticos

Objetivo: Caracterizar los virus informáticos para concientizarnos de los daños que pueden ocasionar y así prevenir una infección en las computadoras.

Actividades

Como ustedes conocen un virus informático es una de las amenazas que pueden atentar contra el buen funcionamiento de la computadora. En muchas ocasiones no se cuenta con una manera efectiva de combatirlo por desconocimiento o porque no se tiene un buen antivirus instalado en la computadora o en el celular. Surgen entonces algunas interrogantes: ¿qué es un virus informático?, ¿cuál será el verdadero alcance de un virus informático?, ¿cuánto daño pueden hacer a las computadoras?

Para responder estas interrogantes vamos a visualizar un material y de ahí van a identificar:

a) ¿Qué es un virus informático?
b) ¿Cuáles son los diferentes tipos de virus informáticos?
c) ¿Qué características presentan estos virus informáticos?
d) ¿Qué daños pueden ocasionar los virus informáticos?
e) ¿Cuáles son las vías más usuales para infectarse con un virus informático?

Investigue en los sitios web de uso en clases y en los softwares a tu disposición: ¿cuál fue el primer virus informático? Elabore un informe escrito y una

presentación en PowerPoint con todos los elementos para debatir en el aula en próximas clases.

Evaluación

Se evaluarán a los estudiantes que tengan las respuestas mejor elaboradas, más completas y acertadas.

Conclusiones

Hacer énfasis en el daño que pueden ocasionar los virus informáticos para las computadoras y las personas, en la necesidad de la protección de la información y como deben pasar el antivirus cada vez que introduzcan un dispositivo de almacenamiento en la computadora. Así como se motivará para que realicen las presentaciones para la próxima clase.

Tarea docente 5

Título: Los Antivirus Informáticos

Objetivo: Caracterizar los Antivirus Informáticos como una herramienta para la prevención y eliminación de amenazas informáticas.

Actividades

Tener un antivirus informático instalado en la computadora es una garantía de seguridad contra la propagación de amenazas que puedan causar daños considerables a la información del sistema. Para conocer más de estos softwares investigaremos sobre uno de factura nacional que a lo mejor ustedes conocen, Segurmática Antivirus. Para ello vamos a visitar su sitio web https://www.segurmatica.cu y a visualizar un material donde responderán las siguientes preguntas:

a) ¿Qué es un software antivirus?
b) ¿Para qué se utiliza un antivirus?
c) ¿Qué es Segurmática?
d) ¿Cuál o cuáles son sus productos informáticos para la eliminación de virus informáticos?

Elabore un informe escrito y una presentación en PowerPoint con todos los elementos para debatir en el aula en próximas clases.

Evaluación

Se evaluarán a los estudiantes que tengan las respuestas mejor elaboradas, más completas y acertadas.

Conclusiones

Se hará énfasis en la necesidad de tener un antivirus informático instalado en la computadora, así como la actualización periódica de sus bases para lograr una correcta seguridad en la computadora.

Tarea docente 6

Título: Sopa de palabras informáticas

Objetivo: Identificar palabras claves relacionadas con la Seguridad Informática de manera que se consolide una cultura informática.

Actividades

La siguiente tarea consiste en encontrar un grupo de palabras que están sumergidas en una sopa de palabras, estás, están relacionadas con la seguridad informática, los elementos que la componen y otros. Deben encontrarlas en el menor tiempo posible, pues se evaluará por equipos los que primero logren encontrarlas. Para ellos se conformarán 8 equipos que tendrán que encontrar las palabras, luego cada uno de los integrantes del equipo tiene que decir una definición de cualquiera de las palabras encontradas. Gana el equipo que mejor lo haga en el menor tiempo posible.

Palabras:

Seguridad Informática	Troyano	Segurmatica
Virus	Gusano	Desinfectar
Antivirus	Computadora	Internet
Malware	Kaspersky	Spam

W	E	R	T	Y	U	I	O	P	A	S	D	F	H	J	L	Z	X	C	J	K	D	G
D	S	E	G	U	R	M	A	T	I	C	A	I	V	H	V	P	O	Z	X	T	Q	A
F	P	K	T	A	D	Q	A	Z	A	Q	D	U	C	G	G	O	U	Ñ	C	Q	W	Z
G	A	I	G	Z	C	R	S	X	S	S	F	Y	X	R	H	I	F	L	V	Z	E	D
H	M	L	B	W	F	T	X	C	D	X	G	H	W	W	J	Ñ	E	K	I	S	R	F
J	Q	M	R	F	V	H	D	V	W	C	V	N	D	Q	L	L	D	J	R	C	T	L
K	A	L	F	M	T	V	F	B	E	E	C	B	B	Z	O	M	S	H	U	B	Y	P

L	S	M	V	G	A	B	G	N	T	R	A	N	T	I	V	I	R	U	S	K	U	O
O	Z	P	E	T	G	L	H	M	Y	T	W	V	V	D	L	K	X	G	C	U	I	I
G	X	L	D	H	H	D	W	Q	U	H	R	C	B	E	P	U	F	F	V	Y	O	U
U	E	M	C	B	J	E	H	A	H	U	F	X	N	F	P	Y	V	D	B	T	P	J
S	D	O	W	N	K	R	J	S	R	I	Y	C	O	M	P	U	T	A	D	O	R	A
A	C	K	D	D	L	F	K	D	Q	E	J	A	K	F	U	J	S	S	N	R	A	Y
N	R	M	C	E	Z	G	L	F	W	K	J	W	I	Y	W	C	C	P	M	E	S	K
O	F	U	W	S	X	H	P	G	E	L	K	S	P	L	S	A	G	O	L	W	D	A
P	V	J	S	I	N	T	E	R	N	E	T	D	L	P	X	Z	V	I	K	Q	F	S
L	T	N	X	N	C	J	O	H	R	P	M	R	I	O	C	A	B	U	J	J	G	P
M	G	Y	Q	F	B	K	I	J	T	O	L	F	O	Y	V	A	G	Y	H	H	H	E
N	B	H	A	E	B	L	U	K	Y	I	H	V	J	Y	B	W	D	T	G	G	J	R
H	N	B	Z	C	N	O	Y	L	U	Y	T	L	Y	Y	A	S	W	R	F	F	K	S
Ñ	Y	Y	T	T	M	I	T	O	I	B	R	R	R	R	J	N	S	E	D	D	L	K
U	H	G	G	A	T	U	E	I	O	N	E	F	D	F	K	F	O	W	S	S	Ñ	Y
I	U	B	B	R	G	Y	W	Y	P	M	W	V	S	C	L	G	P	Q	A	C	Ñ	X
S	E	G	U	R	I	D	A	D	I	N	F	O	R	M	A	T	I	C	A	D	H	F

Evaluación

- Se evaluarán los equipos independientemente del orden que termine.
- Se harán un énfasis especial en el que termine primero.
- El equipo que termine y tenga todos los conceptos y las palabras bien será el ganador.

Conclusiones

Se reforzará el trabajo en equipo, como unidad del grupo. Se trabajarán los conceptos que más dificultades tuvieron a la hora de exponerlos.

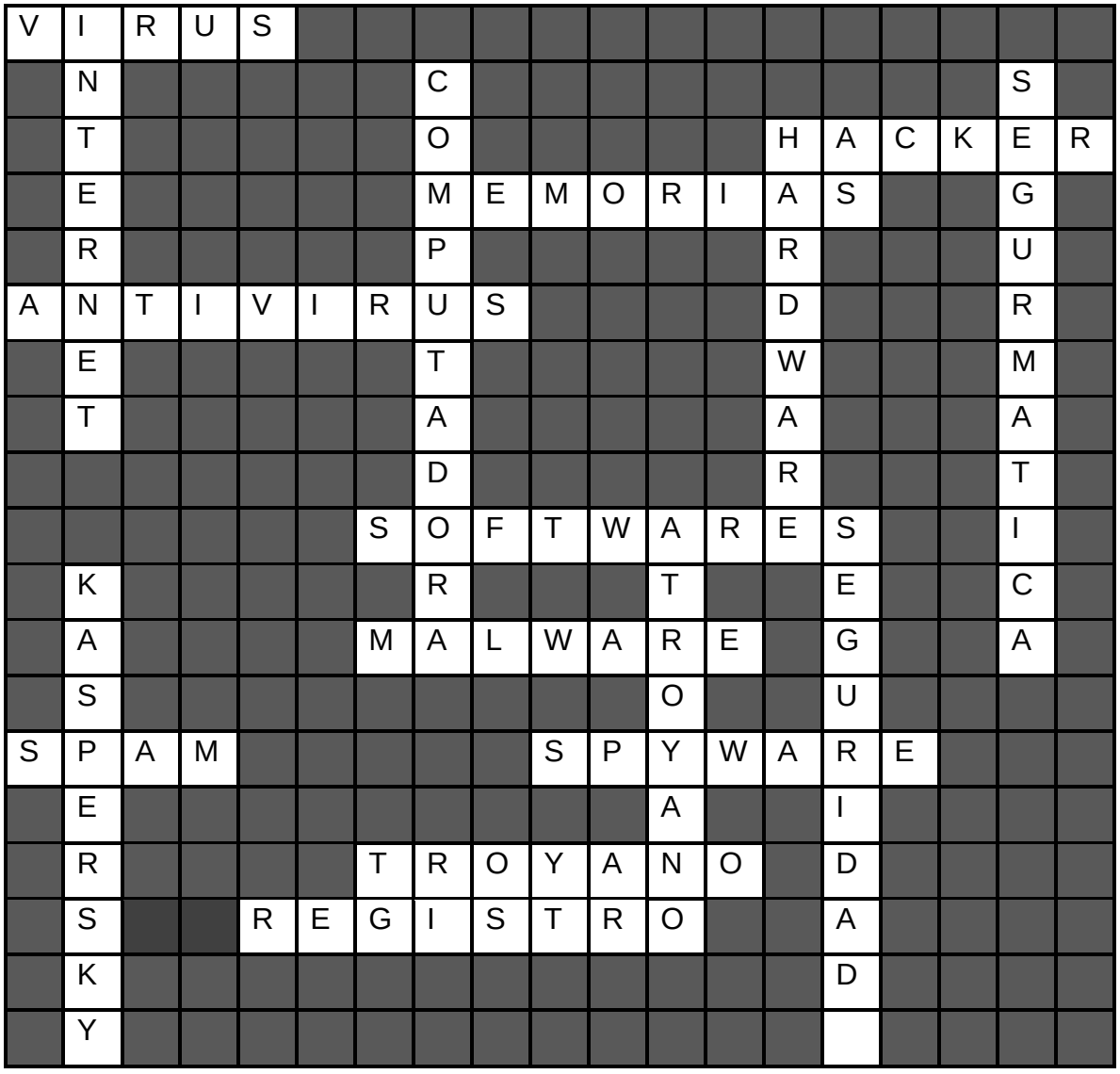
Actividad 7

Título: Crucigrama

Objetivo: Identificar los conceptos claves sobre Seguridad Informática, de manera que favorezca una cultura informática integral.

Actividades

En el siguiente Crucigrama se encuentran una serie de palabras relacionadas con la Seguridad Informática que ustedes necesitan encontrar. Ánimo y suerte.



HORIZONTAL

1. Softwares malintencionados, con el objetivo de dañar o destruir la información y los componentes de una computadora. (P)
2. Software creado con el objetivo de prevenir, detectar y eliminar la presencia de programas malignos en la computadora. (P)
3. Cadena de correos enviados con información multimedia destinada a congestionar la red y el almacenamiento de los servidores. (S)
4. Dispositivo de almacenamiento. (P)

5. Programas de computadora. (P)
6. Programas malignos. (S)
7. Programa maligno destinado al robo y espionaje de información. (S)
8. Programador mal intencionado que puede entrar en otras computadoras sin el consentimiento de los usuarios y puede causar afectaciones. (S)
9. Documento que tiene como finalidad control de usuarios que utilizan la tecnología en los laboratorios.

VERTICAL

1. Red de redes con un alcance mundial.
2. Programa para detectar softwares malintencionados de factura cubana. (S)
3. Programa para detectar softwares mal-intencionado de factura rusa. (S)
4. De estar seguro, que algo tiene … (S)
5. Equipo electrónico para el cómputo y análisis de información, compuesto por periféricos de entrada, salida, almacenamiento, etc. (S)
6. Componentes eléctricos internos y externos de la computadora, que son tangibles y se clasifican en dispositivos de entrada, salida, almacenamiento, comunicación, etc.
7. Programa maligno que usa como camuflaje otro programa. (S)

Evaluación

Se evaluará de la siguiente manera:

- 10: estudiantes que logren completar el crucigrama completo y bien.
- 7 - 9: estudiantes que les falten de 2 – 5 palabras.
- 6: estudiantes que les faltes más de 6 palabras.

Conclusiones

Se hará un cierre con los estudiantes reforzando los conceptos fundamentales sobre Seguridad Informática.

Actividad 8.

Título: Enlaza

Objetivo: Identificar los conceptos claves sobre Seguridad Informática, de manera que favorezca una cultura informática integral.

Actividad

Enlace la columna A con la B según corresponda.

A

a) Seguridad Informática.

b) Spam

c) Hardware

d) Antivirus informático

e) Troyano

f) Software

g) Virus informático

B

__ Programas diseñados intencionalmente con el objetivo de dañar o destruir la información de las computadoras.

__ Programa malintencionado que se enmascara como otro tipo de programa para luego ejecutarse en la computadora y causar daños considerables en la misma.

__ Es la parte dura o tangible de la computadora, sus periféricos.

__ Conjunto de cuadrículas consecutivas dispuestas en forma horizontal.

__ Programas diseñados con el objetivo de eliminar la presencia de programas malignos en la computadora.

__ Cadena de correos con el objetivo de ralentizar los servidores y llenarlos de información innecesaria.

__ Es la parte blanda o intangible de la computadora, lo que no se puede tocar; sus programas.

__ Proceso de prevenir y detectar el uso no autorizado de un sistema informático.

2.1 Ponga 3 ejemplos de los siguientes incisos: g) y d)

2.2 Diga dos medidas para evitar infectarse con un virus informático.

Evaluación

Se evaluará de:

10 puntos: a los estudiantes que logren tener todas las respuestas correctas.

7-9 puntos: a los estudiantes que logren tener bien el enlaza y solo un inciso bien

6 puntos: a los estudiantes que no logren completar correctamente el enlaza y al menos un inciso.

Conclusiones

Hacer énfasis en los conceptos más importantes de la Seguridad Informática como cierre de las actividades propuestas.

Las tareas docentes están dirigidas a la apropiación activa de los contenidos relacionados con la Seguridad Informática en los estudiantes de 7mo grado, además, en ellas se ofrecen las herramientas necesarias para el dominio de estos contenidos de manera creativa e independiente.

3. Evaluación de los resultados de la propuesta de solución al problema detectado.

Después de aplicadas las tareas docentes se emplearon dos instrumentos para constatación final: una observación pedagógica y una prueba pedagógica. En la observación se pudo determinar que el 95.00 % de la muestra cuando introducen dispositivos de almacenamiento en las estaciones de trabajo pasan correctamente el antivirus. El 97.50 % de los estudiantes no ingieren alimentos en el laboratorio. El 39.50 % de ellos refieren que han instalado el Antivirus Segurmática en sus computadoras y que notan una mejoría en rendimiento en comparación con los antivirus anteriores y con la misma seguridad. El 98.00 % de la muestra dominan qué es un virus y un antivirus informático, mientras que el 97.50 % aplican las medidas de seguridad que deben implementarse para evitar infectarse con un virus informático.Con los resultados de la prueba pedagógica, se pudo comprobar que el 92.50 % de los estudiantes conocen que son los virus informáticos. El 97.50% de ellos saben como implementar las medidas para la Seguridad Informática en la escuela y qué son los virus informáticos. El 95.00 % pueden identificar distintos tipos de antivirus informáticos.

Estos instrumentos pudieron constatar el avance de los estudiantes, una vez aplicadas las tareas docentes propuestas, alcanzando una mayor asimilación de los conocimientos propuestos para el nivel, y una mayor motivación en lo referente a la Seguridad Informática.

Conclusiones

1. El análisis de la literatura especializada revela las particularidades del aprendizaje para favorecer a la participa activa y protagónica de los estudiantes, dirigidos por el docente, en el aprendizaje de los contenidos concernientes a la Seguridad Informática de tal forma que pueda ser modificada su actuación, al construir conocimientos, desarrollar habilidades, capacidades y valores de forma individual y colaborativa.
2. El diagnóstico realizado en los inicios de la investigación permitió constatar que es insuficiente el conocimiento que poseen los estudiantes sobre la Seguridad Informática, por lo que su contribución al correcto desarrollo de la misma en la escuela es limitada, produciendo en varios casos violaciones por desconocimiento del contenido que ella tiene implícita.
3. Las tareas docentes propuestas son una vía didáctica esencial para desarrollar la independencia cognoscitiva de los estudiantes, se caracterizan por presentar un carácter problémico que promueva la activación, así como la utilización consciente de procedimientos dirigidos a la autorreflexión y autorregulación del aprendizaje.
4. Las tareas docentes aplicadas fueron efectivas en el logro de un aprendizaje activo de los estudiantes en los contenidos relacionados con la Seguridad Informática lo cual demostró la efectividad de la aplicación de la propuesta.

Recomendaciones

1. Continuar profundizando en el estudio de la Seguridad Informática en la asignatura de Informática Básica.
2. Generalizar los resultados de esta investigación en los grupos de séptimo grado de la ESBU “Ramón Leocadio Bonachea”.

Bibliografía

Addine, F. (2004). *Didáctica: Teoría y Práctica*. La Habana: Editorial Pueblo y Educación.

_____. Metodología de la investigación Científica. Centro de estudios de la educación superior "Manuel F. Gran". Universidad de Oriente. Santiago de Cuba. Cuba. 1996.

Álvarez, C. (1999). *La escuela en la vida.* La Habana: Editorial Pueblo y Educación.

Amoroso, Y. (2002). *El Delito Informático.* Conferencia Magistral Diplomado de Criminalística. La Habana. Cuba.

Anderson, J. P. (2005). *Amenazas de seguridad informática de seguimiento y vigilancia*. Recuperado de http://www.sciencedirect.com/science.

Aneiro, L. O. (2001). *Elementos de Arquitectura y Seguridad Informática.* La Habana: Editorial Pueblo y Educación.

Antivirus Segurmática. (2010). *Enciclopedia EcuRed* [versión electrónica]. La Habana, https://www.ecured.cu/Segurmática

Añorga, J. (2000). *Glosario de términos de Educación Avanzada.* [CD ROM] La Habana.

Araujo, R. (1992). *Lecciones de Filosofía Marxista-Leninista*. La Habana: Editorial Pueblo y Educación.

Ávila, R. (2009). *Sitio Web SegInf para perfeccionar el Sistema de Seguridad informática en las Direcciones Municipales de Educación*. (Tesis de Maestría en Ciencias de la Educación). IPLAC. Las Tunas.

Blanco, L. J. (2003). *Apuntes para una historia de la Informática en Cuba.* La Habana: Editorial Pueblo y Educación.

Blanco, A. (2001). *Filosofía de la Educación.* La Habana: Editorial Pueblo y Educación.

_____. (2005) Introducción a la Sociología de la Educación. La Habana: Editorial Pueblo y Educación.

Cuba, S. (1993). *El proceso de las computadoras*. Editora política. La Habana. Cuba.

_____. (Julio, 1998). El delito Informático, Conferencia Magistral, Congreso de Ciencias Penales. La Habana. Cuba.

Castellanos, D. y otros. (2002) *Aprender y enseñar en la escuela.* La Habana: Editorial Pueblo y Educación.

Colectivo de autores. (2002). *Metodología de la investigación Educacional*. La Habana: Editorial Pueblo y Educación.

Colectivo de autores. (2006). *Los detectives y la prevención de la criminalidad informática.* La Habana: Editora política.

Colectivo de autores. (2006). *Plataforma Política para la Red del MINED*. La Habana: Editorial Pueblo y Educación.

Cordovés, E. (2002). *La prevención en los delitos informáticos*. Ponencia. II Taller Informática. La Habana.

Cuéllar, A. (1977). *Nociones de Psicología General*. La Habana: Editorial Pueblo y Educación.

Fernández, B. (1997). *Temas de didáctica. Primera parte.* La Habana. Editorial Pueblo y Educación.

Fuerte, M. (2003). Compendio de Pedagogía. La Habana: Editorial Pueblo y Educación.

Fuerte, M.I., Labañino, C. y Galán, C. (2016). *Programa Provisional de Informática. Séptimo grado.* La Habana: Editorial Pueblo y Educación.

García, P. (2002). *Incidencia del delito Informático*. (Trabajo de diploma). ISMI. La Habana.

Garnier, J. C. (2006). *La información y su papel en la Seguridad Nacional de la Información*. La Habana.

González, V. y Castellanos, D. (2006). *Psicología para educadores*. La Habana: Editorial Pueblo y Educación.

Leblanch, I. (2008). *Sitio Web Educativo para desarrollar una cultura en Seguridad Informática en los Institutos Politécnicos de Informática de la Educación Técnica y Profesional*. (Tesis en opción al grado de Máster en Ciencias de la Educación.) IPLAC. La Habana.

Manso, M. (2010). *Legislación sobre delitos informáticos en Argentina*. Recuperado de http://www.segu-info.com.ar.

Resolución Ministerial. No. 49/1996. Ministerio de las Comunicaciones. Ciudad de La Habana. Cuba.1996.

Resolución Ministerial. No. 6/1996. Ministerio del Interior. Ciudad de La Habana. Cuba.1996.

Resolución Ministerial. Resolución Ministerial. No. 204/1996. Ministerio de la Industria Sidero Mecánica y la Electrónica. Ciudad de La Habana. Cuba.1996.

Resolución Ministerial. Decreto-Ley. No. 199/1996. La Seguridad y Protección de la Información Oficial. Consejo de Estado. Ciudad de La Habana. Cuba.1996.

Resolución Ministerial. No. 49/1996. Ministerio de las Comunicaciones. Ciudad de La Habana. Cuba.1996

Resolución Ministerial. No .22/2000. Ministerio de la Informática y las Comunicaciones. Ciudad de La Habana. Cuba. 2000.

Resolución Ministerial. No. 90/ 2000. Ministerio de la Informática y las Comunicaciones. Ciudad de La Habana. Cuba. 2000.

Resolución Ministerial. No.124/2000. Ministerio de la Informática y las Comunicaciones. Ciudad de La Habana. Cuba. 2000.

Resolución Ministerial. No. 26/ 2000. Ministerio del Interior. Ciudad de La Habana. Cuba. 2000.

Resolución Ministerial. No. 49/ 2001. Ministerio de la Informática y las Comunicaciones. Ciudad de La Habana. Cuba. 2001.

Resolución Ministerial. No. 39 /2002. Ministerio de la Informática y las Comunicaciones. Ciudad de La Habana. Cuba. 2002.

Resolución Ministerial. No. 65 /2003. Ministerio de la Informática y las Comunicaciones. Ciudad de La Habana. Cuba. 2003.

Resolución Ministerial. No. 127/2007. Reglamento de Seguridad Informática. Consejo de Estado. Ciudad de La Habana. Cuba. 2007.

Resolución Ministerial. No. 207/2007. Reglamento de Seguridad Informática. Ministerio de Educación. Ciudad de La Habana. Cuba. 2007.

Resolución Conjunta. No.1, de 28 de enero de 1999. Ministerio de Comercio Exterior y Ministerio de la Industria Sidero Mecánica y la Electrónica. Ciudad de La Habana. Cuba.1996.

Resolución Económica del V Congreso del Partido Comunista de Cuba. Ciudad de La Habana. Cuba. 1997.

Ribalta, M. A. (2004). *Las Tecnologías de la Información y las Comunicaciones (TIC) en el Sistema Nacional de Educación y en la formación de docentes en la República de Cuba*. VII Taller Internacional Planeamiento, Administración y Supervisión Educativa. IPLAC. La Habana.

Rodríguez, E. (2006). *La Seguridad Informática: Condición indispensable para la preservación de las Tecnologías de la Información en la provincia de Las Tunas*. (Tesis en opción al grado de Máster en Ciencias Jurídicas). Las Tunas.

Seguridad Informática. (2010). *Enciclopedia EcuRed* [versión electrónica]. La Habana, https://www.ecured.cu/Seguridad_Inform%C3%A1tica.

Silvestre, Margarita (2001). Aprendizaje, Educación y Desarrollo.- La Habana: Editorial Pueblo y Educación.

Talizina, N. (1988). *Psicología de la enseñanza.* Moscú. Editorial: Más Progreso.

Tellez, J. (1997). *Derecho Informático.* Segunda Edición. Editorial McGraw-Hill. México.

Urbina, G. (2016). *Introducción a la Seguridad Informática.* Recuperado de https://books.google.com.cu/books?id=IhUhDgAAQBAJ&pg=PR1&lpg=PR1&dq=Urbina+seguridad+inform%C3%A1tica&source=bl&ots=0WPD6DsiCo&sig=ACfU3U1sMpjuLJvIfri7IGa6q_N5he7-8Q&hl=es&sa=X&ved=2ahUKEwij18-

qwc3iAhWFr1kKHXALDRoQ6AEwDHoECAkQAQ#v=onepage&q=Urbina%20seguridad%20inform%C3%A1tica&f=false

Vigotsky, L. S. (1998). *Pensamiento y Lenguaje*. La Habana: Editorial Pueblo y Educación.

Villalón, A. (2002). *Seguridad en unix y redes*. Recuperado de https://www.rediris.es/cert/doc/unixsec/unixsec.pdf

Zilberstein J. y Silvestre M. (2000). *Aprendizaje y la formación de valores*, en Seminario Nacional para el personal docente. La Habana: Ministerio de Educación.

Zilberstein, J. (2004). *Hacia una didáctica desarrolladora.* La Habana: Editorial Pueblo y Educación.

Anexos

ANEXO 1

GUÍA DE OBSERVACIÓN PEDAGÓGICA

Objetivos de la observación: Determinar los conocimientos en la Seguridad Informática de los alumnos.

Cantidad de observadores: 15

Tiempo total y frecuencia de las observaciones: 1 mes.

Tipo de observación: Participante.

Lugar en que se realiza la observación: Laboratorio de Computación de la ESBU Ramón L. Bonachea.

Aspectos a observar en la unidad de investigación:

1. Empleo de las tecnologías.
   - 1.1. Frecuencia con la que asisten los estudiantes al laboratorio de computación fuera del horario de clases.
     - 1.1.1. Mucha Frecuencia __ Bastante__ Poca__ Nunca__
   - 1.2. Cuando están en el laboratorio de computación a qué dedican más tiempo:
     - 1.2.1. Tareas en Software__ Juegos__ Navegación nacional (información escuela)__ Navegación nacional (ocio)__
   - 1.3. Pasan antivirus cuando colocan un dispositivo en la PC
     - 1.3.1. Sí__ No__ A veces__
   - 1.4. Utilizan el celular para pasarse información en las clases
     - 1.4.1. Sí__ No__ A veces__
   - 1.5. ¿Qué es lo que más comparten por la red (Zapya) por el celular
     - 1.5.1. Doc.__ Música__ Imagen__ Video__
   - 1.6. Sitios web más visitados

1.6.1. Cultura__ Investigación__ Juegos__ Chat__

2. Cuidado de las tecnologías.

2.1. Ingieren alimentos en las estaciones de trabajo

2.1.1. Sí__ No__ A veces__

2.2. Usan indebidamente los periféricos de entrada y salida (golpes y aporreo de las teclas del teclado y mouse)

2.2.1. Sí__ No__ A veces__

2.3. Apagan el cliente ligero sin cerrar el SO (por el botón de Power)

2.3.1. Sí__ No__ A veces__

3. Uso del registro de acceso a las tecnologías.

3.1. Conocen el registro de acceso a las tecnologías

3.1.1. Sí__ No__

3.2. Llenan el registro de acceso a las tecnologías.

3.2.1. Siempre__ A veces__ Nunca__

3.3. Conocen para que se usa el registro de acceso a las tecnologías.

3.3.1. Sí__ No__

4. Actualización del plan de Seguridad Informático.

4.1. Conocen el Plan de Seguridad Informática de la escuela

4.1.1. Sí__ No__

4.2. Conocen cuando cometen una violación del Plan de Seguridad Informática.

ANEXO 2

ENTREVISTA A LOS ALUMNOS

Objetivo: Determinar los conocimientos que poseen los alumnos de la ESBU Ramón L. Bonachea en cuanto la Seguridad Informática.

1. ¿Qué entiendes por Seguridad Informática?
2. ¿Qué utilidad tiene la Seguridad Informática en las escuelas?
3. ¿Qué es un virus informático?
4. ¿Cuántos tipos de virus informáticos conocen?
5. ¿Qué pueden hacer para evitar infectarse con un virus informático?
6. ¿Conocen ustedes cuáles son las normas básicas de comportamiento en un laboratorio de computación?
7. ¿Cómo puedes contribuir a que exista en el centro una buena Seguridad Informática?
8. ¿Quiénes se ocupan de velar por la Seguridad Informática en la escuela?

ANEXO 3

ANÁLISIS DOCUMENTAL

Objetivo: Constatar los contenidos que se imparten sobre Seguridad Informática en las clases de Informática contrastándolo con lo orientado por el Ministerio de Educación.

Documentos analizados:

- Planes de Clases
- Programa de la asignatura
- Modelo de Secundaría Básica

Aspectos a analizar:

- Cantidad de Horas Clases destinadas al estudio de la Seguridad Informática.
- Contenidos propuestos por el Ministerio de Educación.
- Cómo se abordan los contenidos propuestos por el Ministerio de Educación en clase.
- ¿Cómo se evidencia en el Modelo de Secundaria Básica la Seguridad Informática en las escuelas?

ANEXO 4

PRUEBA PEDAGÓGICA
Prueba Pedagógica inicial

Objetivo: Determinar el nivel de conocimientos que presentan los estudiantes del 7mo grado de la ESBU: Ramón Leocadio Bonachea en temas de Seguridad Informática.

Preguntas:

Marque con una (X) la respuesta correcta en cada caso.

1. Al insertar una memoria USB o un dispositivo de almacenamiento en la PC, se debe pasar el Antivirus. SI___ No___
2. En el laboratorio ingieres alimentos frecuentemente. SI___ No___
3. Conoces y utilizas el Registro de acceso a la tecnología. Si___ No___
4. Introduces contenidos multimedia en las computadoras de la escuela que no sea material docente. Si___ No___

Evaluación de la Prueba Pedagógica

Si los estudiantes contestan 2 preguntas Bien, conocen sobre Seguridad Informática, si por el contrario contestan 3 preguntan mal, se evalúa como que desconocen sobre la Seguridad Informática.

ANEXO 5
Prueba Pedagógica final

Objetivo: Determinar el nivel de conocimientos que presentan los estudiantes del 7mo grado de la ESBU: Ramón Leocadio Bonachea en temas de Seguridad Informática.

Preguntas:

1. ¿Qué es la Seguridad Informática?
2. Marque con una (X): ¿quiénes son los responsables de la Seguridad Informática en la escuela?
    a. ____ EL director
    b. ____ Secretaria Docente
    c. ____ Jefes de grado
    d. ____ Alumnos
    e. ____ Técnicos del laboratorio
    f. ____ Profesores
3. Marque con una (X) las medidas para implementar la Seguridad Informática en las escuelas.
    a. ____ Llevar cascos en los laboratorios.
    b. ____ Laboratorios de computación protegidos con rejas y tener un pararrayos en la escuela.
    c. ____ Pasar el antivirus a los dispositivos de almacenamiento que se coloquen en las computadoras.
    d. ____ Merendar dentro del laboratorio.
    e. ____ Llenar el registro de acceso a la tecnología.
    f. ____ Navegar por sitios web no seguros de audio y video.
    g. ____ Conocer las medidas más importantes de prevención del Plan de Seguridad Informática.
4. ¿Qué es un virus informático?
5. ¿Cuántos tipos de Antivirus conoces?

6. Diga 7 acciones que usted tomaría para evitar infectarse con un virus informático.

Evaluación de la Prueba Pedagógica Final

Preguntas:

1. Por responder:
    a. Todos los elementos: B
    b. Dar 3 – 4 elementos: R
    c. Dar 1 – 2 elementos: M
2. Por marcar:
    a. De 5 – 6: B
    b. De 3 – 4: R
    c. De 1 – 2: M
3. Por marcar:
    a. Por marcar 4: B
    b. De 2 – 3: R
    c. Por 1: M
4. Por responder:
    a. Todos los elementos: B
    b. Dar 3 – 4 elementos: R
    c. Dar 1 – 2 elementos: M
5. Por decir:
    a. De 5 a más: B
    b. De 3 – 4: R
    c. De 1 – 2: M
6. Por decir
    a. De 6 – 7: B
    b. De 3 – 5: R
    c. De 1 – 2: M

ANEXO 6

Gráfico de la Prueba Pedagógica Inicial

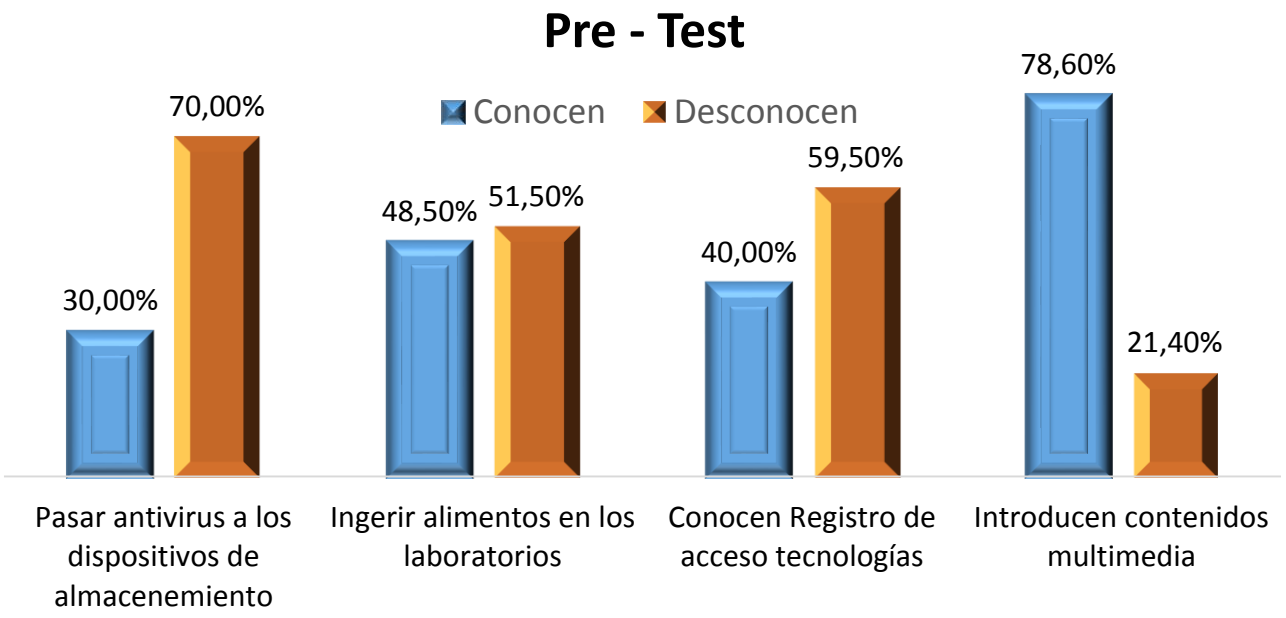


Gráfico de la Prueba Pedagógica Final