ACTIVIDADES EDUCATIVAS PARA CULTURA DE SEGURIDAD INFORMÁTICA, EN POSTGRADO SOBRE PÁGINAS WEB.

MSc. Luis De La Rosa Vaillant[1]. MSc. Beatriz Felicia Menéndez Pérez[2].

1-. Universidad de Matanzas – Centro Universitario Municipal Jagüey Grande, Calle 54 #904 e/ 9 y 11 Jagüey Grande, Matanzas. luis.delarosa@umcc.cu

2-. *Universidad de Matanzas – Centro Universitario Municipal Jagüey Grande, Calle 54 #904 e/ 9 y 11 Jagüey Grande, Matanzas.*

CD de Monografías 2016

ISBN: XXX-XXX-XX-XXXX-X

Resumen

El trabajo tiene como objetivo: elaborar un sistema de actividades educativas para la cultura de la seguridad informática en postgrado Páginas Web del área Informática-Educación Laboral. Este fortalece los conocimientos que poseen en relación con las tecnologías de la información y las comunicaciones, teniendo en cuenta los esfuerzos del Estado Cubano por alcanzar la informatización de la sociedad, además integra los fundamentos teóricos, pedagógicos, psicológicos, prácticos así como las actividades a desarrollar. La propuesta responde a los criterios más actualizados de las ciencias pedagógicas contemporánea, situando a los estudiantes en un lugar priorizado en su desempeño cognitivo. Se aplicó como método general del conocimiento, el dialéctico materialista, así como diversos métodos de nivel teórico y del nivel empírico. La investigación está estructurada en introducción, desarrollo, conclusiones y la bibliografía. El trabajo ha constatado la necesidad de apoyar el desarrollo de una cultura general para la seguridad informática.

Palabras claves*: Seguridad;, Cultura; Informática; Sistema.*

Introducción

La Seguridad Informática ha sido un aspecto prioritario dentro de la Informática, ya que desde el surgimiento de las primeras computadoras y el software a utilizar en las mismas, ha existido dificultad debido a la falta de información, negligencia e indisciplina de algunas personas. No existían los avances en las tecnologías de comunicación y las redes informáticas como en la actualidad, que permitiera una mejor preparación y adquisición de conocimientos para no cometer fallos ni destrucciones por desconocimiento y falta de autopreparación en el manejo del *software* y *hardware*. Un por ciento menor corresponde a incidentes realizados por grupos autorizados, otro por ciento aún menor son delitos y la punta de la pirámide corresponde a casos de espionaje industrial, económico o militar (Aneiro, 1999).

Las causas y fenómenos relacionadas con la seguridad informática que dieron origen a la presente investigación en el municipio de Jagüey Grande fueron: la no aplicación de las medidas de protección por parte de los estudiantes para interactuar con las computadoras y los sistemas informáticos, no actuar correctamente en caso de inclemencia del tiempo, fuego, caída de tensión, calor, interferencias electromagnéticas, no tener en cuenta las medidas de protección lógicas, desconocimiento de las regulaciones globales de protección y poca cultura en el cuidado y conservación de los medios. Todo ello conllevó a que se incrementaran los problemas de seguridad informática. Por todas estas causas, los autores del trabajo se proponen buscar métodos y vías para lograr en los estudiantes del postgrado de Páginas *Web* correspondiente al área Informática-Educación Laboral una adecuada conducta durante la manipulación de la información y los medios, además, proteger y tomar todas las medidas necesarias para mantenerla segura, fuera de riesgos y de amenazas. Por lo que se tiene como objetivo: elaborar actividades educativas para elevar la cultura de la

ISBN: XXX-XXX-XX-XXXX-X

seguridad informática en estudiantes de postgrado sobre Páginas *Web* correspondiente al área Informática-Educación Laboral en el municipio Jagüey Grande.

Desarrollo

Los virus informáticos y otros programas malignos comenzaron a golpear a Cuba a finales de los años 80 y sobre todo a principio de los 90. Esos programas llegaban por diferentes vías y afectaban máquinas y sistemas. "Me recuerdo como una persona, mirando una curiosa pelotita, que como bola de ping-pong se desplazaba a través de la pantalla en la máquina en que estaba trabajando, borrando las letras que encontraba a su paso, en un sistema *DOS* (*Disk Opereting System*)". Fue el primer programa maligno cuya acción sufrí, ya que en un determinado momento la pelotita cesaba su accionar y se borraba el trabajo que se estaba ejecutando. Era el segundo virus reportado en Cuba, llamado oficialmente *ITALIAN* (alias *BOUNCING BALL*), ya que el primero fue el *VIENNA*, que en marzo de 1988 demostró la vulnerabilidad de los sistemas cubanos[1]. Surgió entonces en el país la necesidad de enfrentar un nuevo reto en la informática: el logro de la seguridad y protección de los recursos informativos. Se promulgan algunos textos legales que ofrecen un apoyo a este nuevo objetivo. Entre estos aparece el Reglamento de Seguridad Informática, emitido por el Ministerio del Interior en 1996, el cual estipula que todos los ministerios y organismos centrales de la administración central del estado, así como empresas y otras instituciones, deben analizar, confeccionar y aplicar planes de seguridad informática y de contingencia, para reducir el riesgo de afectaciones a los recursos informativos, por la acción de catástrofes naturales o artificiales, de fraudes, de errores humanos, de los propios programas malignos o de otra naturaleza (Bidot, 1992).
Plan de seguridad informática**:** Se instituyen como una exigencia para todas las entidades, en el cual deben reflejar las políticas, estructura de gestión y el sistema de medidas, para la Seguridad Informática, teniendo en cuenta los resultados obtenidos en los análisis de riesgo y vulnerabilidad realizados. Constituye un documento básico para lograr la confidencialidad, integridad y disponibilidad de la información y la protección de los medios y locales donde se utilice la técnica de computación (Bidot, 1992).

La cultura de la seguridad informática necesita de la adquisición de una conciencia de los estudiantes del postgrado de Páginas *Web* correspondiente al área Informática-Educación Laboral del municipio Jagüey Grande, con la intención de salvaguardar la información evitando amenazas pasivas y activas, en algunos casos realizadas por delincuentes informáticos, ello requiere de la modificación de sus comportamientos pudiendo lograrse mediante la formación técnica para que manifiesten actuaciones responsables.
Información: en sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno (Wikipedia, 2010).

Por lo que es de vital importancia al crear un modelo ético y de acceso a la información, tener en cuenta: respetar el derecho de acceso a la información y el derecho a la privacidad,

ISBN: XXX-XXX-XX-XXXX-X

desarrollando estrategias para proteger la intimidad de los individuos y organizaciones; respetar los derechos de autor sin distinción de tipo de soporte o medio de transmisión de la información; establecer los límites de acceso a la información personal; promover la creación de entidades que regulen y controlen la transmisión y formar y capacitar en los diferentes niveles educativos, sobre conceptos básicos del proceso de la gestión

Actualidad de la Seguridad Informática.

En los últimos años todo lo relacionado con la seguridad informática suscita un gran interés. Las empresas y particulares están más sensibilizados de los riesgos que conlleva su actividad electrónica. Esto es un hecho. También lo es que el desconocimiento general sobre estos temas todavía es demasiado grande.
Cada día se publican decenas de nuevos fallos en el *software* que utilizamos habitualmente. Hay cientos de sitios en Internet que ofrecen información, herramientas y métodos para vulnerar sistemas informáticos. Cada mes se publican nuevos libros con información sobre seguridad. Somos decenas de miles las personas que nos dedicamos en todo el mundo a la seguridad informática. Muchos lo hacemos porque es nuestra profesión y aplicamos estrictas normas éticas a nuestro trabajo. Pero otros están en el "lado oscuro" y tienen intenciones menos amigables.
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 (Wikipedia, 2010).

Sistema de actividades educativas para elevar la cultura de la Seguridad Informática en los estudiantes del postgrado de Páginas *Web* correspondiente al área Informática-Educación Laboral del municipio Jagüey Grande.

Los autores consideran que el sistema de actividades educativas propuesto es un conjunto de situaciones de aprendizaje para dar tratamiento a la cultura de la Seguridad Informática con carácter flexible, personalizado, protagónico, coherente y con estilo adecuado de comunicación, que contribuyen a una preparación más integral de los estudiantes.

C. Álvarez de Zayas uno de los autores que más énfasis hace en la necesidad del uso del enfoque sistémico propone la definición siguiente: Entiéndase por sistema al conjunto de componentes de objetos que se encuentran separados del medio e interrelacionados fuertemente entre ellos, cuyo funcionamiento está dirigido al logro de determinados objetivos, que posibilita resolver una situación problémica (Alvarez, 1999).

En correspondencia con lo anterior, los autores consideran que el sistema de actividades que se ajusta a las necesidades de la presente investigación es el dado por Luis Ernesto Martínez González, "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 (Martínez, 2007).

ISBN: XXX-XXX-XX-XXXX-X

Para la organización de las actividades se utiliza la siguiente estructura:

- Objetivo general.
- Requisitos generales para su implementación y funcionamiento.
- Contenido de las actividades:
  - Título de la actividad.
  - Objetivo específico.
  - Habilidades.
  - Acciones y procedimientos.
  - Evaluación y control.
  - Bibliografía.
  - Recomendaciones.

Actividad 1.

Título: Las máquinas computadoras y la seguridad informática.

Tipo de actividad: Diagnóstico (A tener en cuenta por el profesor).

Objetivos: Al finalizar la actividad los estudiantes del postgrado deben ser capaces de:

- Interpretar las definiciones correspondientes a Seguridad Informática.
- Expresar la importancia de la Seguridad Informática para una institución y las personas.
- Reconocer los elementos que definen una adecuada seguridad Informática.

Habilidades:

- Empleo y búsqueda en enciclopedias.
- Resumir.
- Definir.
- Explicar y Argumentar.

Orientaciones didácticas: Para diagnosticar los conocimientos de la Seguridad Informática, se sugiere que en la primera comparecencia al Laboratorio de Informática desarrollen las siguientes actividades:

1. Redacta un párrafo donde expreses lo que significa para ti la seguridad informática.

ISBN: XXX-XXX-XX-XXXX-X

2. ¿Qué importancia le reporta la Seguridad Informática a una institución o persona? ¿Por qué?

3. ¿Cómo se implementa la seguridad Informática? Argumente.

Evaluación y control: Se recoge el informe escrito, se califica según las reglamentaciones vigentes, se controla en el registro y posteriormente se debate en el colectivo o grupo.

Recomendaciones:

- Orientar bibliografía complementaria, incluyendo intranet.

- Recordar que el debate de los trabajos debe ser crítico y autocrítico, además, debe potenciar valores como la honestidad, laboriosidad y responsabilidad.

Bibliografía: Libro de texto Elementos de Arquitectura y Seguridad Informática. Páginas: (216 y 217) y Plan de Seguridad Informática de muestra de un centro X.

Actividad 2.

Título: Medidas de seguridad físicas y lógicas a tomar.

Tipo de actividad: Grupal (Exposición de ideas por equipos).

Objetivos: Al concluir la actividad los estudiantes del postgrado deben ser capaces de:

- Reconocer las medidas de seguridad físicas y lógicas a tomar en caso de amenazas informáticas.

- Identificar la actitud a tomar para que todas las personas que trabajan con computadoras conozcan las medidas físicas y lógicas en caso de presentarse amenazas informáticas.

- Identificar las ventajas que le traería para él y para el equipamiento que conozcan estas medidas físicas y lógicas.

Habilidades:

- Empleo y búsqueda en enciclopedias informáticas y libros electrónicos.

- Identificar.

- Explicar y Argumentar.

- Navegar en intranet.

ISBN: XXX-XXX-XX-XXXX-X

Orientaciones didácticas: Si usted estuviera a cargo de un laboratorio de informática y tuviera la responsabilidad de la elaboración de las medidas generales para la protección del equipamiento del que dispone:

a) ¿Cuáles serían las medidas físicas y lógicas a tomar?

b) ¿Qué usted haría para que el personal que acude a trabajar en el laboratorio las conozca?

c) ¿Qué ventajas le traería a usted y al equipamiento, que el personal que acude a trabajar al laboratorio conozca las medidas de seguridad?

d) En caso que ocurra una incidencia ¿qué haría? ¿Cómo darle solución a dicha situación?

Evaluación y Control: Se revisa y evalúa la actividad de forma oral, intercambiando ideas con los estudiantes del postgrado.

Recomendaciones: El debate de la actividad debe ser crítico y autocrítico, se debe potenciar valores como la honestidad, laboriosidad y responsabilidad.

Bibliografía: Reglamento del laboratorio de informática, en *Intranet* la página: http//www.segurmática.cu. Plan de Seguridad Informática del centro, Libro electrónico "Elementos de Arquitectura y Seguridad Informática", páginas: 216 y 217.

Actividad 3.

Título: Mal hábito de violar las medidas de seguridad físicas y lógicas.

Tipo de actividad: Investigativa (estudio de caso)

Objetivos: Al concluir la actividad los estudiantes del postgrado deben ser capaces de:

- Identificar las acciones ilícitas que se cometieron.
- Mencionar las medidas a tener en cuenta para que no sucedan estas violaciones.
- Explicar las medidas a tomar con los que cometan este delito.
- Valorar la importancia de las medidas de seguridad físicas y lógicas en las instituciones.

Habilidades:

- Identificar.
- Mencionar.

ISBN: XXX-XXX-XX-XXXX-X

- Explicar.
- Valorar.
- Analizar.
- Lectura y estudio del documento "Reglamento de los laboratorios de Informática", lectura.
- Análisis del Plan de seguridad del centro.

Orientaciones didácticas: En esta actividad se utilizará la técnica Estudio de casos con el objetivo de llegar a conclusiones o formular alternativas sobre una situación que se presentó en el Instituto Politécnico de Informática, sucedió así:

Se encuentran dos estudiantes de 3er año: Estudiante A y Estudiante B en el laboratorio 1 del IPI, en el horario de tiempo de máquina. El estudiante A se acerca al estudiante B y le comenta que el trajo un programa de su casa que permite saber la contraseña que le asignó el usuario que trabaja con la PC, el estudiante B le dice que se lo dé y le enseñe a trabajar con él, así guardo cosas que no puedo tener: videos, música, fotos, películas en otras computadoras y cuando vengan a revisar mi usuario lo tengo limpio.

Estudiante A le dice que él se lo va a dar pero que su idea es entrar a la máquina donde trabaja la profesora de programación y ver la prueba de mañana y como sé que tú estás insuficiente pensé que te interesaría. El estudiante B le contestó con alegría que por supuesto, entre los dos realizarán la acción ilícita. La profesora se percató que estaban conectados por la red a su PC y que estaban husmeando en sus cosas y detectó, además, que habían leído la prueba.

Después de leída la situación anterior, el profesor presentará un cuestionario de preguntas para que los estudiantes del postgrado reflexionen, interpreten y lleguen a resolver el caso.

Preguntas.

- ¿Crees que fue correcta la actitud de los estudiantes? ¿Por qué?
- ¿Qué acciones indebidas realizaron? Menciónelas.
- ¿Violaron el Plan de Seguridad Informática del centro? Explique.
- ¿Qué medidas se deben tomar con estos estudiantes?
- ¿Qué medidas debe tomar la escuela para que hechos como estos no se repitan?

ISBN: XXX-XXX-XX-XXXX-X

- ¿Qué medidas debe tomar el Departamento de Asistencia Técnica conjuntamente con el nodo para que no ocurran hechos significativos?

- ¿Qué importancia tiene para ti hacer cumplir con rigurosidad las medidas de seguridad físicas y lógicas en los laboratorios de informática?

Mientras los estudiantes del postgrado dan sus opiniones, el profesor va anotando aportes significativos y posibles soluciones que surjan de la discusión. Una vez concluido el debate, se realiza una síntesis anotando las ideas y las soluciones sugeridas, analizando su claridad.

Al final de la actividad se llega a elegir las soluciones o conclusiones que el grupo crea correcto y luego se reflexiona acerca de la relación de este caso y esta solución, con la vida real de los participantes.

Evaluación y Control: El profesor revisa y evalúa la actividad de forma oral intercambiando ideas con los estudiantes del postgrado, observando su expresión oral y rectificado en caso de alguna dificultad, se controla en registro de evaluaciones.

Recomendaciones: Durante el desarrollo de toda la actividad se debe lograr un debate crítico y autocrítico, crear un clima de seguridad y confianza, potenciar valores como la honestidad, laboriosidad y responsabilidad.

Bibliografía: Documento digital "Reglamento interno de los laboratorios de computación". "Plan de Seguridad Informática" del centro.

Actividad 4.

Título: Aseguramiento de una *red* de computadoras.

Tipo de actividad: Investigativa.

Objetivos: Al finalizar la realización de la actividad los estudiantes del postgrado deben ser capaces de:

- Explicar cómo asegurar una red de computadoras.

- Exponer elementos a tener en cuenta a la hora de asegurar una *red* de computadoras.

- Interpretar la definición correspondiente a: aseguramiento de una *red* de computadoras.

- Valoración de su accionar como administrador de *red* en caso de serlo algún día.

Habilidades:

- Empleo y búsqueda en libro electrónico.

ISBN: XXX-XXX-XX-XXXX-X

- Identificar.
- Explicar.
- Exponer.
- Valorar.
- Interpretar.
- Extraer la idea esencial de lo que investigue o estudie…

Orientaciones didácticas: Consulte en la biblioteca del centro y en el libro digital "Elementos de Arquitectura y seguridad informática" en la página 221 el subtítulo Redes de ordenadores y resuma en tres párrafos:

a) Los elementos a tener en cuenta para asegurar una *red* de computadoras tanto el *software* como en el *hardware*.

b) ¿Por qué es necesario mantener asegurada la *red* de computadoras con que se trabaja?

c) Si fueras administrador *red* en una empresa o centro que utilice este servicio. ¿Qué harías para asegurarla?

Evaluación y Control: Se recoge de forma escrita y se controla en el registro de evaluaciones y posteriormente se le da a conocer a los estudiantes los resultados, se hace una revisión oral.

Recomendaciones: Profundizar en lo relativo a la Seguridad Informática en la *red*.

Bibliografía: Plan de Seguridad Informática del centro, reglamento del laboratorio de informática, en *Intranet* las páginas: http//alerta-antivirus.red.es y http//www.segurmática. cu, Libro electrónico "Elementos de Arquitectura y Seguridad Informática" páginas: 221 y 222, documento de *Word* titulado: seguridad Informática - Desastres informáticos**.**

Actividad 5.

Título: Los programas malignos, una amenaza informática constante.

Tipo de actividad: Evaluativa (selección múltiple).

Objetivos: Es necesario que los estudiantes del postgrado al concluir el desarrollo de la actividad sean capaces de:

- Identificar los diferentes tipos de virus.

ISBN: XXX-XXX-XX-XXXX-X

- Describir la presencia de virus en las Computadoras.
- Describir la acción que realiza dicho virus en nuestro sistema.
- Caracterizar los daños más comunes ocasionados por los virus.
- Explicar las limitaciones que presenten los programas malignos para la propagación.

Habilidades:

- Identificar.
- Empleo del libro digital y el Plan de Seguridad del centro.
- Explicar.
- Navegar en *Intranet*.
- Caracterizar.
- Describir.

Orientaciones didácticas: Los virus informáticos son programas escritos por especialistas de computación, los cuales se reproducen a sí mismo, además ejecutan una acción o efecto secundario a los sistemas que infectan.

a) Marque con una X los tipos de virus que conozca:

1- ___gusanos.

2- ___*linux*

3- ___melisa

4- ___manzana

5- ___viernes 13

6- ___ *win 32*

7- ___autorum

8- ___bombas lógicas y de tiempo.

9- ___cabayo de troya

ISBN: XXX-XXX-XX-XXXX-X

b) ¿Cómo dirigen sus ataques los virus informáticos? Argumenta.

c) ¿Cómo puedes detectar la presencia de virus en tu sistema? Explique la estructura que lo conforman.

d) ¿Qué limitaciones presentan los programas destructores? Explíquelas.

Evaluación y Control: Se propicia un debate abarcador en un clima de confianza, donde se puede apreciar que los estudiantes del postgrado se sienten motivados, se seleccionan a varios de ellos para ir a la pizarra y revisar el inciso a, por último se controla en el registro de evaluación.

Recomendaciones: establecer en el debate la participación por equipos.

Bibliografía: Libro digital "Elementos de Arquitectura y Seguridad Informática" páginas: 227 a la 234, tabloide: Manual de Informática Básica página 29, la páginas en Intranet: http/www.segurmatica.cu; http// alerta-antivirus.red.es

Actividad 6.

Título: ¿Los antivirus son necesarios en una computadora?.

Tipo de actividad: Investigativa.

Objetivos: Los estudiantes del postgrado, al concluir la actividad deben ser capaces de:

- Explicar el funcionamiento de un antivirus.
- Exponer cómo actuar ante una infección.
- Argumentar sobre que antivirus escoger para mantener la seguridad en la PC.
- Instalar y actualizar un antivirus.

Habilidades:

- Empleo del libro digital y el tabloide: Manual de Informática Básica.
- Explicar.
- Búsqueda y navegación en las páginas de Intranet.
- Argumentar.
- Exponer.

ISBN: XXX-XXX-XX-XXXX-X

- Instalar y actualizar.

Orientaciones didácticas: Los antivirus son software creados para mantener una buena seguridad en las computadoras personales y contrarrestar a los virus informáticos.

Atendiendo a lo planteado anteriormente responde:

10- ¿Crees que puedas mantener una adecuada seguridad en tu computadora sin la necesidad de instalar un antivirus? Argumenta.

11- ¿Cómo funciona un antivirus? Explique.

12- ¿Qué antivirus elegir para mantener nuestras computadoras seguras? Argumenta.

13- Consulte la página http://www.segurmática.cu y desglose los pasos para instalar y actualizar un antivirus.

Evaluación y Control: Se recoge el informe escrito, se revisa y evalúa en el registro y luego se rectifica de forma oral, se realizan los pasos de la instalación y actualización del antivirus de forma práctica.

Recomendaciones: Buscar otras bibliografías referentes al tema y profundizar en la misma, en el debate deben ser críticos y autocríticos.

Bibliografía: Tabloide: Manual de Informática Básica V, página 30, página de Intranet: http://www.segurmática.cu, video de. Instalación.

Actividad 7.

Título: Seguridad Informática.

Tipo de actividad: Grupal (Interactiva).

Objetivos: Al concluir la actividad los estudiantes del postgrado deben:

- Completar el cruciletras relacionado con algunas de las palabras que necesitan conocer para que posean una adecuada seguridad informática de los equipos con que cuentan.
- Analizar y hacer corresponder cada letra en su casilla correspondiente para formar las palabras claves adecuadas.
- Utilizar una adecuada ortografía.

Habilidades:

ISBN: XXX-XXX-XX-XXXX-X

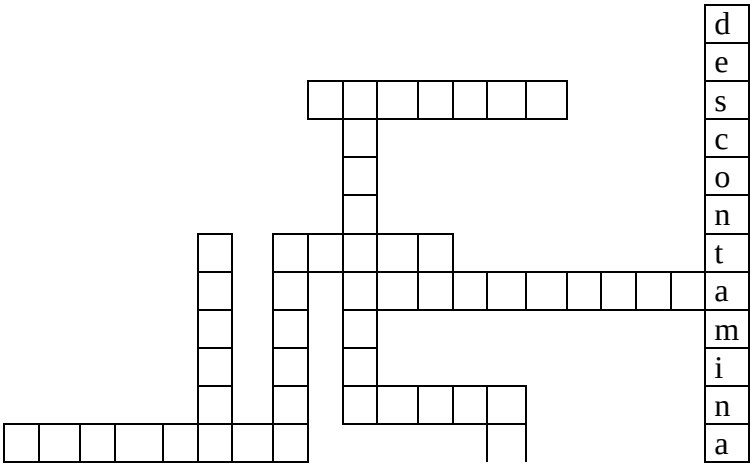
- Completar.
- Analizar.
- Identificar.
- Interpretar.
- Empleo y búsqueda en diccionario informático.

Orientaciones didácticas: Completa el cruciletras, encontrando todas aquellas palabras que te ayuden a tener una correcta seguridad informática.

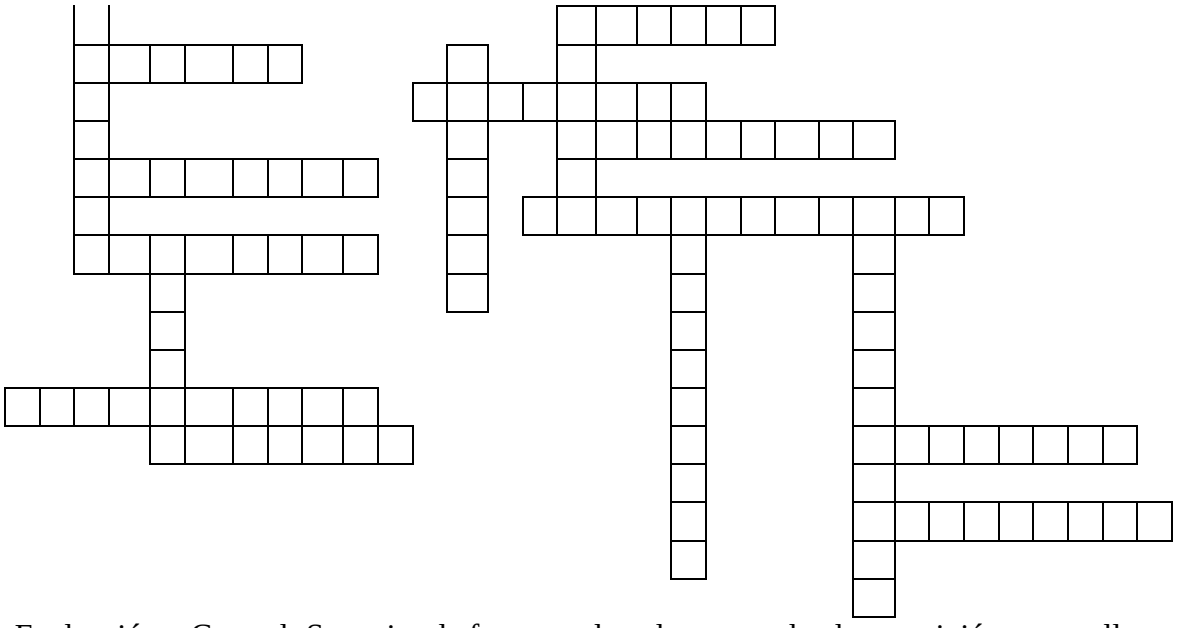
1. Usuario. 8. Política. 15. *Malware.* 22. Protección.
2. Seguridad. 9. Amenazas. 16. Física. 23. Infección.
3. Virus. 10. Informática. 17. Lógica. 24. Instalar.
4. Asegurar. 11. Daños. 18. Antivirus. 25. Enviar.
5. Vacuna. 12. *Software.* 19. Recuperación. 26. Recibir.
6. Programa. 13. *Hardware.* 20. Información. 27. Ocasionan.
7. Actualizar 14. Descontamina. 21. Alerta.

a) Busque el significado de estas palabras en el diccionario informático y redacte oraciones con ellas.

Cruciletras:



ISBN: XXX-XXX-XX-XXXX-X



Evaluación y Control: Se revisa de forma oral, cada uno va dando su opinión, entre ellos se rectifican junto al profesor, con disciplina y organización, al final se da a conocer la evaluación de cada uno y se controla en el registro.
Bibliografía: Diccionario Informático. Enciclopedia Encarta, Bohemia No.4, del 2009 en la antepenúltima hoja.
Recomendaciones: En el desarrollo de la actividad se debe potenciar valores como: la honestidad, laboriosidad y responsabilidad.

Actividad 8.

Título: El código de ética, documento importante para los centros donde se aplique la tecnología informática.
Tipo de actividad: Grupal (Interactiva).
Objetivos: Al concluir la actividad los estudiantes del postgrado deben ser capaces de:

- Definir código de ética.
- Identificar las partes que lo componen.
- Explicar la importancia del código de ética para una institución.
- Explicar la importancia que te reporta a ti el cumplimiento del código de ética.

Habilidades:

- Definir.
- Identificar.
- Explicar.
- Analizar.
- Lectura y análisis del código de ética de las instituciones.

- Navegar en las páginas de *Intranet*.

ISBN: XXX-XXX-XX-XXXX-X

Orientaciones didácticas: Existe una serie de *normas* resumidas en un *código* de *ética*, que están supervisadas por un colegio profesional. Muchos de esos *principios* pueden resumirse en los siguientes: guardar fidelidad a la institución o al jefe que suministra *el trabajo*; dirigirse a los colegas con *respeto* y consideración, evitando la *competencia* desleal; actualizarse con los conocimientos propios de su *disciplina*; guardar el secreto profesional; no sacar provecho de la superioridad del puesto para manipular o chantajear a otros.

1. Atendiendo a lo expuesto anteriormente, elabore un concepto de código de ética apoyándote en tu experiencia personal.

2. Marque con una X las partes que conforman el código de ética:

a) ___ datos personales y laborales.

b) ___ datos de confirmación.

c) ___ estructura organizativa.

d) ___ datos del servicio.

e) ___ datos de la seguridad informática.

f) ___ Compromisos para el uso de las tecnologías de la información.

3. ¿Qué importancia tú crees que le reporta el código de ética a una institución?

4. Explica la importancia que tiene para ti el cumplimiento del código de ética.

5. ¿Qué medidas se tomarían en caso que se viole el código de ética?

Evaluación y Control: se recoge el informe escrito y se evalúa. Después se divide el aula en 4 equipos y se evalúa oral, de forma tal que todos den su opinión, al concluir la actividad se le da a conocer la puntuación individual y por equipo. El mejor equipo se le otorga un reconocimiento. Se destaca al que más participó y se exhorta a los que participaron poco. Al finalizar, el facilitador pasa las notas al registro.

Recomendaciones: Durante el desarrollo de toda la actividad debe evaluar a los estudiantes del postgrado en su expresión oral y en la parte escrita la ortografía. Se debe lograr un debate crítico y autocrítico, crear un clima de seguridad y confianza, potenciar valores como la honestidad, laboriosidad y responsabilidad.

Bibliografía: Documentos digitales: Código de ética, pág., *Wikipedia* 2010.

ISBN: XXX-XXX-XX-XXXX-X

Conclusiones

Las actividades educativas diseñadas han contribuido a elevar la cultura de la seguridad informática en estudiantes de postgrado sobre Páginas Web correspondiente al área Informática-Educación Laboral en el municipio Jagüey Grande, al propiciar conocimientos y habilidades sobre estas tecnologías de la información y su protección.

Bibliografía

ALVAREZ, C. Didáctica: La Escuela en la Vida, La Habana: Ed. Pueblo y Educación, 1999. -- P16.

ANEIRO, L. O... Capítulo VIII: Seguridad Informática. Elementos de Arquitectura y Seguridad Informática. -- La Habana: Ed. Pueblo y Educación, 1999. -- 216-240 p 300

ARREGOITÍA, S. Protección contra los recursos informáticos en Cuba Revista Giga No 4.2008, La Habana, p.38-40

BIDOT, J. La protección contra los virus informáticos. Experiencia en Cuba. Revista CID. Electrónica y proceso de datos en Cuba No 27, -- La Habana.1992. -- p 37-41.

DEL PUERTO, R.. HARTMANN, F... Avanzando hacia la Sociedad de la Información. Artículo en la Revista GIGA, La Revista Cubana de Computación. Editada por Copextel, S.A número 1/ 2002

ENCICLOPEDIA DIGITAL LIBRE, WIKIPEDIA. Disponible en: http://es.wikipedia.org/wiki/Portal:Informa

MARTÍNEZ, L. E. El sistema de actividades como resultado científico en la maestría en Ciencias de la Educación: ¿ser o no ser?. Soporte Magnético, 2007, p 11.

PÉREZ, V.; DE LA CRUZ M. DEL P. La preparación del maestro para la inserción de la computación en la actividad docente; Instituto Superior Pedagógico para la Educación Técnica y Profesional, en soporte digital, s/a.

ROSABAL, H. "Tecnologías y curso escolar". En: punto cu. Mensuario de Informática y Comunicaciones, No 24, Ciudad de La Habana, Septiembre de 2004.

_____ ¿Cómo hacer más eficiente el aprendizaje?; Ediciones CEIDE, México, 2000.

_____ Enseñanza y aprendizaje desarrollador; Ediciones CEIDE, México, 2000.

ISBN: XXX-XXX-XX-XXXX-X

ZILVESTEIN, J.; SILVESTRE, M. Una didáctica para una enseñanza y un aprendizaje desarrollador. Habana. 2001 (soporte magnético).

ISBN: XXX-XXX-XX-XXXX-X