

Universidad de Matanzas
Facultad de Ciencias Pedagógicas
“Juan Marinello Vidaurreta”



Sistema de Actividades metodológicas que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana “28 de Octubre” del municipio Pedro Betancourt.

AUTORA: Jany Rivero Tarifa

TUTOR: MSc. Hanoi Peña Colina.

Cotutora: MSc. Idania Tarifa Campos

Curso 2014 - 2015

PENSAMIENTO

“El mundo camina hacia la era electrónica.... Todo implica que esta ciencia se convertirá en algo así como una medida del desarrollo; quien la domine será un país de vanguardia. Vamos a volcar nuestros esfuerzos en este sentido con audacia revolucionaria.”



AGRADECIMIENTOS

Quiero agradecer de una manera sencilla y modesta a todas las personas que con dedicación y sacrificio permitieron hacer realidad mis sueños de ser una profesional más preparada en aras de cumplir las metas de nuestra Revolución victoriosa, en especial a: Hanoi Peña Colina mi tutor.

DEDICATORIA

Estudiar requiere de mucho sacrificio, por ello, quiero dedicar esta investigación a:

La Revolución, por darme la posibilidad y la oportunidad de superarme.

A mis padres y hermana porque siempre han confiado en mí.

A mi esposo por la comprensión y su ayuda incondicional para lograr este objetivo.

RESUMEN

Los recursos informáticos, como apoyo a la educación es una realidad palpable. Repensar en su utilidad, así como replantearse el rol del profesor y de los estudiantes conlleva a perfeccionar las acciones pedagógicas en el proceso de enseñanza-aprendizaje, lo cual resulta cada vez más necesario por lo que se determina el problema científico ¿Cómo contribuir al desarrollo de una cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt? Se determinó el objetivo principal: Elaborar un sistema de actividades metodológicas que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt. Se rectorea por el método dialéctico materialista y la aplicación de métodos científicos de investigación, de nivel teórico y empíricos Esto permitió la obtención del resultado mencionado y la validación del mismo.

ÍNDICE



Tabla de contenidos	Pág.
INTRODUCCIÓN	1
CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA DE LA SEGURIDAD INFORMÁTICA.	6
1.1 Aspectos fundamentales de la Seguridad Informática. Documentos normativos y conceptos básicos sobre Seguridad Informática	6
1.2 . Elementos fundamentales para el logro de una cultura Informática en los profesores.	7
. 1.3 La Seguridad Informática, elemento de la cultura Informática.	13
1.4 Sistema de actividades	17
CAPÍTULO II. FUNDAMENTACIÓN PRÁCTICA SOBRE EL SISTEMA DE ACTIVIDADES METODOLÓGICAS QUE CONTRIBUYA A LA CULTURA EN SEGURIDAD INFORMÁTICA	21
2.1 Resultados del análisis del diagnóstico inicial aplicado para comprobar la necesidad de dar solución al problema	21
2.2 Consideraciones para la elaboración del sistema de actividades metodológicas.	23
2.3 Sistema de actividades metodológicas sobre la Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.	26
2.4 Valoración del sistema de actividades por compañeros que se desempeñan como responsables de Seguridad Informática en áreas de la UMCC Sede "Juan Marinello Vidaurreta"	42
CONCLUSIONES	44
RECOMENDACIONES	45
BIBLIOGRAFÍA	46
ANEXOS	48

INTRODUCCIÓN

Los finales del siglo XX y los inicios del siglo XXI se han caracterizado a escala mundial por un desarrollo acelerado de las tecnologías de la información y las comunicaciones, donde se ponen de manifiesto, la electrónica, la informática y las telecomunicaciones, que constituye el núcleo central de la transformación multidimensional que experimenta la economía y la sociedad, imponiéndole al ser humano modificar no solo sus hábitos y patrones de conducta, sino incluso su forma de pensar.

En tal sentido el Comandante en Jefe Fidel Castro expresó en el año 1999: *“El mundo camina hacia la era electrónica.... Todo implica que esta ciencia se convertirá en algo así como una medida del desarrollo; quien la domine será un país de vanguardia. Vamos a volcar nuestros esfuerzos en este sentido con audacia revolucionaria.”*¹

El impacto social que viene produciendo el desarrollo computacional ha alcanzado, por supuesto, la esfera educativa. El sistema de enseñanza en Cuba ha evolucionado y realizado transformaciones a lo largo de los años siempre con el objetivo principal de perfeccionar el sistema educacional. Se trata, entonces, que los estudiantes aprendan que la educación se prolonga más allá del sistema educativo obligatorio, se hace necesario el aprendizaje permanente.

En Cuba los recursos informáticos, como apoyo a la educación, han pasado vertiginosamente de la utopía a una realidad palpable. Repensar en su utilidad educativa, así como replantearse el rol del profesor y de los estudiantes conlleva a perfeccionar las acciones pedagógicas en el proceso de enseñanza-aprendizaje, lo cual resulta cada vez más necesario.

José Martí, el Héroe Nacional cubano expresó: *“Educar es depositar en cada hombre toda la obra humana que le ha antecedido: es hacer a cada hombre resumen del mundo viviente, hasta el día en que vive: es ponerlo a nivel de su*

¹Hanoi Peña Colina. La educación de una cultura informática en los usuarios de la red del Instituto Superior Pedagógico “Juan Marinello” en materia de Seguridad Informática”. Tesis en opción al título académico de Máster en Ciencias de la Educación .2009, pág.27.

*tiempo, para que flote sobre él y no dejarlo debajo de su tiempo, con lo que no podrá salir a flote; es preparar al hombre para la vida*², por lo que es tarea de los profesores preparar a los futuros profesionales y pueblo en general para insertarse en el mundo contemporáneo altamente preparados y capacitados y poseedores de una cultura integral que refuerce y pondere la identidad nacional.

El uso de las Tecnologías Informáticas, ha significado un adelanto incuestionable, pero también su uso inadecuado ha introducido nuevas manifestaciones inapropiadas para la sociedad, su introducción en el sistema educativo cubano, en su etapa actual y su desarrollo continuo, debe avanzar con los fines sociales trazadas en los lineamientos para la Informatización de la Sociedad Cubana, con las estrategias y metas planteadas en eventos nacionales e internacionales, donde se destaca la misión que desempeña la educación en estos propósitos.

El dominio de conocimientos y habilidades así como el establecimiento de una ética en el empleo de las Tecnologías de la Información y las Comunicaciones, se considera parte de la cultura informática necesaria en el mundo contemporáneo y parte también de la cultura general integral a que se aspira consolidar en el país.

Por tanto se declara como **objetivo** de esta investigación: Elaborar un sistema de actividades metodológicas que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.

En visitas de ayuda metodológica e inspección realizadas en la ESBU “28 de Octubre”, se han detectado carencias en los distintos usuarios en cuanto al conocimiento a la hora de trabajar con las tecnologías informáticas y de cómo actuar ante cualquier indicio que atente contra la confidencialidad, la integridad y la disponibilidad de la información, también se pudo constatar el grado de interés que tienen los maestros para trabajar con las tecnologías informáticas, así como el cuidado que desde el punto de vista físico ofrecen a estos medios.

²José Martí Pérez. Obras Completas. – La Habana: Edit. Nacional de Cuba, 1963. – T. VIII. P. 281.

Por las razones antes mencionadas la autora asume como **problema científico** de la investigación: ¿Cómo contribuir al desarrollo de una cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt?

El **objeto de investigación** es: La cultura Informática.

El **campo de acción**: La cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.

Para la realización de la investigación y la posible solución al problema detectado fue necesario responder las siguientes **preguntas científicas**:

1-¿Cuáles son los fundamentos teóricos metodológicos más actuales que sustentan la educación de la cultura informática?

2-¿Cuál es el estado actual de la cultura en Seguridad Informática en los profesores de la ESBU “28 de Octubre” del municipio Pedro Betancourt?

3-¿Cómo elaborar un sistema de actividades, con todos sus elementos constitutivos que contribuya a la educación de una cultura en Seguridad Informática en los profesores de la ESBU “28 de Octubre” del municipio Pedro Betancourt?

4-¿Cuáles son los resultados obtenidos a partir de la valoración crítica de un grupo de especialistas sobre el sistema de actividades metodológicas que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana “28 de Octubre” del municipio Pedro Betancourt?

Para el logro del objetivo propuesto se realizaron las siguientes **tareas de investigación**:

1- Sistematización de los fundamentos teóricos metodológicos más actuales que sustentan la educación de la cultura informática.

2- Caracterización del estado actual de la cultura en Seguridad Informática en los profesores de la ESBU “28 de Octubre” del municipio Pedro Betancourt.

3- Elaboración de un sistema de actividades, con todos sus elementos constitutivos que contribuya a la educación de una cultura en Seguridad Informática en los profesores de la ESBU “28 de Octubre” del municipio Pedro Betancourt.

4- Constatación de los resultados obtenidos a partir la valoración crítica de un grupo de especialistas sobre el sistema de actividades metodológicas que

contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana “28 de Octubre” del municipio Pedro Betancourt.

En la investigación se asume como método general de la ciencia el dialéctico materialista, el cual permite revelar las relaciones causales y funcionales del objeto de estudio. De igual forma se emplean métodos específicos de la investigación educativa que responden al nivel teórico y empírico del conocimiento. Los mismos permitieron la fundamentación teórica del objeto de investigación y la elaboración de un resultado para su tratamiento.

De los **métodos del nivel teórico** se utilizaron:

El histórico-lógico: Este facilitó el estudio de la evolución histórica del objeto de investigación así como la relación lógica y los nexos causales entre todas las partes que condicionan la investigación.

El analítico-sintético: que permitió el estudio de los diferentes componentes que influyen en la apropiación de la cultura en Seguridad Informática en los profesores de las secundarias y así como la interacción dialéctica que se establece entre ellos y el condicionamiento mutuo que ejercen en la apropiación de la cultura en Seguridad Informática.

El inductivo-deductivo: Se utilizó para estrechar relaciones con otros métodos, el análisis y el procesamiento de su información, determinando los fundamentos teóricos de la investigación, a partir de las posiciones que expresan diferentes autores e inducir las principales regularidades que aportan los instrumentos aplicados para determinar el sistema de actividades que influye en el logro de una cultura en Seguridad Informática.

Modelación: Se utilizó en el diseño del sistema de actividades metodológico con todos sus elementos constitutivos que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.

El enfoque de sistema: posibilitó el estudio concatenado del objeto de investigación así como permitió establecer las relaciones de subordinación y coordinación entre los objetivos, contenidos, métodos, medios de enseñanza, formas de organización y evaluación en la elaboración del sistema de actividades metodológicas.

Métodos matemáticos (Análisis porcentual) para el análisis y tabulación de los resultados que se derivan de los métodos empíricos aplicados.

Los métodos del nivel empírico empleados fueron:

La **entrevista** permitió la profundización en algunos elementos necesarios dentro de la información acerca de la cultura en Seguridad Informática que deben poseer los profesores según el criterio del director y dos jefes de grados.

La observación: para valorar el dominio que poseen los profesores acerca de la Seguridad Informática.

La **encuesta** se utilizó para recoger información de los diferentes profesores, al atender a su diversidad en lo relacionado con sus opiniones sobre la cultura en Seguridad Informática.

Los métodos aplicados dan respuesta a la necesidad de establecer la adecuada relación entre problema, objeto, campo de acción y tareas investigativas para cumplir el objetivo trazado. El mismo constituye el fundamento teórico integrador y la metodología general de todo el desempeño científico acometido por la autora.

La población está formada por los 49 profesores que conforman la ESBU “28 de Octubre” del municipio de Pedro Betancourt, un director, y tres jefes de grado y la muestra que se selecciona de manera intencional por los intereses de la propia investigación, es de un director para un 100% de la población, dos jefes de grados para un 66,6% y 15 profesores para un 30,6%.

La significación práctica está dada en la concreción, o sea, elaboración y aplicación de un sistema de actividades, que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana “28 de Octubre” del municipio Pedro Betancourt.

Estructura Capítular

El trabajo está estructurado en dos capítulos. En el Capítulo I se aborda la importancia de la fundamentación teórica metodológica sobre el desarrollo de la capacitación sobre Seguridad Informática en los profesores de la escuela secundaria básica urbana “28 de Octubre” del municipio Pedro Betancourt. En el Capítulo II su contenido está dada en la elaboración y aplicación, del resultado investigativo: un sistema de actividades que aporta los recursos necesarios y los elementos que sustenta y faciliten la adquisición de una capacitación sobre Seguridad Informática en los profesores de la escuela secundaria básica urbana “28 de Octubre” del municipio Pedro Betancourt.

CAPITULO I: FUNDAMENTACIÓN TEÓRICA DE LA SEGURIDAD INFORMÁTICA.

1.1 Aspectos fundamentales de la Seguridad Informática. Documentos normativos y conceptos básicos sobre Seguridad Informática.

La Seguridad Informática es reconocida legalmente como:... medio de prevención de delitos en los sistemas informáticos. Las normas que fijan las medidas de Seguridad Informática rigen para diversos ámbitos de aplicación:

- Administrativo y de organización,
- Personal,
- Entorno Físico,
- Sistemas Electrónicos,
- Equipos y programas de computación,
- Educativas...

Los esfuerzos se encuentran dispersos entre varios ministerios: MININT, MTSS, MIC, Consejo de Estado. Solamente el actuar organizado de estas instituciones y una norma uniforme y extensa sobre Seguridad Informática sentarán las bases para un marco legal satisfactorio.

El acelerado desarrollo de la ciencia y la tecnología ha conllevado a un nuevo y extraordinario aumento de las capacidades para procesar, almacenar y transmitir información, la conexión a distintas redes expone a cada usuario de las mismas al contacto con un universo variado. Ese universo contiene, información, programas valiosos, virus informáticos y otros elementos no deseados que pueden afectar al hombre y a la tecnología. En tal sentido, el hombre contemporáneo necesita de una cultura informática con todos sus componentes y dentro de ellos muy especialmente la consolidación de una ética en su carácter de usuario.

El concepto de Seguridad Informática no es nuevo, nació con los grandes centros de cómputo, donde los datos informatizados eran relativamente fáciles de defender y proteger, ya que estos no salían de allí y su seguridad se conseguía con cierta facilidad. Con el pasar de los años, las computadoras pasaron de ser grandes monstruos, que ocupaban salas enteras a pequeños elementos de trabajo perfectamente ubicables dentro de una oficina,

multiplicándose el número de usuarios. En este proceso de digitalización y miniaturización la característica más importante que se perdió fue la seguridad, al hacerse la información más vulnerable.

Esta constituye una razón para hacer que se imponga la preparación de todo el personal que opere con estas tecnologías en aras de elevar su cultura en materia de Seguridad Informática.

Entre los documentos normativos que rigen la Seguridad Informática tenemos:

- ✓ Acuerdo 6058 del Comité Ejecutivo del Consejo de Ministro (CECM): Se emite el 9 de julio de 2007. Aquí se aprueban los Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información en el país. Los organismos de la Administración Central del Estado adoptarán las medidas necesarias para el fortalecimiento de la seguridad de las tecnologías de la información
- ✓ Decreto ley 199/99: Es emitido el 25 de noviembre de 1999, el presente Decreto-Ley tiene como objetivo, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, cuyas normas deben cumplimentar tanto los órganos organismos, entidades o cualquier otra persona natural o jurídica residente en el territorio nacional, como las representaciones cubanas en el exterior.
- ✓ Resolución 127/2007 del MIC: Reglamento de Seguridad para las Tecnologías de la Informática en todas las entidades del país.
- ✓ Resolución 188/2006 MTSS: Es emitida por el Ministerio del Trabajo y Seguridad Social. Aquí se aborda todo lo referente a los reglamentos disciplinarios internos.
- ✓ Resolución 176/2007 MINED: Se emite el 1 de diciembre del 2007 y plantea aprobar y poner en vigor el Reglamento de Seguridad Informática en la Actividad Educacional del Ministerio de Educación.

1.2 Elementos fundamentales para el logro de una cultura Informática en los profesores.

El desarrollo científico tecnológico alcanzado por la humanidad desde mediados del siglo XX y el transcurso del siglo XXI en cuanto a la informática y las comunicaciones es tan vertiginoso que cada día la interrelación entre ambas es mayor, cuestión que se manifiesta con la aparición y crecimiento

inusitado de Internet, hecho que ha traído como consecuencia infinidad de implicaciones en la vida práctica.

Con ella ha cambiado la forma en que se genera, disemina y consume la información, y consecuentemente se han producido verdaderas revoluciones a nivel internacional en todos los ámbitos, de ahí la necesidad a nivel mundial, regional y nacional de poseer una cultura informática, ello a consideración de la autora de la investigación es un imperativo y una necesidad social en estos momentos y la misma debe comenzar a fomentarse desde edades tempranas en las escuelas, por lo que la educación juega un papel decisivo en la misma. La sociedad a nivel mundial y nacional debe desarrollar individuos capaces, competitivos, altamente calificados y preparados cada vez más con vistas a que asuman los desafíos que les impone el desarrollo científico tecnológico de la época en que viven. "... la cultura no es algo accesorio a la vida del hombre, está comprometida con el destino humano y ejerce un papel funcional en la historia. Situada en el sistema nervioso central de las civilizaciones, en ella hacen síntesis los elementos necesarios para la acción y el funcionamiento de la sociedad como organismo vivo".³

Se define por informática, según el Diccionario Enciclopédico Grijalbo a "el conjunto de técnicas que permiten procesar unos datos dando unos resultados, proceso que debe realizarse mediante ordenadores".⁴

El término informática surgió en Francia en el año 1962 bajo la denominación informática, que significa "información automática".⁵ La autora considera esta definición como la más aceptada ya que la informática es la ciencia que tiene como objeto de estudio el procesamiento automatizado de la información, al utilizar las computadoras con este propósito.

A partir del análisis por separado de los diferentes conceptos que integran la definición de cultura informática como un todo, la autora valora el criterio de

³Armando Hart. Identidad vs globalización. Hacia una ética humanista en la postmodernidad. – En: Revolución y cultura, Nro. 1, Ciudad de La Habana, 1977, pág. 5. Véase también de este autor: ¿Qué es la cultura? P. 3- 6. – En: Honda. Revista de la Sociedad Cultural José Martí. Nro. 11 del 2004. Ciudad de La Habana.

⁴ Diccionario Enciclopédico Grijalbo Grijalbo T 3 p 1017

⁵ MINED. Tabloide Fundamentos de la investigación educativa, Módulo I ,Segunda parte, p 21

diferentes autores y publicaciones⁶, con vistas a la toma de posiciones sobre el tema en cuestión.

En el libro de "Informática Educativa" se señala que el concepto de Cultura Informática más que ser un concepto definido, es un concepto en construcción: la Cultura Informática incluye conocimientos y destrezas básicas que debe poseer todo ciudadano para desempeñarse en una sociedad informatizada, fuertemente dominada por las computadoras, y se define como "... tratar de entender qué son los computadores, qué hacen, que son capaces de hacer, sus implicaciones y aplicaciones en el mundo que los rodea. Para ello se requiere desarrollar destrezas necesarias para comunicarse con los computadores y reconocer las capacidades y limitaciones de ellos".⁷

En este concepto solo se hace referencia a los elementos cognitivos y a las destrezas necesarias, pero no se incluyen los aspectos éticos que forman parte de esa concepción de la cultura según se expuso en el concepto general de la misma que sirve de plataforma teórica plantea que, "... la cultura informática es poseer habilidades básicas en la utilización de la informática como apoyo a la actividad del individuo, lo cual es de utilidad en cualquier área de aplicación, al utilizar como apoyo la búsqueda, procesamiento y presentación eficiente de la información, mediante las herramientas técnicas y servicios que la informática y los servicios de información ofrecen, y el conocimiento del estado actual de desarrollo de la computación (hardware y software) y sus posibilidades de aplicación en las áreas de interés correspondientes."⁸

La autora de la investigación asume la definición anterior en este caso de Edelia García González⁹-, al considerarla la que más se ajusta a los fines de la investigación, ya que la **cultura informática** no solo es poseer esas habilidades básicas en la utilización de la informática, sino que para el

⁶Armando Hart. Identidad vs globalización. Hacia una ética humanista en la postmodernidad. – En: Revolución y cultura, Nro. 1, Ciudad de La Habana, 1977: ¿Qué es la cultura? P. 3- 6. – En: Honda. Revista de la Sociedad Cultural José Martí. Nro. 11 del 2004. Ciudad de La Habana. Diccionario de Filosofía en CD Room. Barcelona: Edit. Herder, 1996. Diccionario Enciclopédico Grijalbo Grijalbo. Tabloide Fundamentos de la investigación educativa. Informática Educativa. Edelia González García.

⁷José Sánchez. Informática Educativa...Artículo "CULTURA INFORMÁTICA"<http://revista.inie.ucr.ac.cr/articulos/1-2004/archivos/informatica.pdf>.

⁸<http://www.monografías.com/trabajos7/tain/tains.html>

⁹Doctora en Ciencias Técnicas profesora del Centro Nacional de Superación y Adiestramiento en Informática (CENSAI).

procesamiento y presentación eficiente de la información debe regirse por normas establecidas legalmente las cuales regulan el trabajo con los distintos tipos de información y medios informáticos, por lo que deben contemplarse también dentro de la concepción los elementos éticos de valor regulativo en la actuación de los individuos y en el empleo que hacen de la tecnología. Como precisión conceptual sobre la cultura informática se apunta, que esta la compone:

- Los conocimientos sobre las tecnologías que comprende el equipamiento en todas sus variedades al uso, las instalaciones y los paquetes de programas que se empleen, dicho de otro modo la parte “dura” y la parte “blanda”.
- Las habilidades básicas que se requiere para un empleo adecuado y provechoso de la tecnología y de las potencialidades que contienen los paquetes de programas instalados o a los que se tengan acceso.
- El comportamiento ético y autorregulado del usuario en relación con el empleo correcto de la tecnología en cualquiera de las formas en que se encuentre, así como los paquetes de programas y la información de la que se dispone con carácter legal y con una proyección o finalidad social.

No se puede pensar en un modelo de planificación de las comunicaciones, que solo se sustente en grandes ganancias financieras de los servicios de información y de comunicación, o que solo piense en las ventajas industriales de los productos informáticos, porque ese modelo estaría alejado de la realidad estructural de los países latinoamericanos y de sus papeles en las relaciones internacionales. Mientras que a los países productores de las Tecnologías de la Información y las Comunicaciones, les resulta vital para su modelo económico-social competir con sus productos telemáticos en el mercado internacional porque de eso depende su posición como potencias y su nivel de progreso, a los países en desarrollo solo les está asignado en ese modelo ser receptores pasivos de los productos tecnológicos y de los programas y contenidos producidos por los primeros.

Sin embargo esta realidad que se impone por parte de las potencias del primer mundo basadas en un hegemonismo informático, necesita ser cambiada y en ese sentido se hace necesario el fomento de la Cultura Informática la cual descansa en el papel que desempeñan los educadores, quienes a nivel

mundial, regional y de cada país deben transformar las realidades educativas de cada (lugar) país.

En tal sentido Cuba desarrolla el Programa para el Fomento de la Cultura Informática (IS-E) el cual tiene como premisa esencial que el acceso a la educación desde el preescolar a la universidad es un derecho de todo ciudadano, garantizado por el estado, la Informatización de la Sociedad implica la cultura Informática de todos sus miembros y esa cultura sólo tiene sentido en la Infosociedad.¹⁰

El Sistema de la Cultura Informática en la sociedad cubana tiene como centro a la persona, sea esta un escolar, un trabajador industrial o agrícola, un funcionario, un ejecutivo, un especialista, un profesional, e inclusive un ama de casa o un jubilado y por ello forman parte de los mismos todas las instituciones pertenecientes al proceso regular de educación (preescolar, primaria, secundaria, preuniversitario, universitario, postgrado, entre otras), de capacitación ramal y territorial (centros de adiestramiento y superación de los ministerios, gobiernos territoriales, casas de cultura y Joven Club de Computación) y los medios de difusión masiva.¹¹

De ahí que se considere que el desarrollo de la Cultura Informática es un objetivo priorizado de la educación cubana con los recursos financieros disponibles que ha dispuesto para ello el estado cubano con vistas a adquirir tecnología de punta, lo realmente complejo y, sin embargo, decisivo es el uso eficiente y óptimo de las Tecnologías de la Información y las Comunicaciones adquiridas, ya que existe el síndrome conocido como USTED (Uso Subdesarrollado de Tecnologías Desarrolladas), que hace poco rentables las inversiones en estos tipos de tecnologías, al no estar preparados para utilizarlas a plena capacidad los países que las adquieren¹². Es por ello que el

¹⁰ Término comúnmente utilizado para referirse a la informatización de la sociedad.

¹¹ René Herrera Santana; "La informatización de la sociedad: un reto para la educación cubana. P4

¹² Los objetivos de la Cultura Informática en Cuba son:

- Lograr que todos los cuadros, profesionales, técnicos, trabajadores, alumnos en general y ciudadanos comunes que lo requieran, sean capaces de utilizar personalmente las computadoras y otros sistemas informáticos disponibles en el país.
- Lograr que todas las personas en dependencia de su función social puedan acceder a la información necesaria y suficiente para contribuir a una informatización de la sociedad ordenada, armónica y eficaz.
- Contribuir a la preparación permanente de los cuadros, especialistas y técnicos.
- Contribuir a la actualización permanente de los maestros, profesores y todo aquel que juegue un papel directo en la enseñanza para el logro de una cultura informática.

papel trascendental que adquiere la educación en la estrategia para llevar a toda la población el disfrute de la infosociedad.

En Cuba, el punto base para la relación entre infosociedad-educación-desarrollo, tiene que ver con el acceso universal a la educación, con el objeto de generar una población poseedora de competencias básicas y herramientas para desenvolverse en la sociedad informacional y tecnológica. En esta sociedad de la información y de la gestión de las tecnologías relacionadas con la información y el conocimiento, se exigen conocimientos y destrezas, que habiliten para el tratamiento de información, para el aprender a aprender, para el aprendizaje selectivo y rápido y para el manejo con soltura y asertividad en las lógicas de redes.

Las telecomunicaciones y las tecnologías de la información y las comunicaciones, han sido importantes motores del cambio cultural, social y económico en las últimas décadas. El impacto de estos medios, y las exigencias de la sociedad actual se hacen notar de manera creciente en el mundo educativo, a pesar de que los mayores cambios no son una consecuencia directa de la tecnología sino de las evoluciones que la tecnología ha provocado en el sistema social.

Una política estratégica en lo que a las Tecnologías de la Información y las Comunicaciones se refiere tiene necesariamente que conceder un peso fundamental al sector educacional, que es uno de los centros vitales de desarrollo social en el presente siglo. Para que cualquier país pueda sacar provecho de esa situación requerirá, a la larga, tomar decisiones de regulación, planificación y seguridad del desarrollo tecnológico en este campo, lo cual significará considerar lo anterior.

La escuela, y el sistema educativo no solamente tienen que enseñar las tecnologías de la información y las comunicaciones, no sólo tienen que enseñar materias a través de éstas, sino que estas tecnologías, aparte de producir cambios en la escuela, producen un cambio en el entorno y, como la escuela lo que pretende es preparar a la gente para este entorno, si éste cambió, la actividad de la escuela tiene que cambiar. Hay que cambiar los contenidos y las metodologías docentes.

El empleo de las tecnologías de la información proporciona incontables beneficios los cuales son palpables en la sociedad y en la educación no obstante como parte de esa cultura informática que es necesario que posea todo usuario de la red tanto a nivel mundial como regional y nacional es importante conocer, analizar y dominar cuales son los diferentes riesgos potenciales con el objetivo de minimizarlos mediante el establecimiento de las políticas, medidas y procedimientos que garanticen un nivel aceptable de seguridad.

1.3 La Seguridad Informática, elemento de la cultura Informática.

La seguridad es la palabra habitual en las revistas técnicas de informática y comunicaciones y cada vez se escucha más en las reuniones de profesionales de las Tecnologías de la Información y las Comunicaciones. Es difícil convencer a los directivos o gestores de la importancia que tiene la misma, ya que muchos la consideran tediosa y poco interesante; se considera por parte de la autora que aún la sociedad no está totalmente sensibilizada; en muchos casos depende de estos y su nivel de compromiso con el centro escolar que realmente cumpla con la seguridad de los datos, todavía no es suficiente.

El término seguridad proviene de la palabra **securitas** del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. Tomado de [es.wikipedia.org/wiki/Seguridad_\(concepto\)](http://es.wikipedia.org/wiki/Seguridad_(concepto))

Seguridad: Según el Diccionario Cervantes de la Lengua Española significa, confianza, tranquilidad, calidad de seguro, dispositivo que impide que las armas se disparen solas: mecanismo de seguridad, conjunto de leyes y organismos que la aplican, que protegen contra determinados riesgos tales como, enfermedad, paro, vejez, accidente de trabajo.

Por lo que se define como Seguridad Informática a la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos. Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí

contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La Seguridad Informática en su evolución desde los años 50, ha venido mostrando patrones característicos e inquietudes particulares, generalmente atadas con la evolución de la inseguridad de la información. Si bien, cada vez que evolucionan las plataformas tecnológicas, la inseguridad se transforma, es importante observar que los profesionales de seguridad no lo hacen de la misma manera, pues, deben recorrer nuevamente la curva de aprendizaje que les exige el nuevo contexto computacional o de tecnológico que se enfrenta.

Uno de los pioneros en el tema de la Seguridad Informática fue James P. Anderson¹³, quien en el año 1980 solicitado por el gobierno de Estados Unidos, produjo uno de los primeros escritos relacionados con el tema, y 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.

Hoy en día se realizan investigaciones sobre el impacto de la Seguridad Informática ante el avance tecnológico, como parte de la necesaria ciencia informática en materia de Seguridad Informática.

La Seguridad Informática es un aspecto que se integra dentro de la sabiduría de este mismo carácter, hoy en día para el logro y dominio de una ciencia en materia de Seguridad Informática se necesita establecer el vínculo entre ciencia informática y la Seguridad Informática, en tal sentido se entiende que la Seguridad Informática es un componente de la cultura informática, ya que en la medida que los usuarios de la red tengan conocimientos sobre las tecnologías, la cual incluye desde su equipamiento en todas sus variedades de uso, las instalaciones y los paquetes de programas que se empleen se accederá a la cultura informática y los usuarios de la red estarán en mejores condiciones para ejercer sus deberes y derechos en materia de Seguridad Informática.

La Seguridad Informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, se tiene en

cuenta los componentes lógicos y físicos, sin embargo no tiene en cuenta la prevención, detección y enfrentamiento ante aquellas acciones que pueden poner en riesgo, la información, los programas y el control de los accesos.

La autora asume la definición dada por el MIC: “El conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información, que incluye la misma los medios informáticos ¹⁴ (computadoras con todos sus periféricos su cuidado y conservación.)

Todas estas definiciones tienen objetivos básicos de un sistema de Seguridad Informática que están dirigidos a lograr:

❖ **Confidencialidad:** Es el servicio de seguridad, o condición, que asegura que la tramitación no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. La confidencialidad se refiere a la capacidad del sistema para evitar que usuarios no autorizados puedan acceder a la información almacenada en él y, a su vez, asegurar que los usuarios autorizados puedan acceder a la información necesaria para el cumplimiento de sus deberes funcionales y misiones con la debida compartimentación.

❖ **Integridad:** En este segundo aspecto de la seguridad: precisión, integridad y autenticidad. El concepto de integridad significa que el sistema informático no debe modificar o corromper la información que almacene o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información, por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se hayan producido ninguna modificación, adicción o borrado. De hecho, el problema de la integridad no solo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados.

❖ **Disponibilidad:** “(...) Se entiende por el grado en que un dato está en el lugar, momento y forma en que el usuario autorizado lo requiera, a la situación que se produce cuando se puede acceder a un sistema informático en un

¹⁴MIC.Folleto”Aspectos Básicos de la Seguridad Informática” .pág. 4

período de tiempo considerado aceptable. Un sistema informático seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto el hardware como el software, se mantiene funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.”(...) ¹⁵

A partir del análisis de las diferentes definiciones de Seguridad Informática, la autora de la investigación considera que la Seguridad Informática es: El conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información ,que incluye la misma los medios informáticos (computadoras con todos sus periféricos su cuidado y conservación.)

En tal sentido es necesario tener presente que la Seguridad Informática está compuesta por dos elementos esenciales, la seguridad física y la seguridad técnica o lógica, dentro de la seguridad física se puede precisar lo relacionado con el local, (estado constructivo, enrejado, climatización), el control de los accesos, (entrada de personal no autorizado), sistemas de detección de intrusos, (alarmas); dentro de la seguridad técnica o lógica está, la autenticación (uso de identificadores y contraseñas), instalación y actualización de antivirus, implementación de fireware (cortafuegos, evitar la penetración de intrusos por la red), salvadas de informaciones o de un software específico, la criptografía como medio para resguardar la información clasificada.

El término seguridad física en informática, es el usualmente empleado para describir las medidas de protección externas, éstas tratan de proteger a los medios informáticos y su entorno de amenazas físicas, las principales de las cuales se deben proteger los medios informáticos son: Inundaciones por intensas lluvias, desborde de ríos, penetraciones del mar, inundaciones

¹⁵López Miera Álvaro. Orden No. 361 del Vice Ministro Jefe Estado Mayor General para poner en vigor el Manual de Seguridad Informática de las FAR, La Habana, 2009. –5p

internas producto a filtraciones de agua por techos, paredes y pisos; fuegos, caídas de tensión, calor, interferencias electromagnéticas, atentados y hurtos.

Por lo que respecta a las medidas técnicas o lógicas pretenden proteger tanto el software, sea de base o de aplicación, como los datos. Estas medidas pueden implementarse en dispositivos hardware o en productos software.

Consecuentemente a todo lo anterior, la seguridad de las tecnologías de la información, y por ende de la informática, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de la sociedad.

La labor de seguridad suele requerir actualizaciones periódicas o las revisiones correspondientes, estos cambios se realizan cuando las configuraciones así como otras condiciones o circunstancias cambian considerablemente o en el momento que se modifican leyes y normas organizativas.

Las instituciones y los programas de formación deben liderar y servir como modelo para la capacitación y superación de los profesores sobre Seguridad Informática y de su personal de apoyo, en lo que respecta a nuevos métodos pedagógicos y nuevas herramientas de aprendizaje.

1.4 Sistema de actividades. Potencialidades

Para la elaboración de las actividades se consultó la R/M 200/14 de trabajo metodológico y se realizó el análisis de sus diferentes formas y vías para el desarrollo del sistema de actividades que se presentan, estas se elaboran a partir de los principios propuestos y del modelo de la preparación de los profesores sobre Seguridad Informática. Tiene como propósito la organización y la preparación de los implicados, la determinación de las precisiones que garanticen una dirección coherente, así como la utilización de la diversidad de fuentes de información que en un proceso comunicativo para una preparación objetiva, válida y confiable.

La autora asume la definición dada por el Dr. Luís Ernesto Martínez González en su tesis sobre el tema El Sistema de actividades: "(...)Conjunto de actividades relacionadas entre sí de forma tal que integran una unidad, el cual contribuye al logro de un objetivo general como solución a un problema científico previamente determinado (...)”¹⁶ y la que se da en la resolución

¹⁶Martínez L. E. El Sistema de Actividades Como Resultado Científico en la Maestría en Ciencias de la Educación. “Juan Marinello”, Matanzas, 2008.

200/2014 sobre sistema de actividades metodológicas: ... Sistema de actividades que de forma permanente y sistemática se diseña y ejecuta por los cuadros de dirección, funcionarios y los docentes en los diferentes niveles y tipos de educación para elevar la preparación política – ideológica, pedagógica metodológica y científico técnica de los funcionarios en diferentes niveles, los docentes graduados y en formación... a fin de ponerlos en condiciones de dirigir eficientemente el proceso educativo...

El sistema de actividades metodológicas está organizado de acuerdo a los objetivos específicos, que tiene como finalidad dirigir y orientar a los profesores en los procesos de asimilación de los contenidos a través de los mecanismos de búsqueda, selección, creación, conservación y procesamiento interactivo de la información

El sistema de actividades metodológicas debe proporcionar en los educadores la apropiación del contenido y desarrollar, paralelamente con él, habilidades informáticas. Para la elaboración de las actividades metodológicas se proponen los pasos en correspondencia con la estructura de la acción (orientación, ejecución y control).

Recomendaciones al educador para la elaboración de las actividades.

1. Diseñar la actividad a realizar:

Definir el objetivo de la actividad, el cual debe estar en correspondencia con los objetivos de la materia.

- Analizar las ventajas y desventajas al utilizar el sistema de actividades.
- Para qué educadores va a orientar la actividad.

2. Establecer la relación objetivo-contenido:

- Partir del diagnóstico integral de los profesores contextualizado en la materia que se imparte y en Informática. Integrado a las informaciones acerca del grupo, el contexto social y el individuo.
- Determinar en qué momento se va a utilizar la actividad.

3. Establecer la secuencia de pasos a seguir por el profesor:

- ¿Cuál o cuáles actividades va a utilizar?
- ¿El qué (qué contenidos del sistema de actividades va a seleccionar)?
- ¿Para qué (resultado)?

4. Exigencias metodológicas generales a considerar en el proceso de elaboración.

- Potenciar la integración de la unidad de lo instructivo, lo educativo y lo desarrollador en la formación del educador.
- Debe comprender orientaciones, acciones y operaciones que conduzcan a los educadores a: Integrar, generalizar, consolidar, ejercitar, evaluar y autoevaluar lo aprendido.

Potencialidades para orientar un sistema de actividades metodológicas que contribuyan a la cultura en Seguridad Informática

La informática como ciencia del tratamiento de la información, considerada como soporte de los conocimientos humanos en los campos técnico-económico-social, permite a costos cada vez más bajos obtener calidades superiores en un menor tiempo y con un menor esfuerzo.

El desarrollo de la capacitación para apoyar la labor de los profesores durante el proceso de enseñanza aprendizaje en materia de Seguridad Informática, tiene como objetivo fundamental hacer más asequible, científico, motivante, objetivo, consciente, activa y amena la adquisición de conocimientos, al preservar la labor educativa del profesor dentro del proceso antes mencionado. Un empeño de tal naturaleza requiere, sin lugar a dudas, el empleo de los recursos de la informática, los cuales se han adentrado en el trabajo educacional como una necesidad de primer orden.

Mediante la creación de un sistema de actividades metodológicas que contribuya a la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre, se facilita la apropiación de contenidos científicos actualizados, conocer las amenazas, peligros, que atentan contra la Seguridad Informática en el ámbito educativo, los tipos de virus, las principales violaciones, entre otros elementos.

Proporcionar la realización de nuevas actividades metodológicas y de evaluación, el desarrollo de la Seguridad Informática aplicada a estas. Sobre lo mostrado anteriormente reafirma que el uso de estos medios ofrece importantes oportunidades en la preparación de los educadores, para la gestión y para la administración del sistema educativo y de los centros docentes, y para el intercambio de conocimientos y de experiencias.

Tiene como objetivo brindar una panorámica acerca del diagnóstico y sus resultados que permitieron la determinación de los principales problemas que en el orden de la superación tienen los profesores sobre Seguridad Informática de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.

Para ello se tuvo en cuenta el proceso de investigación realizado para el desarrollo del presente trabajo pasó por 3 fases básicas, que se refieren de manera breve a continuación:

- Estudio de antecedentes y tendencias: En esta etapa se trabajó en la elaboración del diseño teórico de la investigación, en particular lo referente al análisis histórico del objeto de investigación, y se realizó el análisis de los fundamentos teóricos referidos al objeto y campo de la investigación.
- Diagnóstico del estado actual del problema: Igualmente se trabajó en el análisis del estado actual del problema de investigación para lo cual se aplicaron un conjunto de instrumentos previamente diseñados que permitió la recopilación de datos y evidencias, se procedió al procesamiento de la información y la valoración e interpretación de los resultados, todo lo cual derivó en la determinación de problemas en la cultura informática de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.
- Construcción de la propuesta: Como respuesta al objetivo de la investigación se trabajó en el planteamiento de la alternativa de solución al problema de investigación, consistente en la propuesta de un sistema de actividades para contribuir a la cultura en Seguridad Informática de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.

A partir de lo antes expuesto se considera pertinente que las potencialidades del sistema de actividades metodológicas para contribuir a la cultura en Seguridad Informática en los profesores permiten: La utilización de los recursos informáticos en su justa medida. Para ello hay que partir de una estructura adecuada, que es tan importante como la propia información.

CAPITULO II: FUNDAMENTACIÓN PRÁCTICA SOBRE EL SISTEMA DE ACTIVIDADES METODOLÓGICAS QUE CONTRIBUYA A LA CULTURA EN SEGURIDAD INFORMÁTICA

2.1- Resultados del análisis del diagnóstico inicial aplicado para comprobar la necesidad de dar solución al problema.

La situación del estado actual de la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt fue diagnosticada a partir de la aplicación de diferentes métodos empíricos. Dentro de los métodos empíricos que se emplearon durante la investigación se encuentran: **entrevista, observación y la encuesta.**

La entrevista: Fue aplicada a 3 directivos, (el director y dos jefes de grado,) con el objetivo de comprobar cómo se concibe por parte de los directivos de la escuela actividades que contribuyan a una cultura en Seguridad Informática. **(Ver anexo 1)**

Los resultados de la entrevista fueron los siguientes:

El 100 % de los directivos expresan conocimientos acerca del concepto Seguridad Informática y conocen la importancia que tiene el uso eficiente de los medios informáticos, 2 de los entrevistados para un 66,6% con respecto al tema de la Seguridad Informática plantean en su opinión personal que a los docentes les falta preparación o responsabilidad pues en ocasiones se les pierde las informaciones o permiten que los usuarios realicen actividades no prevista es; en relación a las actividades se refieren a las preparaciones metodológicas a nivel municipal que le dan a los docentes por parte del municipio, ya que no pueden opinar acerca del contenido y no incorporan estas en las preparaciones a nivel de centro para que contribuyan favorablemente con la misma, por lo que reconocen que existen dificultades y problemas que atentan contra el conocimiento de la Seguridad Informática.

Lo anterior evidencia que los directivos, al tener poca cultura en materia de Seguridad Informática no logran integrar de modo sistemático estos conocimientos al proceso docente educativo. Es significativo que el 33 % de las respuestas reflejan no haber realizado nunca esta actividad.

Se puede concluir que los elementos ofrecidos permiten plantear que es necesario profundizar en algunos elementos necesarios dentro de la

información acerca de la cultura en Seguridad Informática que deben poseer los profesores según el criterio del director y dos jefes de grados.

La observación: Con el objetivo de obtener información acerca del desarrollo de las actividades para la educación de una cultura en Seguridad Informática en los usuarios de la ESBU “28 de Octubre” del municipio Pedro Betancourt.

Resultados de la observación. (Ver anexo 2)

Se observaron indistintamente actividades metodológicas, tiempos de máquina y clase de computación para ver en las mismas cómo se le da seguimiento a la Seguridad Informática para determinar la problemática y los errores periódicos de la misma.

De las actividades observadas, 3 fueron clases, 2 fueron actividades metodológicas y 1 fue tiempo de máquina; en las mismas se pudo constatar:

En el 100 % de las clases observadas el papel protagónico lo desempeñó el profesor y la actividad de los alumnos se limitó a observar, escuchar y tomar notas, en ningún momento se pudo apreciar ninguna acción que contribuyera al desarrollo de una cultura en Seguridad Informática lo que evidencia desconocimiento o poca importancia al tema por parte de este.

En el 50 % de las actividades metodológicas observadas se apreció en limitados momentos algunos aspectos relacionados con la Seguridad Informática.

En el tiempo de máquina observado se pudo apreciar:

El 80 % de los profesores de los diferentes grados de enseñanza muestran habilidades informáticas, poseen conocimientos básicos pero de estos solo 25% aplican las normas y procedimientos de la Seguridad Informática.

Se puede plantear que los docentes juegan el rol protagónico en las clases y no profundizan en los elementos de cultura informática.

La Encuesta: (anexo 3) Fue aplicada a 15 profesores (5 de cada grado de enseñanza) para constatar el nivel de cultura en Seguridad Informática, que poseen los profesores de la escuela.

Los resultados de la encuesta fueron los siguientes:

De los profesores encuestados: El 100% reconoce que las tecnologías de la informática y de las comunicaciones se han convertido en medios indispensables para el procesamiento de información, sin embargo 12 profesores que representa el 80% son capaces de identificar que ellas además

permiten conservar, reproducir y transmitir la información. El 73,3 % plantea que en cualquier sistema informático lo que se debe proteger es el hardware, el 66,6% opina que son los datos, el 26,6% dicen que es el hardware, pero solo el 33,3% manifiesta que son los tres; solamente el 46,6% fue capaz de identificar las características de la información que debe ser conservada en un sistema informático, el 60% identificó las características de la información que se pueden preservar en un sistema informático, relacionadas con la confidencialidad, la integridad y disponibilidad. El 40 % conoce la clasificación de la información según sus características y naturaleza, el 33,3 % expresa de manera adecuada lo que se entiende por cultura en Seguridad Informática, el 86,6 % declara que el máximo responsable de los medios informáticos en la escuela es la persona que está al frente de colectivos de trabajo que operan con este medio. Únicamente el 80% sabe cómo actuar ante indicios de contaminación por un programa maligno nuevo o desconocido, lo que ratifica las limitaciones que tienen los profesores en relación con la cultura en materia de Seguridad Informática.

Se puede determinar que los encuestados conocen los beneficios que brinda la computación para el desarrollo de los estudiantes pero les falta cultura en el dominio de elementos fundamentales de la Seguridad Informática.

Una vez aplicados y valorados los distintos instrumentos se concluye que:

Se conocen los beneficios que brinda la computación para el desarrollo de los estudiantes

Es necesario profundizar en elementos acerca de la cultura en Seguridad Informática.

Los profesores juegan el rol protagónico en las clases y no profundizan en los elementos de cultura informática

2.2 Consideraciones para la elaboración del sistema de actividades metodológicas.

La concepción de la propuesta se concibió a partir de los resultados obtenidos con el estudio previo a la muestra de investigación.

La propuesta del sistema de actividades metodológicas se caracteriza por un carácter, dinámico integrador y desarrollador de los elementos del proceso de enseñanza-aprendizaje.

Dinámico: por el modo en que declaran las relaciones existentes y concibe el desarrollo de la capacitación como parte medular en el proceso de enseñanza-aprendizaje, donde en cada paso del proceso se realizan reflexiones sobre la Seguridad Informática, su alcance y lugar en el sistema.

Integrador: por permitir la integración de todos los elementos en el desarrollo de la cultura en Seguridad Informática en el proceso de enseñanza-aprendizaje.

Desarrollador: por estimular la motivación para instruirse, la activación y regulación del aprendizaje a partir del desarrollo cognitivo alcanzado. Responde a la necesidad de perfeccionar la preparación sobre Seguridad Informática utilizando las nuevas tecnologías.

La propuesta del sistema de actividades metodológicas sugiere el cambio de determinadas insuficiencias detectadas en el desarrollo de la preparación sobre Seguridad Informática en los profesores.

Los fundamentos que constituyen la base teórica de esta investigación recrean los análisis realizados por la ciencia pedagógica acerca del desarrollo de la cultura en Seguridad Informática de los profesores. Ello, unido al empleo de las tecnologías de la Informática, constituye un apoyo importante en el proceso docente educativo; la fundamentación práctica sobre la propuesta de un sistema de actividades metodológicas para la cultura en Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt

Para la elaboración de las actividades metodológicas se tuvo presente los siguientes principios básicos:

- El sistema de habilidades en la materia de Seguridad Informática.
- Etapas del proceso de asimilación de la preparación sobre Seguridad Informática.
- Vías para la formación y desarrollo de la preparación sobre Seguridad Informática.

Se determina el objetivo para el sistema de actividades:

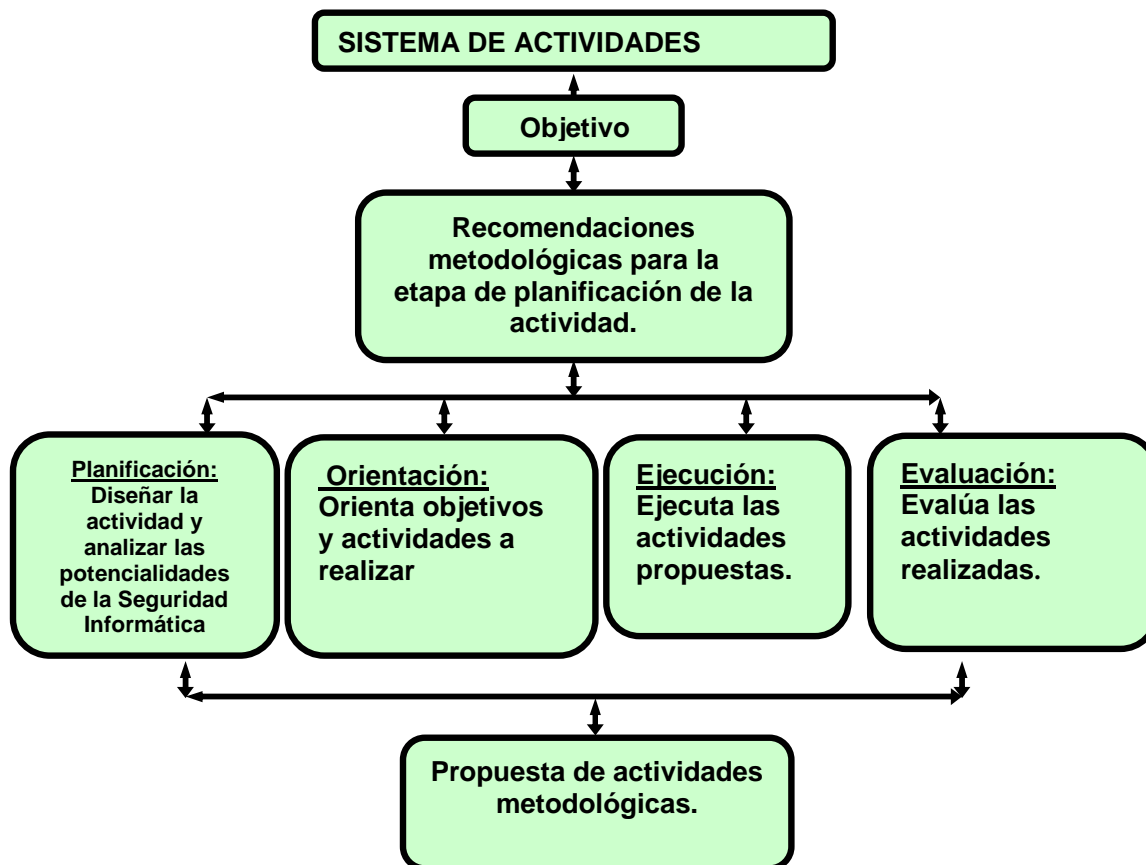
Objetivo: Capacitar a los profesores de las ESBU en el desarrollo de la Seguridad Informática a través de las actividades para lograr una cultura informática correcta.

El sistema de actividades se estructura de la siguiente forma:

- Tema

- Título
- Objetivo
- Introducción
- Desarrollo de la actividad
- Método
- Medios de enseñanza.
- Evaluación.
- Conclusión.

A continuación se presenta un esquema con los elementos esenciales que contiene el sistema de actividades metodológicas propuestas por la autora de esta investigación.



Este sistema de actividades metodológicas está organizado de acuerdo con el objetivo específico de la materia determinada, y deberá:

- Lograr niveles de asimilación superiores en los profesores.
- Proporcionar al educador procedimientos o procesos (paso a paso) que le

permitan el logro de los objetivos propuestos (estructura interna de la habilidad).

- Brindar algoritmos, secuencias de acciones, que induzcan a los profesores, a pensar, a solucionar problemas.
- Actuar de forma independiente en trabajos investigativos.

En correspondencia con lo anterior para desarrollar el sistema estratégico de la cultura sobre Seguridad Informática se utilizó un diseño de las actividades metodológicas.

La autora consideró necesario realizar acciones encaminadas a la preparación del personal de manera que el sistema de actividades que se propone para el desarrollo de la cultura en Seguridad Informática resulte efectivo y pueda ser aplicado en otros grupos de profesores de la escuela.

2.3 Sistema de actividades sobre la Seguridad Informática en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt.

A continuación, se presentan las diferentes actividades metodológicas que se incluyen en la propuesta para el desarrollo de la cultura en Seguridad Informática:

Actividad No.1

Tema: Medidas para la seguridad de los locales donde se ubican los medios de automatización y su clasificación

Título: Seguridad y protección de la información en el trabajo con los medios de automatización.

.Objetivos: Establecer requerimientos de seguridad física y técnica que deben ser cumplidos para trabajar con los medios informáticos.

Cumplir con las medidas para la seguridad de los locales donde se ubican los medios de automatización en que se procesa información.

Métodos: Conversatorios, debates, charlas y preguntas

Medios de enseñanza:

Curso Básico de Seguridad Informática.doc.

Manual del régimen especial de seguridad.doc.

Manual de la seguridad informática.doc.

Principales términos y definiciones de Seguridad Informática.doc

Introducción: Para asignar clases a las computadoras que se encuentren conectadas en redes locales, se tomarán en consideración los permisos otorgados a los usuarios de éstas para acceder a las informaciones almacenadas en la red. La clase que se le asigne se corresponderá con la información de mayor categoría de clasificación a la cual se pueda acceder desde la computadora.

Desarrollo de la actividad:

Cuando se les comunica a los profesores el objetivo de la actividad a desarrollar también se especificará el trabajo con los medios de automatización y que deben lograr por lo que se orientarán un grupo de actividades.

Sugiere las medidas que se debe garantizar en la seguridad de la instalación desde el punto de vista constructivo y de protección física de sus accesos de forma tal que imposibilite la entrada de personal no autorizado.

Después como se asegura el acondicionamiento con los medios técnicos de protección y control de acceso, los que deberán complementarse con las medidas organizativas para la compartimentación y protección de la información.

Se tomarán en consideración la clasificación de las computadoras conectadas en red, además de la clasificación de la información que se procesa y conserva en su disco duro, la mayor categoría de la información almacenada a la que se tenga acceso desde ellas, según los permisos otorgados a cada usuario.

Tener en cuenta que se prohíbe procesar, reproducir o conservar en los medios de automatización conectados en red, la información clasificada con la categoría Secreto.

Al finalizar las actividades desarrolladas se les aplica las siguientes preguntas de control:

1. ¿Qué entiendes por Seguridad Informática?
2. Los directivos y educadores de tu entidad, consideran la Seguridad Informática como responsabilidad de quién.
3. ¿Qué valores deben estar presentes en una persona que tiene a su disposición un medio informático?
4. De acuerdo a su conocimiento, ¿Qué obstáculos atentan contra la Seguridad Informática en su centro de trabajo?

5. ¿Qué otros conceptos importantes están asociados a la Seguridad Informática?

6. ¿Qué medidas de Seguridad Informática adopta usted para el respaldo de información a la hora de trabajar con los medios informáticos?

Aquí los profesores expresarán sus juicios y valoraciones.

A continuación se les orientan los siguientes ejercicios de trabajo independiente:

1. Relacionamos una lista de elementos que pueden constituir riesgos o vulnerabilidades para el sistema informático. Identifique cada caso, marque con una R los que consideres sean un riesgo y con una A los que consideres sean una amenaza.

Personal poco calificado y no confiable.

Inundaciones (intensas lluvias)

Fuego

Caídas de tensión

Interferencia electromagnética

Fluctuaciones eléctricas

2. Marque con una X: los tipos de amenazas a la que se encuentra expuesta esta entidad.

a) Clasifíquelas en accidentales o intencionales

Modificación de la información

Roturas de los medios informáticos

Pérdida de la información

Robo de tecnologías

Interrupción total o parcial de todos los servicios

3. Sus directivos, educadores, estudiantes y trabajadores en general, consideran la Seguridad Informática como responsabilidad del:

Departamento de informática

La dirección de la escuela

Todos los directivos

Todos los trabajadores

Del Jefe de Seguridad Informática

Todos los indicados en las opciones anteriores

Evaluación:

Las tareas propuestas en este grupo se recomiendan, fundamentalmente, para la fijación y consolidación mediante el trabajo independiente.

Se debe realizar una selección de las tareas más significativas, lo cual le permitirá controlar el cumplimiento del objetivo; mientras que otras servirán como complemento necesario para la preparación independiente.

Se les presenta a los profesores los siguientes análisis:

1. ¿Cuáles son las violaciones más frecuentes de la Seguridad Informática que ocurren en su centro de enseñanza?
2. Identifique algunos obstáculos asociados a la Seguridad Informática en sus locales.
3. Identifique los tipos de amenazas según su origen, accidentales (causas naturales o causas laborales y/o sociales), intencionales (internas o externas).
4. Identificar vulnerabilidades asociadas a los usuarios, a la disciplina y la tecnología informática.

Aspectos a tener en cuenta para la evaluación de la actividad.

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Actitud asumida en su realización.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Exposición del trabajo.
- ✓ Fluidez al expresar las ideas.

Conclusión:

Al finalizar la actividad los profesores podrán expresarse clara y coherentemente sobre el cumplimiento con las medidas para la seguridad de los locales donde se ubican los medios de automatización que se procesa información y permitiendo aplicar las medidas necesarias para los procedimientos de la clasificación a los medios de automatización que se exploten en las escuelas. Escriba sus conclusiones y principales reflexiones, y entrégelas al capacitador, cumpliéndose, analizando, comprendiendo y dando conformidad todos los objetivos trazados por parte de éste. También,

compártalas con sus compañeros, para comenzar a debatir tópicos relacionados con la temática.

Actividad No. 2

Tema: Procedimientos para la entrada y salida de soportes de información.

Título: Seguridad y protección en el trabajo con los soportes de información.

Objetivo: La organización de los soportes de información de acuerdo con el empleo para el que se destina cada uno.

Métodos: Debates, conversatorios y preguntas.

Medios de enseñanza:

Presentación electrónica Seguridad y protección de la información.ppt

Manual del régimen especial de seguridad.doc.

Manual de la Seguridad Informática.doc.

Principales Definiciones de Seguridad y protección de la información y sus soportes.doc

Técnicas para prevenir el acceso a la información confidencial.doc

Introducción: La organización, protección, control y correcta manipulación de los soportes de información son elementos básicos para lograr la seguridad de la información que se procesa y almacena en los medios informáticos. La autorización para la entrada/salida o entradas de soportes de información se realizará en correspondencia con lo establecido.

Desarrollo de las actividades:

Cuando se les comunica a los profesores el objetivo de la actividad a desarrollar también se especificará el trabajo con los medios de automatización y que deben lograr por lo que se orientarán un grupo de actividades.

Se requiere el chequeo de los soportes con los detectores de programas malignos.

Se exige que la persona que posea medios de almacenamientos masivos deba cumplir con las normativas para su uso, así como los distintos tipos de informaciones que en estas deben aparecer.

Se hace necesario que los profesores a partir de las actividades desarrolladas debe dirigir la atención de estos a recapacitar sobre:

1. ¿Qué valores deben estar presentes en una persona que tiene a su disposición un soporte de información?

2. ¿Cuáles son a su juicio, los tres elementos fundamentales al abordar el tema de la manipulación de los soportes de información?
3. ¿Cuáles otras medidas importantes están asociados a la correcta manipulación de los soportes de información?
4. ¿Qué establece el Manual de Seguridad Informática de tu escuela respecto al uso de los soportes de información?

Aquí los profesores expresan sus reflexiones y valoraciones.

Evaluación:

Este grupo de tareas presupone la realización de cada acción inherente a la práctica. Todas serán ejecutadas por la totalidad de los profesores manteniéndose una atención diferenciada a los que no han logrado satisfacer las condiciones necesarias relativas al dominio de cada acción.

Las tareas propuestas en este grupo se recomiendan, fundamentalmente, para la fijación y consolidación mediante el trabajo independiente, momento en que el profesor contará con la siguiente guía.

A continuación se orienta a la observación los siguientes ejercicios de trabajo independiente:

1. ¿Qué medidas tomas para proteger la información diaria que tú procesas en los soportes de información de acuerdo a su importancia. Qué procedimientos utilizas para las salvadas de información en sus soportes?
2. Cuál es el rol de los directivos, funcionarios y profesores ante un incidente de Seguridad Informática de mala manipulación en los soportes de información en una escuela?
3. ¿Cuáles son a su juicio, las medidas que se deben tomar en una computadora para el uso de los soportes de información?
4. Haga una valoración crítica al respecto y que debe conocer usted y el resto de los usuarios para no cometerlas.
5. ¿Qué establecen las medidas de la Seguridad Informática, sobre tu responsabilidad personal, como usuario de estos recursos, referente a la organización, protección, control y correcta manipulación de los soportes de información. Cómo lo harías.
6. Diga al menos tres ideas de cómo te gustaría que fuera abordado este tema en tu entidad.

La evaluación de cada trabajo se hará individual teniendo en cuenta los niveles de desempeño.

Para la evaluación de la actividad (todo lo que se realiza de ellas, como trabajo independiente) se tendrán en cuenta los siguientes aspectos:

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Calidad del trabajo final.
- ✓ Actitud asumida en su realización.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Fluidez al expresar las ideas.

Conclusión:

Al finalizar la actividad los profesores podrán expresarse clara y coherentemente sobre los procedimientos para la entrada y salida de soportes de información y permitiendo aplicar las medidas necesarias para el traslado de dichos soportes. Escriba sus conclusiones y principales reflexiones, y débatalas con sus compañeros, compártalas con sus compañeros, para comenzar a debatir tópicos relacionados con la temática.

Actividad No. 3

Tema: Protección contra programas malignos. Normativas para los programas de detección y descontaminación.

Título: Las medidas de seguridad técnica.

Objetivo: Explicar la responsabilidad individual de los ejecutores que responden o trabajan con la información que se procesa, conserva e intercambia por los medios informáticos.

Métodos: Conversatorios, debates, charlas y preguntas

Medios de enseñanza:

Fichero sobre las bases legales de la Seguridad Informática en Cuba

Manual del régimen especial de seguridad.doc.

Manual de la Seguridad Informática.doc.

Principales Términos y Definiciones de Seguridad Informática.doc

Consejos para navegar de forma segura.doc

Introducción: Los jefes de cada entidad son los responsables de la

implementación de las aplicaciones y programas para la protección de contra programas malignos, específicamente los antivirus. Se consideran programas malignos los virus, caballos de Troya, gusanos o worm, bombas lógicas, jokes, hoaxes u otros programas cuya explotación no esté autorizada en el MINED, que afecten el rendimiento y la eficiencia de las redes informáticas y las microcomputadoras.

Desarrollo de las actividades:

Cuando se comunica el objetivo de la actividad también se sugiere tener presente las medidas de seguridad técnica y las normativas para los programas de detección y descontaminación.

En esta actividad tendrás en cuenta la posibilidad de la orientación para detectar los códigos malignos. Se utilizarán los programas propios desarrollados y otros productos antivirus definidos por la dirección de comunicaciones en los estándares de software y garantizarán que, al detectar dicho código maligno se realice las acciones siguientes:

Se debe bloquear la microcomputadora y la interrupción del trabajo.

Se descontamina la microcomputadora y la continuidad del trabajo.

No permitir que no se disemine el programa maligno.

El personal especializado realice los trabajos de descontaminación y se evite la pérdida de la información.

Se debe realizar las investigaciones y los análisis necesarios sobre el tipo de programa maligno, las fuentes y vías de contagio.

Determinar las responsabilidades del personal involucrado en la contaminación y las violaciones cometidas.

Garantizar los programas de detección implantados, su ejecución de forma obligatoria una vez al día o la activación de éstos como centinela en memoria y se prohíbe la interrupción de su ejecución y su alteración.

Se hace obligatorio para preservar los programas y la información ante las consecuencias que pudieran derivarse de la aparición de un programa maligno, durante la explotación de los medios informáticos que:

Se requiere que el jefe de Seguridad Informática revisa con los programas detectores todo soporte de información removible al recibirse de los depósitos habilitados por los ejecutores.

Se verifica con los detectores todos los soportes removibles que se entreguen o

reciban, en presencia del usuario.

Debe someterse todo soportes a revisión con los programas detectores en el momento de su utilización y antes de realizar cualquier otra operación sobre éste.

Impedir que alguna persona ajena a la escuela haga uso de los medios informáticos sin la presencia de una persona autorizada que supervise la correcta operación y el cumplimiento de las medidas de protección.

Mantener protegidos contra escritura los soportes de información originales de los softwares básicos y de aplicación que no requieran actualización periódica.

Ejecutar la carga del sistema operativo siempre desde el disco duro, a menos que existan condiciones objetivas que lo impidan.

Después de ejecutar las actividades desarrolladas se indica las siguientes preguntas de control:

1-¿Qué virus han afectado en tu entidad, que efectos ha provocado en tu computadora?

2-¿Cuáles son a su juicio, las medidas que se deben tomar en una computadora para el uso de dispositivos externos?

3-Ponga un ejemplo de amenazas, riesgos, vulnerabilidad e incidentes de seguridad técnica en el sistema informático de tu entidad.

Los profesores expresarán sus prudencias y valoraciones.

A continuación se orienta los siguientes ejercicios de trabajo independiente:

1.- Al detectar un programa maligno usted actúa de la siguiente forma:

___Apaga la PC y se retira sin informar al personal facultado para su tratamiento.

___Retira su dispositivo y reinicia la PC

___Informa al personal facultado para su tratamiento

___Aísla (desconexión) el medio, procede a descontaminar utilizando la herramienta para ello (antivirus), escribe el incidente en el registro designado.

2.- ¿Qué vulnerabilidades pudieran determinarse a partir de estas amenazas?

_____Antivirus ineficientes.

_____Antivirus desactualizados.

_____Usuarios con desconocimientos.

3.- Proponga al menos tres actividades que sean factibles desarrollar en su entidad, con un carácter sistemático y posibiliten la vitalidad al tratamiento de los temas de seguridad técnica.

Evaluación:

Se realizará de forma individual. La misma será evaluada de acuerdo a los niveles de progreso. Las tareas propuestas en este grupo se recomiendan, fundamentalmente, para las clases de ejercitación y consolidación, así como mediante el trabajo independiente, momento en que el profesor contará con la siguiente guía.

¿Cómo se percata usted de que el antivirus instalado en su PC no se encuentra actualizado?

¿Qué acciones deben tener en cuenta cuando se trabaja con medios extraíbles?

Identifica las causas que pudieran provocar conductas de amenazas en sus instituciones.

Mencione algunas amenazas más comunes.

Para la evaluación de la actividad (todo lo que se realiza de ellas, como trabajo independiente) se tendrán en cuenta los siguientes aspectos:

Análisis realizado al responder cada una de las preguntas.

-
- ✓ Si todas fueron contestadas.
 - ✓ Originalidad de las respuestas.
 - ✓ Actitud asumida en su realización.
 - ✓ Grado de reflexión y coherencia del trabajo.
 - ✓ Utilización adecuada de todos los recursos disponibles.
 - ✓ Fluidez al expresar las ideas.

Conclusión:

Al finalizar la actividad los profesores podrán expresarse clara y coherentemente sobre la protección contra programas malignos y permitiendo aplicar las medidas necesarias para los procedimientos ante la aparición de éstos programas. Escriba sus conclusiones y principales reflexiones, y entrégalas al capacitador, cumpliéndose, analizando, comprendiendo y dando conformidad todos los objetivos trazados por parte de éste. También, compártalas con sus compañeros, para comenzar a debatir tópicos

relacionados con la temática.

Actividad No 4:

Tema: Las contraseñas.

Título: Sistema de control de acceso a los medios informáticos.

Objetivo: Restringir el acceso a un archivo, red, o computadoras autónomas a las personas autorizadas.

Métodos: Conversatorios, debates y preguntas

Medios de enseñanza:

Presentación electrónica Seguridad y protección de la información.ppt

Manual del régimen especial de seguridad.doc.

Manual de la seguridad informática.doc.

Programas malignos y virus informáticos.ppt

Principales Definiciones de Seguridad y protección de la información y sus soportes.doc

Amenazas en los sistemas de mensajería instantánea y las redes.doc

Técnicas para prevenir el acceso a la información confidencial.doc

Introducción: Las contraseñas de protección son intransferibles a personal no autorizado y deben conservarse en sobres lacrados en la oficina de procesamiento y control de la información. El jefe de la Seguridad Informática responde por la actualización sistemática de éstas en las computadoras.

Desarrollo de las actividades:

Cuando el capacitador comunica el objetivo de la actividad también explicará el sistema de control de acceso a los medios informáticos.

Mediante una conversación con los profesores se debe dirigir la atención de estos a reflexionar sobre las contraseñas, que por lo general es uno de los eslabones más débiles de la seguridad cuando no se cumplen los procedimientos establecidos. Para establecer, generar, controlar y emplear las contraseñas, se deben orientar las siguientes actividades:

Se permite solamente las personas autorizadas al acceso a los recursos y sólo serán de conocimiento de éstas.

Deberá cambiarse de inmediato al cumplir el período de vigencia máximo de 90 días, excepto en caso de comprometimiento, siendo responsabilidad del propietario modificarlas.

Se procederá de inmediato a deshabilitar los permisos y a cambiar las claves

que empleaba el personal que fue objeto de movimiento. (al producirse traslados, bajas, etc.).

Guardar en el local habilitado las contraseñas de acceso a la máquina en sobres registrados y sellados por el propietario de la contraseña y sólo tendrá acceso el propietario y sus jefes superiores.

Se garantizará que las contraseñas se conserven cifradas y que no sean accesibles a los administradores.

Clasificar en correspondencia con la clasificación de la máquina o aplicación a la que permite el acceso y se entregará al usuario cumpliendo lo establecido para el registro, control y manipulación de información clasificada.

Se dividirá el teatro en seis equipos donde se orientará a los profesores, a investigar para dar respuesta a las preguntas de control: ¿Qué establece el Manual de Seguridad Informática de tu escuela respecto al empleo de las contraseñas?

2. ¿Qué establecen las medidas de seguridad y protección, sobre tu responsabilidad personal, como cuadro de dirección y como usuario el control y empleo de las contraseñas?

3. ¿Cuáles son a su juicio, los elementos fundamentales al abordar el tema del correcto empleo de las contraseñas en tu escuela?

4. ¿Cuáles otras restricciones importantes están asociados al control, y empleo de las contraseñas?

Aquí los profesores expresan sus reflexiones y valoraciones.

Evaluación:

Se debe realizar una selección de las tareas más significativas, lo cual le permitirá controlar el cumplimiento del objetivo; mientras que otras servirán como complemento necesario para la preparación independiente.

El capacitador presenta a los profesores el siguiente estudio de trabajo independiente:

1. ¿Qué medidas de Seguridad Informática adopta usted para el respaldo del control y empleo de las contraseñas a la hora de trabajar en su computadora?

2. ¿Cuáles son las violaciones más frecuentes en generar, controlar y emplear las contraseñas que ocurren en su centro de enseñanza?

3. ¿Cuáles son a su juicio, los procedimientos establecidos que se deben tomar en una computadora para el empleo correcto de las contraseñas?
 4. ¿Qué aspectos de código de ética de tu entidad sobre el uso de las tecnologías y las comunicaciones abordan el tema del uso de las claves de acceso y del correo electrónico?
 5. ¿Cómo está conformada tu clave de acceso, total de dígitos, de ellos cuantos números, cuántas letras y cuántos caracteres especiales?
 6. Ponga un ejemplo de amenazas, riesgos, vulnerabilidad e incidentes de seguridad en el sistema informático de tu entidad, en la utilización de las contraseñas en el correo electrónico y el uso de claves de acceso.
- La evaluación de cada labor se hará grupal teniendo en cuenta los niveles de trabajo.

Para la evaluación de la actividad (todo lo que se realiza de ellas, como trabajo independiente) se tendrán en cuenta los siguientes aspectos:

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Exposición del trabajo.
- ✓ Fluidez al expresar las ideas.

Actividad No. 5

Tema: Auditoría y control.

Título: Controles al Estado de la seguridad y protección de la información en el trabajo con los medios de automatización y sus soportes.

Objetivo: Evaluar el comportamiento de los sistemas informáticos, en correspondencia con los procedimientos técnicos-organizativos de seguridad y protección.

Métodos: Conversatorios, debates y preguntas

Medios de enseñanza:

Manual del régimen especial de seguridad.doc.

Manual de la Seguridad Informática.doc.

Algunos ejemplos para que sirvan de guía en el análisis con los usuarios.doc

Presentación electrónica Seguridad y protección de la información.ppt

Principales Definiciones de Seguridad y protección de la información y sus soportes.doc

Técnicas para prevenir el acceso a la información confidencial.doc

Introducción: La auditoría y control desempeñan un papel prioritario en el funcionamiento eficiente y el perfeccionamiento constante de los sistemas de seguridad, ya que permiten a los directivos y ejecutores desarrollar una persuasiva y preventiva ante las violaciones y deficiencias que puedan existir en los sistemas.

Desarrollo de las actividades:

Cuando el capacitador comunica el objetivo de la actividad también hablará sobre los Controles al estado de la seguridad y protección de la información en el trabajo con los medios de automatización y sus soportes, por lo que se orientarán un grupo de actividades.

Sugiere las medidas que se debe garantizar en todos los sistemas operativos, aplicaciones, servicios y equipamiento que conforman los sistemas informáticos que se procesen, almacenan y transmita información, se implementarán los registros de las trazas de las operaciones realizadas y las herramientas para su consulta y procesamiento, además en esta actividad tendrás la posibilidad de aplicar:

Los mecanismos de auditoría que correspondan, lo cual estará descrito en la carpeta de administración del sistema de aplicación en los medios informáticos que tengan instalados programas de control de acceso, sistemas operativos y sistema de gestión de base de datos.

Organizar la realización de autocontroles al empleo de las aplicaciones y servicios informáticos por el personal subordinado al director, en el marco de autocontroles mensuales, empleando para ello las herramientas de auditoría implementadas en cada aplicación o servicio y reflejando los resultados en la libreta de autocontrol mensual de la oficina de procesamiento y control de la información.

Controlar, durante los controles de la Seguridad Informática los resultados de los autocontroles realizados por los jefes a cada nivel.

Comprobar los soportes técnicos de información removibles y no removibles existentes en la entidad.

Chequear el cumplimiento del control del cambio de formato y de su movimiento fuera de la entidad, el empleo del formato establecido por el sistema de protección de las computadoras en vigor para el intercambio de información en estos soportes.

Analizar la conservación actualizada de las contraseñas de acceso a las computadoras existentes en la entidad.

Comprobar el cumplimiento de lo establecido en el plan de Seguridad Informática para la clasificación de los medios de automatización de la escuela y la instalación de los productos de Seguridad Informática.

Inspeccionar la existencia y objetividad del plan de evacuación y los medios necesarios para su cumplimiento.

Se hace necesario que los profesores a partir de las actividades desarrolladas deben dirigir la atención de estos a reconsiderar sobre las siguientes preguntas de control:

1. ¿Qué establece el Manual de Seguridad Informática de tu escuela respecto a la actualización y cumplimiento de los controles y auditoría de los sistemas informáticos?
2. ¿Qué establecen las medidas de seguridad y protección, sobre tu responsabilidad personal, como cuadro de dirección y como usuario el control y auditoría de los sistemas de seguridad?
3. ¿Cuáles son a su juicio, los procedimientos fundamentales al abordar el tema del empleo del control y auditoría de los sistemas informáticos en tu escuela?
4. ¿Cuáles otros procedimientos importantes están asociados al control, y evaluación del comportamiento de los sistemas informáticos?

Aquí los profesores expresan sus juicios y valoraciones.

Evaluación:

Se realizará de forma individual. La misma será evaluada de acuerdo a los niveles de perfeccionamiento, lo cual le permitirá controlar el cumplimiento del objetivo.

Este grupo de tareas presupone la realización de cada acción inherente a la práctica.

El capacitador orienta a los profesores la siguiente observación de trabajo independiente:

1. Qué importancia le concede a la auditoría y control en el funcionamiento eficiente y el perfeccionamiento constante de los sistemas de seguridad?
2. ¿Cuáles son los objetivos y procedimientos para la realización del control de los sistemas informáticos?
3. ¿Cuáles son los documentos legales que rigen el trabajo con la Seguridad Informática en nuestro país?
4. ¿Cuáles son las violaciones detectadas que ponen en evidencia la superficialidad en el trabajo de los sistemas informáticos?

Para la evaluación de la actividad (todo lo que se realiza de ellas, como trabajo independiente) se tendrán en cuenta los siguientes aspectos:

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Calidad del trabajo final.
- ✓ Actitud asumida en su realización.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Las evaluaciones obtenidas en la realización de los ejercicios de la actividad (más del 97% de efectividad). La calificación de 5 es de sobresaliente, la de 4 es de bueno (las 3 primeras bien y la cuarta no menos de regular), la de 3 puntos es de regular (las 3 primeras bien y una mal) y la calificación de 2 es de mal (cuando no se cumple los requisitos).

Conclusión:

Al finalizar la actividad los profesores podrán expresarse clara y coherentemente sobre la auditoría y control y acceder en el funcionamiento eficiente y el perfeccionamiento constante de los sistemas de seguridad. Escriba sus conclusiones y principales reflexiones, y entrégelas al capacitador, cumpliéndose, analizando, comprendiendo y dando conformidad todos los objetivos trazados por parte de éste. También, compártalas con sus compañeros, para comenzar a debatir tópicos relacionados con la temática.

(Actividades 6, 7, 8, 9, 10 en los anexos)

2.4 Valoración del sistema de actividades metodológicas por docentes especialistas en informática.

Se consultaron 10 especialistas en informática de ellos 2 metodólogos que atienden informática, el jefe del departamento de Seguridad Informática del municipio, 4 docentes licenciados en informática con experiencias en el trabajo y 4 profesores que se desempeñan como responsables de Seguridad Informática en áreas de la UMCC Sede “Juan Marinello Vidaurreta” con experiencia en el trabajo con la tecnología informática y el cumplimiento de las normativas para el trabajo con las mismas se determinó:

1ro. La totalidad de los consultados coincidieron en que el Sistema de Actividades Metodológica elaborado por la autora resulta ser una vía ideal en los profesores de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt a fin de garantizar una preparación efectiva de los profesores para el trabajo con los medios informáticos.

2do La elaboración del mismo refleja los requisitos teóricos que lo sustentan, tiene gran importancia para la comprensión por los profesores.

3ero. Los consultados consideraron que la disponibilidad del Sistema de Actividades Metodológica elaborado por la autora de la investigación, resulta ser una solución de importancia a las limitaciones que aún presentan los usuarios de la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt para el trabajo con la información y los medios informáticos.

4to. Se expresó, por parte de los consultados, que la autora debe tener en cuenta la facilitación al máximo de las potencialidades que el Sistema de Actividades Metodológica brinda para garantizar los procesos de retroalimentación de sus profesores. Este aspecto se tuvo en cuenta y se enfatizó con posterioridad por parte de la investigadora en la culminación de su trabajo.

Las consideraciones anteriores evidencian que el Sistema de Actividades Metodológica elaborado, objeto de proposición en la presente investigación, a criterio de los compañeros consultados, responde a las exigencias esenciales para lo que se propone.

El análisis de los resultados obtenidos en la fase de diagnóstico demuestran que, aunque es importante el uso de las tecnologías de la información para la enseñanza y obtención de los conocimientos en el proceso de capacitación,

estos se deben usar de forma sistemática, y que todos los especialistas estén preparados para interactuar con estos medios para aumentar el acceso a la información más actualizada.



CONCLUSIONES

- La sistematización lograda sobre el objeto de la investigación permitió obtener los fundamentos teóricos necesarios que se sustentan en lo declarado por el Ministerio de Educación en cuanto al conocimiento que se debe poseer para trabajar con los medios informáticos.
- El diagnóstico realizado a partir de la utilización del método dialéctico materialista como metodología general del conocimiento científico y los métodos de nivel empírico permitieron determinar que existen insuficiencias en el desarrollo de una cultura informática en los profesores de la ESBU “28 de Octubre” del municipio Pedro Betancourt.
- La concepción de las actividades elaboradas contribuyen a elevar la cultura en Seguridad Informática en los profesores de las escuelas secundarias básicas y se contextualizan en un grupo de dimensiones e indicadores como premisas para el logro del objetivo propuesto.
- La valoración crítica de un grupo de especialistas sobre el sistema de actividades metodológicas demostró su pertinencia para ser aplicada en la ESBU “28 de Octubre” del municipio Pedro Betancourt.

RECOMENDACIONES

- Incluir el sistema de actividades metodológicas en la escuela secundaria básica urbana 28 de Octubre del municipio Pedro Betancourt como un modo de contribuir a la capacitación en los profesores sobre Seguridad Informática.
- Perfeccionar la estructura del sistema de actividades metodológicas en función de nuevas necesidades que surjan en proceso de informatización de la sociedad.
- Ofrecer este ciclo de actividades metodológicas al resto de las escuelas secundarias básicas del municipio Pedro Betancourt.



BIBLIOGRAFÍA

- 200/2014, R. (2014). Reglamento del Trabajo Metodológico del Ministerio de Educación. Cuba: MINED.
- Fundamentos de las Educación: metodología de la investigación y calidad de la educación. Metodología de la investigación educacional en Maestrias en ciencias de la Educación Ciencias. (2006). La Habana: MINED.
- Aspectos Básicos de la Seguridad Informática. (2009). La Habana, Cuba.
- Reglamento Plan de Seguridad Informática. Resolucion 17/2010 del reglamento sobre la Seguridad y Proteccion de la Información Oficial. (2009). Cuba.
- Autores, C. d. (2007). Introducción de las tecnologías de la información y las comunicaciones en la escuela y su impacto en el aprendizaje. La Habana: Educación Cubana.
- Autores, C. d. (s.f.). Introducción de las tecnologías de la información y las comunicaciones en la escuela y su impacto en el aprendizaje de los estudiantes. Ministerio de Educación.
- autores, C. d. (s.f.). Metodología de la investigación (Parte II). Pueblo y Educación.
- Autores, C. d. (s.f.). Metodología de la Investigación (I parte). Habana: Pueblo y Educación.
- Castro Ruz, F. (1999). Cuba Socialista. Habana.
- Diccionario Enciclopédico Grijalbo. (s.f.).
- Ernesto, M. G. (2008). El sistema de actividades como resultado científico en la maestría en Ciencias de la Educación. Matanzas, Cuba.
- Exposito Ricardo, C. (2002). La informática educativa en la escuela cubana. La Habana.
- Genaro Navarro, E. (2005). Temas de Informática Básica. La Habana: Pueblo y Educación.
- Hart, A. (1977). .Identidad vs globalización. Hacia una ética humanista en la postmodernidad.
- Herrera Santana, R. (s.f.). La informatización de la sociedad: un reto para la educación cubana. .

<http://www.monografias.com>. (s.f.). Obtenido de <http://www.monografias.com/trabajos7/tain/tains.html>

Lopez Miera, A. (2009). Orden No. 361 del Viceministro Jefe de Estado mayor general para poner en vigor el manual de Seguridad Informática en las FAR. La Habana, Cuba.

Martí Pérez, J. (1963). Obras Completas T.8. La Habana: Nacional de Cuba.

MINED. (s.f.). Fundamentos de la investigación educativa. I. La Habana, Cuba.

Peña Colina, H. (2009). La educación de una cultura informática em los usuarios de la red del Instituto Superior Pedagógico Juan Marinello en materia de seguridad informática. Tesis en opcion al título de maestría. Matanzas, Cuba.

Pérez Fernández, V. (1997). La preparación del maestro para la inserción de la computadora en la actividad docente. Curo 63 de pedagogía. Cuba.

Pontes, A. (2005). Aplicaciones de las tecnologías de la información y de la comunicación en la educación científica. Eureka, 2(1).

Reglamento sobre seguridad Informática, puesto en vigor por la Resolución No 6 de 2006 del Minsiterio del Interior. (s.f.).

Reglamento sobre seguridad Informática. . (s.f.). Resolución No 176 de 2007 del Ministerio de Informática y Comunicaciones.

Sánchez, J. (s.f.). ""<http://revista.inie.ucr.ac.cr/articulos/1-2004/archivos/informatica.pdf>.

ANEXOS

ANEXO 1

Entrevista

Objetivo: Comprobar el criterio que tienen los directivos del centro sobre la cultura en Seguridad Informática que poseen los docentes, así como las actividades que se planifican y concretan para lograr dicho objetivo.

Compañero directivo: Es necesario su cooperación al responder las siguientes preguntas sobre la Seguridad Informática en la escuela.

Datos generales:

Nombre y apellidos: _____

Años de experiencias en la labor educativa: _____

Su especialidad es: _____

- 1- ¿Qué entiendes por Seguridad Informática?
- 2- ¿Consideras importante el tema de la Seguridad Informática para ser tratado con los docentes? ¿Por qué?
- 3- En su opinión como directivo ¿Consideras que los docentes están preparados con respecto a lo que es Seguridad Informática? Argumenta.
- 4- ¿Qué espacio le aportas al tema Seguridad Informática en las preparaciones metodológicas?
- 5- Existen algunas bibliografías en el centro que tengan relación con este tema. ¿Cómo se utilizan?
- 6- ¿Qué solución usted propone?

ANEXO 2

GUÍA DE OBSERVACIÓN

Objetivo: Obtener información acerca del desarrollo de las actividades para la educación de una cultura en Seguridad Informática en los usuarios de la ESBU “28 de Octubre” del municipio Pedro Betancourt.

Aspectos a Observar:

- ✓ Como se manifiestan los alumnos, profesores y personal de apoyo a la docencia a la hora de trabajar con las tecnologías informáticas.
- ✓ Comportamiento ético y auto regulado.

✓ Habilidad de los usuarios al aplicar las normas y procedimientos de la Seguridad Informática.

Para la observación al laboratorio esta investigación se rige por la guía establecida por el MINED y el Ministerio de la Informática y las Comunicaciones con las siguientes dimensiones a medir:

- Organización en el local.
- Orientación hacia los objetivos trazados.
- Selección, organización y tratamiento de los contenidos.
- Utilización de medios de enseñanza.
- Métodos de trabajo.
- Formas de organización de la actividad.
- Control y evaluación del aprendizaje.
- Integración del contenido de la materia.
- Clima psicológico y político moral.
- Trabajo coordinado entre los profesores.
- Algoritmos de trabajo

ANEXO 3

ENCUESTA A PROFESORES DE LA ESBU “28 DE OCTUBRE”.

Estimados usuarios:

Para contribuir al desarrollo de una cultura en Seguridad Informática en los profesores de la ESBU “28 de Octubre” se está desarrollando la presente investigación para lo cual se solicita su cooperación en el llenado de esta encuesta.

Muchas gracias.

Objetivo. Constatar el nivel de cultura en Seguridad Informática, que poseen los profesores de la escuela.

Para el caso de cada pregunta marque con una x las definiciones que considere acertadas.

1-Las tecnologías de las informáticas y de comunicaciones se han convertido en medios indispensables para:

_____ El procesamiento de información.

_____ Conservación de la información.

_____ Reproducción de información.

_____ Transmisión de información.

2-En cualquier sistema informático los elementos que se deben proteger son:

___ El hardware.

___ El software.

___ Los datos.

3-Las características de la información que deben ser preservadas en un sistema informático son:

_____ Su confidencialidad.

_____ Su integridad.

_____ Su disponibilidad.

_____ Su contenido.

4- La información por sus características y naturaleza se divide en tres grupos:

_____ Limitada _____ Confidencial _____ Secreta.

_____ Clasificada. _____ Limitada. _____ Ordinaria.

5- Por capacitación sobre Seguridad Informática se entiende:

_____ Manejo adecuado de los recursos informáticos.

_____ Habilidades en el trabajo con los medios informáticos.

_____ No divulgación de la información que se procesa, intercambia reproduce o conserva en los medios informáticos.

_____ Habilidades básicas en la utilización de la informática como apoyo a la actividad del individuo, lo cual es de utilidad en cualquier área de aplicación, utilizando como apoyo la búsqueda, procesamiento y presentación eficiente de la información, teniendo en cuenta todo lo reglamentado para su adecuado uso.

6- El máximo responsable de los medios informáticos en la escuela es:

_____ El director de la entidad.

_____ El técnico de seguridad y protección.

_____ El responsable de Seguridad Informática.

_____ La persona que está al frente de la cátedra

7-Ante indicios de contaminación por un programa maligno nuevo o desconocido usted debe:

_____ Descontaminar.

_____ Aislar el ordenador.

_____ Comunicarlo de inmediato al asesor de Seguridad Informática del área.

_____ Esperar que lleguen los especialistas.

ANEXO 4

ENTREVISTA A LOS ESPECIALISTAS

Datos Generales del Especialista

Nombres y Apellidos: _____

Categoría Docente: _____

Categoría Científica: _____

Especialidad: _____

Centro de trabajo: _____

Cargo que ocupa: _____

Años de experiencia: _____

Estimado compañero(a)

Solicitamos su cooperación con vista a valorar el Sistema de Actividades propuesto, el cual fue elaborado con el objetivo de contribuir a la educación de una cultura informática en los profesores de la ESBU "28 de Octubre" del municipio Pedro Betancourt. Sus criterios son de gran importancia, por lo que pedimos su colaboración marcando con una X en la casilla correspondiente.

MUCHAS GRACIAS.

Escala:

TA ___ Totalmente de acuerdo

PA ___ Parcialmente de acuerdo

D ___ Desacuerdo

ASPECTOS A CONSIDERAR				
PEDAGÓGICOS		TA	PA	D
1	El Sistema de actividades propuesto fortalece la preparación de los profesores en materia de Seguridad Informática.			
2	Responde a necesidades reales que tienen los profesores de la ESBU			
3	Desarrolla en los usuarios habilidades para el trabajo con la información en los medios informáticos.			

4	El Sistema de actividades se creó teniendo en cuenta los fundamentos que sustenta la educación media cubana.			
FUNCIONALES.		TA	PA	D
1	Validez (Facilita el logro de los objetivos que se pretende).			
2	Factibilidad de uso (Posibilidad de llevar el resultado a la práctica, sin realizar grandes gastos).			
3	Aplicabilidad (Otras personas pueden utilizarlo como material de consulta).			
4	Constituirá el Sistema de Actividades como un medio que contribuya a la educación de una cultura informática en los profesores de la ESBU en materia de Seguridad Informática			
TÉCNICOS, ESTÉTICOS Y PSICOLÓGICO.		TA	PA	D
1	Aceptable estructuración y adecuación de los contenidos desarrollados.			
2	Presenta un sistema de navegación e interacción apropiado para los distintos tipos de usuarios con que cuenta la ESBU			
3	Uso de las tecnologías avanzadas.			
4	Proporciona a los usuarios la motivación a la hora de su preparación.			

ANEXO 5

Actividad No 6

Tema: Base Legal de Seguridad Informática en Cuba.

Título: Los fundamentos de la Seguridad Informática en la educación.

Objetivo: Profundizar en los fundamentos de la Seguridad Informática, los conceptos asociados a las mismas, sus bases legales y los valores que deben estar presente en una persona que tiene a su disposición un medio informático.

Métodos: Debates, conversatorios y preguntas.

Medios de enseñanza:

Fichero sobre las bases legales de la Seguridad Informática en Cuba
Presentación electrónica Seguridad y protección de la información.ppt
Curso Básico de Seguridad Informática-16-2-2011.doc
MANUAL DE SEGURIDAD DE USUARIOS.rtf
Material_sobre_la_evolucion_Hist_de_la_SI.doc
Principales Términos y Definiciones de Seguridad informática.doc
SEGURIDAD COMPUTACIONAL Rev2.pdf
Libro Electrónico v4.1

Introducción: La Seguridad Informática en Cuba es regida desde el punto de vista legal por un grupo de acuerdos, resoluciones y decretos leyes, en las cuales se estipula el uso adecuado que se le debe dar a cada una en correspondencia con el objeto social de la entidad donde se encuentren.

Desarrollo de las actividades

Cuando se les comunica a los profesores el objetivo de la actividad a desarrollar también se les explica que en todo sistema informático deben cumplirse tres principios básicos para lograr un funcionamiento adecuado de los mismos y que esto solo se logra haciendo cumplir lo establecido desde el punto de vista legal, además dando muestra de una cultura informática.

A través de esta actividad podrán percatarse cuáles son las principales violaciones que se cometen a la hora de trabajar con las tecnologías informáticas, cómo se clasifican por su naturaleza y como actuar ante estas, para ello se apoyarán en las resoluciones 127/2007 del MIC y la 176/2007 del MINED.

Se debe investigar sobre los documentos existentes en el centro donde se plasman las incidencias ocurridas con las tecnologías informáticas, así como los análisis realizados en el consejo de dirección con sus respectivas acciones, determinando las responsabilidades de la o las personas involucradas en cualquier echo.

Se hace obligatorio preservar estos documentos o registros de incidencia y mantenerlos actualizados, para ello el jefe Seguridad Informática lo verificará diariamente.

Se mantendrán un grupo de acciones ya tratadas en otras actividades como

por ejemplo el escaneo de cualquier soporte removible, la salva y conservación de la información por parte de los usuarios, el uso de la tecnología solo por personal autorizado, etc.

Los controles o inspecciones sobre estos medios juegan un papel fundamental evitando su uso inadecuado logrando de cierto modo un funcionamiento eficiente.

Se hace necesario que los profesores a partir de las actividades a desarrollar deben dirigir la atención de estos sobre estos elementos:

- ✓ ¿Qué es para ti la Seguridad informática?
- ✓ De acuerdo a la información diaria que tú procesas en tu actividad profesional cómo la clasificarías y que medidas tomas para protegerla de acuerdo a su importancia.
- ✓ Los directivos, funcionarios, docentes, estudiantes y trabajadores en general de tu institución, consideran la Seguridad Informática como responsabilidad de quien.
- ✓ ¿Qué valores deben estar presentes en una persona que tiene a su disposición un medio informático?
- ✓ ¿Cuál es el rol de los directivos, funcionarios, maestros y profesores, secretarias, oficinistas con la Seguridad Informática en una institución del MINED?
- ✓ ¿Cuáles otros conceptos importantes están asociados a la Seguridad Informática?
- ✓ Ponga un ejemplo de amenazas, riesgos, vulnerabilidad e incidentes de seguridad en el sistema informático que usted utiliza en su institución.
- ✓ ¿Qué aspectos del código de ética de tu institución sobre el uso de las TI te llaman más la atención y por qué?
- ✓ ¿Qué establece el Reglamento disciplinario interno de tu institución respecto al uso de las TI?
- ✓ ¿Qué otros documentos rigen el trabajo con las tecnologías informáticas?
- ✓ ¿Qué establecen las bases legales de la Seguridad Informática en Cuba, sobre tu responsabilidad personal, como cuadro de dirección y como usuario de estos recursos
- ✓ Diga al menos tres ideas de cómo te gustaría que fuera abordado este tema en tu institución.

Evaluación

Se realizará de forma individual. La misma será evaluada de acuerdo a los niveles de progreso.

- ✓ ¿Cuáles son las tres violaciones más frecuentes de la Seguridad Informática que ocurren en tu escuela?
- ✓ ¿Cuáles son a su juicio, los tres elementos fundamentales para tu institución al abordar los temas de Seguridad Informática?
- ✓ ¿Qué documentos establecen la política para el trabajo con los medios informáticos?

Para la evaluación de la actividad se tendrán en cuenta los siguientes aspectos:

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Actitud asumida en su realización.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Fluidez al expresar las ideas.

Conclusión:

Al finalizar la actividad los profesores podrán expresarse sobre los principales documentos legales que rigen la actividad informática en nuestro país, las principales violaciones que se cometen al trabajar con estos medios, así como las medidas a tomar ante cualquier eventualidad.

Se les orienta de trabajo independiente la siguiente guía:

- ¿Qué entienden por hacker y cracker?
- ¿En qué se diferencian los mismos?
- ¿Cómo proceden a salvaguardar la información con la que trabajan?
- ¿A su juicio qué elementos constituyen amenazas en los sistemas informáticos de su escuela?
- ¿Cómo proceden ante la contaminación por programas malignos?

Actividad No 7

Tema: Principales escenarios para el trabajo con las tecnologías informáticas.

Título: La Seguridad Informática en las actividades cotidianas de la escuela.

Objetivo: Desarrollar actividades que permitan identificar los diferentes escenarios en que se pone en riesgo la Seguridad Informática en las actividades cotidianas de la escuela, así como las vías y procedimientos que se deben emplear para su identificación y solución.

Métodos: Conversatorios, debates y preguntas

Medios de enseñanza:

Fichero sobre las bases legales de la Seguridad Informática en Cuba

Presentación electrónica Seguridad y protección de la información.ppt

MANUAL DE SEGURIDAD DE USUARIOS.rtf

Presentación electrónica Modulo 2-Diapo 3.ppt

Principales Términos y Definiciones de Seguridad informática.doc

SEGURIDAD COMPUTACIONAL Rev2.pdf

Libro Electrónico v4.1

Hacker.doc

Hacker y cracker.doc

Amenazas en los sistemas de mensajería instantánea y las redes.doc

Algunos ejemplos para que sirvan de guía en el análisis con los usuarios.doc

Programas malignos y virus informáticos.ppt

Técnicas para prevenir el acceso a la información confidencial.doc

Introducción: El desarrollo de la actividad informática en los centros escolares constituyen escenarios donde se pueden presentar situaciones inadecuadas en el trabajo con los mismos de ahí la importancia de velar para que estas situaciones no ocurran.

Desarrollo de las actividades:

Al comunicarles a los profesores el objetivo de la actividad a desarrollar también se les recuerda lo abordado en la actividad anterior sobre los principios que deben cumplir todo sistema informático para lograr un funcionamiento adecuado de los mismos y que esto solo se logra haciendo cumplir lo establecido desde el punto de vista legal, ya que estas áreas constituyen escenarios donde se pueden materializar indisciplinas.

Con esta actividad podrán percatarse de un grupo de violaciones que se cometen a la hora de trabajar con las tecnologías informáticas.

Continuar el trabajo relacionado con los documentos existentes en el centro en las áreas donde se plasman las incidencias ocurridas con las tecnologías

informáticas, así como los análisis realizados en el consejo de dirección con sus respectivas acciones, determinando las responsabilidades de la o las personas involucradas en cualquier echo.

Se mantendrán un grupo de acciones ya tratadas en otras actividades.

Para el desarrollo de la actividad se trabajarán las siguientes preguntas:

- ¿Qué es hacker, cracker, ponga ejemplo de casos de sus formas de actuar?
- De acuerdo a la información diaria que tú procesas en tu actividad profesional que medidas tomas para protegerla de acuerdo a su importancia. Qué procedimientos utilizas para las salvadas de información.
- ¿Qué virus han afectado tu institución, que efectos ha provocado en tu computadora?
- ¿Cuál es el rol de los directivos, funcionarios, maestros y profesores, secretarías, oficinistas ante un incidente de Seguridad Informática en el centro?
- ¿Cuáles son a su juicio, las medidas que se deben tomar en una computadora para el uso de dispositivos externos?
- ¿Cómo está conformada tu clave de acceso, total de dígitos, de ellos cuantos números, cuántas letras y cuántos caracteres especiales?
- ¿Qué establecen las bases legales de la Seguridad Informática en Cuba, sobre tu responsabilidad personal, como cuadro de dirección y como usuario de estos recursos, referente a las copias de respaldo y control de usuarios y acceso a las TI de tu institución. Cómo lo harías.

Evaluación

Se realizará de forma individual, de acuerdo a los niveles de progreso.

¿Qué importancia le concede a la Seguridad Informática en el proceso de enseñanza aprendizaje desde el punto de vista educativo?

La evaluación de cada labor se hará grupal teniendo en cuenta los niveles de trabajo.

Para la evaluación de la actividad (todo lo que se realiza de ellas, como trabajo independiente) se tendrán en cuenta los siguientes aspectos:

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Grado de reflexión y coherencia del trabajo.

- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Exposición del trabajo.
- ✓ Fluidez al expresar las ideas.

Actividad No 8

Tema: Configuraciones en herramientas y aplicaciones para una mayor protección.

Título: Algunas configuraciones en herramientas y aplicaciones informáticas utilizadas más comúnmente en las instituciones del MINED.

Objetivo: Desarrollar actividades que permitan identificar las diferentes aplicaciones y herramientas más comunes utilizadas en el procesamiento de la información en las instituciones educativas, así como los procedimientos a emplear para lograr una configuración más segura de las mismas en su utilización.

Métodos: Conversatorios, debates y preguntas

Medios de enseñanza:

Fichero sobre las bases legales de la Seguridad Informática en Cuba

Presentación electrónica Seguridad y protección de la información.ppt

MANUAL DE SEGURIDAD DE USUARIOS.rtf

Presentación electrónica MODULO 3-Diapo 4.ppt

Principales Términos y Definiciones de Seguridad informática.doc

SEGURIDAD COMPUTACIONAL Rev2.pdf

Libro Electrónico v4.1

Quince consejos para navegar por internet.doc

LISTA DE RECOMENDACIONES PARA NAVEGAR POR INTERNET EN FORMA SEGURA.doc

Consejos para navegar de forma segura.doc

Cómo eliminar cookies.doc

Introducción: Muchos de los programas malignos utilizan vulnerabilidades asociadas a algunas aplicaciones que son de uso común en el trabajo con los medios informáticos, de ahí se hace necesario algunas configuraciones que ofrecen mayor seguridad al trabajo con las mismas.

Desarrollo. Comunicarles a los profesores el objetivo de la actividad a desarrollar, la importancia que tiene la misma no solo para evitar la contaminación, por algún virus de tipo macro, sino para impedir que otras

personas puedan acceder y modificar ficheros atentando contra la integridad de los mismos.

Abordar otros temas ya tratados con el respaldo de información, la forma de actuar ante la contaminación por programas malignos, los diferentes tipos de violaciones que se pueden cometer al trabajar con estos medios.

Con esta actividad podrán establecer algunas directivas que le posibilitará mantener la integridad de algunos documentos.

Para el desarrollo de la actividad se trabajarán las siguientes preguntas:

- ¿Cuáles son las principales aplicaciones con la que ustedes trabajan?
- ¿Podrían ser modificados estos ficheros por virus o por personas no autorizadas?
- ¿Qué acciones realizan para cumplir con el principio de la integridad de los mismos?
- ¿Qué se les ha informado acerca de este tema?
- ¿Cómo protegen un determinado documento?

Para el desarrollo de estas interrogantes, ejemplificarles con un documento dado, así como el nombre de algunos virus informáticos de tipo macro que hayan afectado ficheros.doc.

Evaluación

- Active en diferentes aplicaciones protecciones para evitar contaminación por virus de tipo macro, así como el establecimiento de contraseñas para la protección de los mismos. Estas evaluaciones serán totalmente prácticas y se medirán, la originalidad en cada uno y el cumplimiento de las normativas para el establecimiento de contraseñas.

Actividad No 9

Tema: Principales obstáculos asociados a la actividad cotidiana con los medios informáticos.

Título: Obstáculos asociados a la Seguridad Informática

Objetivo: Reconocer los principales obstáculos que atentan contra la Seguridad Informática, así como las amenazas, riesgos y vulnerabilidades expuestas los sistemas informáticos

Métodos: Conversatorios, debates y preguntas

Medios de enseñanza:

- Seguridad Informática (MSc .Alejandro Miguel Rodríguez Cuervo, UCP

Enrique José Varona.)

- Arquitectura y Seguridad Informática. (Ing. Lázaro Orlando Aneiro Rodríguez, Instituto Politécnico Eduardo García Delgado. 2001)
- Resolución Ministerial 127/2007 MIC
- Decreto Ley 199/1999 MININT
- Resolución Ministerial 188/2006 MTSS

Introducción: Muchos de los problemas que aparecen en los sistemas informáticos están dados por elementos que en ocasiones pasan desapercibidos ocasionando, inconformidades y hasta malestar a la hora de trabajar con la nueva tecnologías por lo que se hace necesario identificarlos y combatirlos para lograr un uso óptimo de estos medios.

Desarrollo. Comunicarles a los profesores el objetivo de la actividad, su importancia y vigencia en el contexto computacional actual, como de manera intencional o accidental se pueden cometer actos que representan conductas negativas; para ello presenta las siguientes interrogantes:

¿Qué elementos integran un sistema informático? Diga cuál es su objetivo.

¿Qué entienden por Seguridad Informática?

¿Cuáles son los principales objetivos de la Seguridad Informática?

Mencione los tres principios que deben cumplir los sistemas informáticos. Explique uno de ellos.

¿Qué entienden por obstáculos?

Continuar conversando sobre los elementos que impiden o dificultan los objetivos de la Seguridad Informática, los cuales llegan a convertirse en obstáculos entre los que se encuentran:

Para ustedes qué elementos pueden atentar contra la Seguridad Informática (Puntualizar en cada caso hasta llegar a resumir lo siguiente)

- Falta de conciencia de usuarios finales.
- Falta de presupuesto.
- Falta de apoyo de la dirección de la entidad.
- Falta de conocimiento.
- Pobre definición de responsabilidades.
- Falta de herramientas.

Explicarles que estos obstáculos pueden llegar a convertirse en amenazas: Recuerdan a qué se denominaba amenaza a la Seguridad Informática?

¿Cómo se podían clasificar estas?

Puntualizar:

Por su origen se clasifican en:

Accidentales.		Intencionales.	
Causas naturales	Causas laborales o sociales	Internas	Externas
Tormentas eléctricas, ciclones, etc.	Fallas de software.	Programas malignos.	
Inundaciones.	Fallas de hardware, de comunicaciones, del fluido eléctrico.	Robo de información.	
Incendios.	Destrucción de la información.	Modificación o destrucción de la información.	

Precisar las amenazas más comunes en los sistemas informáticos; así como las causas que lo podrían provocar:

1. Contaminación con programas malignos.
2. Destrucción o modificación del SO y las aplicaciones.
3. Robo de información.
4. Robo de tecnologías informáticas.
5. Acceso pirata a la red.
6. Accesos no autorizados.
7. Fallas del fluido eléctrico.
8. Fallas en las comunicaciones.
9. Fallas de hardware.
10. Tormentas eléctricas severas.
11. Incendios.

Causa que pueden provocar conductas de amenazas

- Impulsos mezquinos o codiciosos.
- Descontento por falta de reconocimiento al trabajo que realiza, condiciones inadecuadas o desacuerdo con las políticas de dirección.
- Desequilibrios psicológicos.

- Personal experimentado y ávido de hacer público y centrar atención sobre sus conocimientos.
- Existencia de profesionales de espionaje electrónico.
- Personal sin la calificación necesaria.

Evaluación

- Cree un documento Word, configúrelo para su mayor protección, haga un resumen desde su posición donde plasme los principales obstáculos que atentan contra la Seguridad Informática en su centro de trabajo.

Para la evaluación de la actividad se tendrán en cuenta los siguientes aspectos:

- ✓ Originalidad.
- ✓ Calidad del trabajo final.
- ✓ Actitud asumida en su realización.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.

Actividad No 10

Tema: Análisis de situaciones problemáticas donde se evidencien conductas que atentan contra la Seguridad Informática.

Título: Situaciones problemáticas.

Objetivo: Reconocer amenazas, vulnerabilidades y riesgos a los sistemas informáticos expresadas en diferentes situaciones problemáticas.

Proponer acciones que contribuyan a enfrentar estos elementos con el objetivo de minimizar los riesgos.

Métodos: Conversatorios, debates y preguntas

Medios de enseñanza:

- Seguridad Informática (MSc.Alejandro Miguel Rodríguez Cuervo, UCP Enrique José Varona.)
- Arquitectura y Seguridad Informática. (Ing.Lázaro Orlando Aneiro Rodríguez, Instituto Politécnico Eduardo García Delgado. 2001)
- Resolución Ministerial 127/2007 MIC
- Decreto Ley 199/1999 MININT
- Resolución Ministerial 188/2006 MTSS

Introducción: En muchas ocasiones se violan los principios y normas éticas a la hora de trabajar con los sistemas informáticos y para muchos se convierte en

algo normal, es por ello que se debe prestar la debida atención al trabajar con estos medios y así no incurrir de manera negativa en su uso.

Desarrollo. Comunicarles a los profesores el objetivo de la actividad, su importancia y concientización para lograr una cultura en Seguridad Informática en cada usuario que utilice estos medios; para ello presentan las siguientes situaciones problémicas:

A continuación se presentan dos situaciones que pueden ocurrir en cualquier centro con tecnologías informáticas conectados a una red:

Lee detenidamente las siguientes situaciones problémicas, una vez concluido

1. *Señale los elementos que considera obstáculos que atentan contra la S.I; así como los que constituyan amenazas, riesgos o vulnerabilidades en los sistemas informáticos.*
2. *En el caso de las amenazas, especifique como se clasifican por su origen y que causas motivaron a estas conductas de amenazas.*
3. *En cuanto a las vulnerabilidades que causas pudieron incidir.*
4. *Haga una valoración crítica al respecto y qué debe conocer usted y el resto de los usuarios de las TIC para no cometerlas. (POSITIVO Y NEGATIVO)*

Equipo 1

A continuación, le presentamos la secuencia de hechos ocurridos en una entidad (ficticia) de nuestro país donde se labora con la tecnología informática. En una Universidad de Ciencias Pedagógica, se crean “todas las condiciones” para la informatización del centro, se colocan computadoras de última generación en cada uno de los departamentos, así como en los laboratorios docentes tanto de profesores como de estudiantes, se prepara un local donde se sitúan servidores que permitirán brindar un grupo de servicios a través de la red, cada una de estas computadoras está compuesta por todos sus periféricos, así como de medios para el respaldo eléctrico.

Por la premura de la puesta en marcha de dicho proceso (informatización), se decide la contratación de personal para trabajar con los mismos sin una revisión profunda de sus referencias, tanto de los administradores de la red como de los técnicos de laboratorios, cada computadora permanece instalada con las aplicaciones que trajeron a modo de prueba sin colocarle los parches necesarios para su protección, pues según alegan los directivos, así lo exigía el

momento; al comenzar con los primeros trabajos de conectividad y de esta forma iniciar los servicios, los administradores le plantean al rector del centro que no tienen las condiciones indispensables para lograr una red segura pues los cables que permitirían dicho acceso no se encontraban protegidos, por lo que sugirieron la colocación de regletas o tubos plásticos para proteger los mismos, a lo que el rector respondió que no podían desviar esos recursos solo para proteger los cables de la red.

Por una solicitud de los profesores del departamento de informática comienzan a impartirse cursos para el trabajo adecuado con esta tecnología a cada uno de los usuarios del centro; Roberto es un profesor del departamento de Matemática quien alega que su contraseña para acceder a los servicios tanto del correo como de navegación es de conocimiento popular pues él no tiene nada que ocultar, por lo que no toma las medidas necesarias a la hora de logearse, e incluso su usuario y su contraseña lo tiene escrito en un papel de pegatina colocado en la primera gaveta de su buró.

En cuanto a los técnicos de laboratorio hay que señalar que estos solo controlan desde el punto de vista físico los medios que hay en su local, sin interesarse por controlar quién y qué tipo de información trabaja en estos. Los mismos no poseen ninguna aplicación que permita protegerlos de programa malignos y nadie a mostrado interés por ello.

Al poseer respaldo eléctrico (UPS) muchas de estas computadoras permanecen encendidas durante toda la semana, incluso conectadas a la red, pues dicen que así no pierden tiempo para comenzar a laborar y de esta forma protegen el disco duro. Muchos profesores han planteado esta situación a la dirección de la entidad pues le preocupan en gran medida el deterioro de estos medios pero aún no han recibido respuesta.

EJEMPLO 2 CASO “UN DÍA EN LA VIDA DE ALBERTO”

A continuación, le presentamos la secuencia de hechos ocurridos a Alberto durante una jornada en su escuela. Le solicitamos que lea con atención la cronología de los hechos y luego responda lo que aparece al final del texto.

Alberto es un estudiante de Politécnico de Informática, como estudiante aventajado en la Informática, forma parte de un grupo de desarrollo de proyectos. Hace mucho tiempo que le han asignado una PC con acceso a Internet y un buzón de correo electrónico para recibir y enviar información y le

sirva como ayuda en la búsqueda e intercambio de información sobre el proyecto que desarrolla. Está muy habituado a manejar este recurso porque lo considera una herramienta fundamental para cumplir en tiempo y forma con el cronograma de trabajo del proyecto. Por lo tanto, lo que le sucede en el día que relatamos está dentro de las posibilidades de un día normal en la vida de Alberto.

Un lunes de diciembre de 2008, Alberto llega al laboratorio de informática como todos los días, dispuesto a cumplir con su deber. Lo que sigue es la transcripción de sus pensamientos y de su actuación a partir de su llegada.

07:30

Alberto entra a al laboratorio y realiza las rutinas habituales, se sienta en su puesto de trabajo y mantiene un diálogo interior y callado consigo mismo, mientras empieza a operar la PC.

“Pone los libros sobre la mesa y prende la máquina. Piensa internamente..... hoy es mi día de suerte.....Avanzaré más de un 70% en el proyecto.... Pulsa “Enter”

“Ingrese su Clave”, le responde la máquina.

En fin.....a ver..... *****

¿Qué estará haciendo Roberto ahora? Debe estar en otro laboratorio... Se llevó ayer mi flash? Sí, creo que la puso en la mochila que está en aquella mesa.....

Bueno mientras bajan los correos voy a buscar la flash o localizar a Roberto...

07:52

¡Cuánta publicidad que viene por correo Roberto, ¡mira, mira!

Ahh... un mail de Ricardo, mi primo, que atorrante, hacía mucho que no me escribía...

De: Ricardo Tuprimo

Fecha: Domingo 10 de diciembre 2008 05:36 AM

Para: Alberto

Asunto: Fotos Impresionantes !!! Adjunto: photo.exe

Te mando estas fotos que encontré en Internet, son impresionantes !!!

Míralas, no las vas a poder creer !!!

No es virus!!!

Saludos

¡Qué tipo!, siempre me manda chistes y cosas graciosas... a ver...

09:57

Comienza para Alberto la evolución de un día agitado, a partir de una llamada desde la puerta del laboratorio de un profesor.

Alberto: Buenos días profesor...

Profesor: Buen día, el Director de la escuela está en estos momentos en una reunión, llamó por teléfono y solicita con urgencia la presentación electrónica sobre la escuela, que viene una visita y debe ser presentada.

Alberto: Ehhhh... lo que pasa es que esa presentación la tiene Carlos, y hoy no viene...

Profesor: Escúcheme, yo no tengo problemas, le digo al Director que Uds. no me dieron la presentación....

Alberto: Entiéndame, lo que pasa es que...

Profesor: Hace falta resolver y antes de que llegue el Director y la visita debemos tener la presentación.....

Alberto: profesor resolveremos el problema, haré otra presentación y trataré de recordar la información que ubicamos en.....

Profesor: Mira, Alberto, si yo no le llevo esa presentación al Director cuando el llegue te aseguro que habrá problemas...

Alberto: yo voy a hacer todo lo posible para hacerla....lo que necesito son los datos... ¿a dónde se lo llevo cuando termine?

Profesor: Mándemelo por mail..... anota paezumpierrez15@hotmail.com

Alberto: Bueno, en cuanto la tenga se lo envío... no se preocupe...

Profesor: Eso espero, eso espero... adiós...

Ufff... ¡Qué día! ¡Y justo Carlos no viene hoy!

Dispuesto a colaborar con el Profesor, Alberto busca la ayuda de su compañero, Antonio

Alberto: Antonio, ¿no sabes la clave de la máquina en que trabaja Carlos?

Antonio: Uhmhhh, prueba con "1234..."

Alberto: A ver... No Antonio, no es ésa...

Antonio: Ehhhh... prueba "qwerty"...

Alberto: No, no... Tampoco... Qué mala suerte...

Antonio: ¿Qué necesitas?

Alberto: Nada, un documento y una presentación electrónica que tiene Carlos en su máquina y como hoy no viene...

Antonio: Fíjate si no está en la de Sara, que siempre tiene copia de lo que hace Carlos.....

Alberto: ¿Y sabes la clave? (¡Para qué le pondrán tanta clave!)

Antonio: Creo que es “1111”...

Alberto: Ufff... Si, ¡es ésa! Grande, Antonio... eres un bárbaro....tiene todo hasta la presentación electrónica de la escuela que hizo Carlos...

De: Alberto

Fecha: Lunes 11 de diciembre de 2008 10:07 AM

Para: paezumpierrez@hotmail.com

Asunto: Copia de presentación Adjunto: presentación.doc

Profesor

Le envío, tal como lo solicitara, copia de la presentación electrónica sobre la escuela, trabajo realizado por Carlos.

Atentamente.

Alberto

Listo, ¡¡¡¡¡menos mal!!!

El profesor me lo va a agradecer...!!!!

EJEMPLO 3 CASO: “UN DÍA EN LA VIDA DE ROBERTO”

A continuación, le presentamos la secuencia de hechos ocurridos a Roberto durante una jornada laboral. Le solicitamos que lea con atención la cronología y luego responda lo que aparece al final del texto.

Roberto es un profesor de una institución educativa. Por los resultados de sus trabajos de investigación en la educación tiene asignada una PC con acceso a Internet y un buzón de correo electrónico institucional para recibir y enviar información.

Está muy habituado en enviar y recibir manejarse para sus propios trabajos de investigación, ha desarrollado confianza en el uso de este medio y permanentemente lo utiliza para realizar contacto con entidades y otros organismos relacionados con su trabajo de investigación.

En sus ratos libres, utiliza el servicio de Internet para actividades relacionadas con sus estudios y para comunicarse con amigos, quienes muchas veces le hacen llegar noticias, ofertas y páginas con diverso contenido de ocio, diversión, información de artistas, y él envía correos de felicitaciones o anuncios, fotos a varios destinatarios muy allegados simultáneamente.

El Administrador de la red tiene conocimiento acerca de estas “actividades personales” de Roberto, pues las mismas quedan registradas en el log de actividades navegación de cada trabajador con autorización ha estos servicios, pero como se trata de un amigo, que privilegia su trabajo por sobre todo, no informa acerca de las actividades personales de Roberto.

Por lo tanto, la información que recibió ese día a través de la cuenta institucional de correo electrónico y los hechos que se desarrollaron, están dentro de las posibilidades de un día normal en la vida de Roberto.

Un viernes, Roberto llega a su oficina como todos los días, dispuesto a cumplir con su deber pero recordando en que es el último día de la semana laboral y su pensamiento puesto en lo prometedor del fin de semana.

Sólo ruega que el tiempo lo ayude.

Con esa idea en mente, se sirve un café, intercambia bromas con sus compañeros de trabajo acerca de los partidos de pelota del próximo domingo, prende su PC, cumple con el protocolo de identificación y autenticación mientras empieza a saborear el café, se conecta a la intranet local y va directamente a su buzón de cuenta de correo electrónico.

En su oído, escucha las conversaciones cruzadas de sus compañeros de trabajo. Lo que sigue es la transcripción de sus pensamientos y de su actuación a partir de ese momento.

09:40

En la “casilla de entrada” de su cuenta de correo electrónico hay una lista de 20 mensajes nuevos.

Inmediatamente identifica a 15 de ellos como relacionados a su trabajo diario. Son mensajes sobre los cuales deberá trabajar y desarrollar acciones. Con cada uno de ellos, deberá aplicar conocimientos, comunicarse internamente y tomar acción. Cada uno de ellos consumirá entre 5 y 15 minutos de su tiempo.

“¡¡Ufa, cuánto trabajo, reflexiona con un poco de malhumor..... .ni siquiera aflojan un viernes! ¡Es más, parece que esperaran el viernes para hacer todo lo que no hicieron en la semana! Y con ese humor y esos pensamientos, decide que, ya que va a emplear en el tratamiento de los mismos casi todo el resto de su día laboral, bien vale la pena dedicar la primera media hora de la mañana a responder cuatro correos que le enviaron sus amigos y otro que parece ser de una institución de investigación que él utiliza para hacer consultas

Decide empezar con los correos de sus amigos.....

09:45

Mientras saborea el café, abre uno por uno los correos que le remitieron sus amigos y los contesta. Nada especial: preguntas acerca de exámenes, resultados de juegos de pelota y coordinación de una reunión de viernes en la noche. Todo esto le llevó quince minutos y decide “abrir” y ver de qué se trata el último mensaje antes de dedicarse por entero a los laborales.

Todavía perdura en su ánimo el malhumor que le produjo encontrarse con “semejante promesa de carga laboral”. Mira su reloj y piensa en el tiempo que deberá dedicarle a estos correos y su malhumor aumenta.....

Es increíble el tiempo que deberá dedicarle a estos correos!, reflexiona. ¡Y además hay que agregarle lo que se le pueda ocurrir a mi jefe, las llamadas por teléfono que deberá contestar y vaya a saber que otra cosa que se les pueda imaginar ¡!! ¡¡¡Y encima se interrumpe el fluido eléctrico por unos 40 minutos!!! Ya decididamente malhumorado, se dispone a leer el último mensaje del día.... piensa.... ”Vamos a ver qué me ofrece ahora esta correo no sea que me complique el resto del día.....

12.00

Abre el último correo y se encuentra con el siguiente mensaje:

Fecha: Mon, 06 Apr 2009 02:34:58 -1200 [06/04/09 10:34:58 CDT]
De: ["RIMED.CU WEBMAIL TEAM" <WEBMAILTEAM@YMAIL.COM>](mailto:WEBMAILTEAM@YMAIL.COM)
Para: robertoinves@rimed.cu
Asunto: Gracias por utilizar RIMED.CU Webmail
Cabeceras: [Mostrar todas las cabeceras](#)

Estimado usuario de RIMED.CU Dueño de la cuenta, robertoinves@rimed.cu

Este mensaje es de la web los usuarios RIMED.CU centro de mensajes para todos los propietarios de cuentas de Webmail .RIMED.CU En estos momentos la actualización ourweb / base de datos y la de llevar a cabo el mantenimiento

de todas nuestras cuentas de correo electrónico con el fin de reducir la tasa de los mensajes de spam. Estamos también en la supresión de todos correos y cuenta no utilizados en Webmail RIMED.CU para crear más espacio para las cuentas nuevas.

Para evitar que su cuenta sea cerrada innecesariamente, tendrá que contactar con nosotros con la siguiente información, para saber y ratificar sus datos sobre su cuenta de correo y facilitar la operación de mantenimiento.

CONFIRMAR SU EMAIL DEBAJO DE IDENTIDAD

1.Full Dirección de correo electrónico:::

2.password:::

3.age/country:::

4.date de nacimiento:::

5.First Nombre / Apellido:::

Código de aviso: VX2G99AAJ

Advertencia a! Titular de la cuenta que se niega a actualizar su accountwithin en el día de hoy, advertencia perderá su cuenta inmediatamente.

Código de aviso: VX2G99AAJ

Gracias por utilizar RIMED.CU Webmail!

Gracias RIMED.CU equipo web

Al leer el mensaje, lo primero que le viene a la cabeza fue “ ¡¡Lo único que me faltaba en el día de hoy es que me quiten el servicio de correo, sino confirmo toda esta información, donde hay palabras que no entiendo!! “ Enojado, su primera reacción fue la de borrar el mensaje, e ir donde el administrador de la Red y averiguar lo que pasaba, pero dudó un instante y reflexionó “ ¡Esta gente está peor que yo!. Con todo eso de la red, la luz que se fue e Internet no funciona, deben estar como aturdidos...

2.05

Ya cambiada totalmente su actitud y decidido a colaborar, movió el mouse hacia el botón “Responder” sobre el cual cliqueó e inmediatamente se le desplegó una pantalla con texto en inglés, en la cual se le agradecía su colaboración y se le pedían una serie de datos personales, que fue llenando rápidamente.

Mientras hacía esto, su mente ya se había enfocado en los correos laborales que lo estaban esperando.

Decidió colaborar y escribió sus datos personales, su cuenta y contraseña...., que fue lo que pudo entender del cuestionario que le enviaron para la respuesta

“¡Podrían haberse tomado el trabajo de traducir todo al español!”, se dijo a si mismo.... Ya reducido su malhumor por el efecto de la acción que hacia para que no le cancelaran su correo, se dispuso a abrir el primer mensaje laboral.....

Evaluación:

Las actividades propuestas se revisarán por equipos

Aspectos a tener en cuenta para la evaluación de la actividad.

- ✓ Análisis realizado al responder cada una de las preguntas.
- ✓ Si todas fueron contestadas.
- ✓ Originalidad de las respuestas.
- ✓ Actitud asumida en su realización.
- ✓ Grado de reflexión y coherencia del trabajo.
- ✓ Utilización adecuada de todos los recursos disponibles.
- ✓ Exposición del trabajo.
- ✓ Fluidez al expresarlas ideas.

Conclusión:

Al finalizar la actividad los profesores podrán expresarse sobre las principales violaciones que se cometen al trabajar con las tecnología informáticas y como muchas de estas pasan desapercibidas ante los diferentes usuarios y directivos de entidades, así como propondrán un grupo de medidas para contrarrestar tales efecto.

Se propiciará el debate para analizar la efectividad de las actividades desarrolladas.