UNIVERSIDAD DE SANCTI SPÍRITUS "JOSÉ MARTÍ PÉREZ" FACULTAD CIENCIAS TÉCNICAS.

TRABAJO DE DIPLOMA EN OPCIÓN AL TÍTULO DE LICENCIADA EN EDUCACIÓN ESPECIALIDAD: EDUCACIÓN LABORAL-INFORMÁTICA.

La preparación de la seguridad informática.

Autora: Isadaris Morales Wright.

Curso: 2017.

UNIVERSIDAD DE SANCTI SPÍRITUS "JOSÉ MARTÍ PÉREZ" FACULTAD CIENCIAS TÉCNICAS.

TRABAJO DE DIPLOMA EN OPCIÓN AL TÍTULO DE LICENCIADA EN EDUCACIÓN ESPECIALIDAD: EDUCACIÓN LABORAL-INFORMÁTICA.

La preparación de la seguridad informática.

Autora: Isadaris Morales Wright.

Tutora: Lic. Lisbel Valdés Leal. MSc. Profesora instructora.

Curso: 2017.

Dedicatoria

A la Revolución que me ha permitido el derecho de ejercer mi carrera y a todas aquellas personas que han hecho lo posible por guiarme y ayudarme incondicionalmente. En especial a mi madre y mi padre que ha realizado todo el esfuerzo por inculcarme el amor a mi profesión.

A mi profesora y tutora MSc. Lisbel Valdés Leal por su incondicional apoyo, por tener la paciencia y dedicación para salir adelante en esta investigación.

A mis padres, mi hermano y mi tío José Alberto Wright Whesters por la ayuda e inmenso apoyo que me ha brindado en todos los sentidos de mi vida laboral y estudiantil al arribar a la Licenciatura.

A todos los que de una forma u otra hicieron posible la culminación de esta investigación.

A todos muchas gracias.

RESUMEN

El Ministerio de Educación le presta especial atención a este tema pues un gran por ciento de sus trabajadores son usuarios de la tecnología. La seguridad informática, es una serie de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. El presente trabajo tiene como título: La preparación de la seguridad informática, en la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila y tiene como objetivo elaborar un sistema de actividades que contribuya a la preparación en la seguridad informática de estos alumnos. En la investigación se utilizaron métodos del nivel teóricos, como son: el analítico-sintético, inductivo-deductivo, histórico-lógico, enfoque de sistema. Del nivel empírico: la observación, la encuesta, la entrevista, triangulación y el pre–experimento. Dentro de los métodos estadísticos-matemáticos, se emplea el cálculo porcentual, presentando los datos en tablas y gráficos. Mediante ellos se pudo determinar que la preparación teórica elemental de los alumnos en la seguridad informática es insuficiente, careciendo de actividades que la faciliten. Se diseñó un sistema de actividades donde se realiza tres conversatorio, dos charla, dos talleres, un debate y una mesa redonda.

ÍNDICE

Páginas

INTRODUCCIÓN

En la Educación, constituye un hecho fundamental, que tiene como propósito lograr que la nueva generación adquiera habilidades computacionales, desarrollen habilidades de asimilación y resolución de conceptos a través de los medios de cómputo.

La utilización de la Informática se va volviendo cada vez más usual e indispensable en el Ministerio de Educación y ya es prácticamente imposible concebir una actividad en la que la misma no esté presente, en una u otra medida. Un factor elemental a tener en cuenta en la escuela cuando se usan las tecnologías, es la seguridad informática, como manera de prevenir daños y riesgos en los diferentes escenarios donde se encuentran las computadoras.

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Varios autores han abordado el tema, entre los que se destaca Rodríguez, E (2006) se refiere al trabajo con la seguridad informática y a los delitos informáticos. Además Garnier, J. (2006 y 2007) establece un concepto de Seguridad informática, Ávila, R. (2007) ofrece un sitio Web sobre seguridad informática y Meneses, A. (2008) se refiere a la necesidad de indicadores de vigilancia en la seguridad informática.

En la etapa exploratoria de la investigación se pudieron determinar las siguientes **problemáticas** en cuanto a la preparación en la seguridad

informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila.

- Insuficiente conocimiento teórico de lo que es la seguridad informática.
- Evidencia de violaciones de la seguridad informática, referida a la introducción de archivos no autorizado en el Ministerio de Educación.
- Insuficiencia en la implementación del Plan de seguridad informática.
- Los alumnos se contemplan como usuarios de la tecnología y es insuficiente la preparación desde el proceso docente educativo en la seguridad informática.

Por lo que se establece una **contradicción**, pues hoy se desea que los alumnos sean usuarios de la tecnología de la Información y las comunicaciones y sin embargo poseen desconocimiento teóricos de la seguridad informática.

Por los motivos anteriormente expuestos se propone el siguiente **problema científico**: ¿Cómo contribuir a la preparación en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila?

El **objetivo** de esta investigación es proponer un sistema de actividades que contribuya a la preparación en la seguridad informática de los alumnos del primer subgrupo del 7mo A en de la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila.

Para dar respuesta al problema científico se proponen las siguientes **preguntas científicas.**

1. ¿Cuáles son los fundamentos teóricos y metodológicos que sustentan la preparación metodológica de la seguridad informática de los alumnos del 7mo A de la ESBU Carlos J. Finlay de la de la provincia de Ciego de Ávila, para el desempeño de sus funciones?
2. ¿Cuál es el estado real que presenta la preparación en la seguridad informática de los alumnos del 7mo A de la ESBU Carlos J. Finlay de la de la provincia de Ciego de Ávila?

3. ¿Qué actividades confeccionar para la preparación elemental en la seguridad informática de los alumnos del 7mo A de la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila?
4. ¿Qué nivel de efectividad tiene en práctica el sistema de actividades diseñado para los alumnos del 7mo A de la ESBU Carlos J. Finlay de la de la provincia de Ciego de Ávila?

Para dar cumplimiento a las preguntas científicas señaladas se plantean las siguientes **tareas investigativas**.

1. Determinación de los fundamentos teóricos y metodológicos que sustentan la preparación metodológica en la seguridad informática de los alumnos del 7mo A de la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila, para el desempeño de sus funciones.
2. Diagnóstico del estado real del fortalecimiento de la preparación en la seguridad informática de los alumnos del 7mo A de la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila.
3. Elaboración de un sistema de actividades para la preparación en la seguridad informática de los alumnos del 7mo A de la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila.
4. Evaluación de la efectividad del sistema de actividades diseñado, donde ha sido propuesto los alumnos del 7mo A de la ESBU Carlos J. Finlay del municipio Primero de Enero de la provincia de Ciego de Ávila.

La **población** de esta investigación está conformada por 146 alumnos de la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila que es la totalidad de los alumnos de 7mo grado del municipio Primero de Enero de la provincia de Ciego de Ávila de la provincia de Ciego de Ávila, ya que son usuarios de la tecnología en el centro y necesitan de la preparación para contribuir al desarrollo de la seguridad informática, además de interactuar de manera directa la autora con el grupo. Se seleccionó como **muestra** 15 será un subgrupo del 7mo A, ya que son los alumnos que presentan mayores dificultades en cuanto a la seguridad informática.

Para el desarrollo de esta investigación se utilizaron los **métodos** de los niveles: teóricos, empíricos y estadísticos-matemáticos. Dentro de los métodos del nivel teórico se utilizaron:

Analítico-sintético: Permitió obtener conocimientos sobre la preparación elemental de la seguridad informática, a partir de la información encontrada en artículos, informes, revistas, libros y periódicos publicados. Además, se pudo descomponer a la seguridad informática y la preparación, en los principales elementos que las conforman y determinar sus particularidades. Se empleó para la interpretación de los resultados derivados del diagnóstico, en la elaboración de sistema, las conclusiones parciales y generales.

Inductivo–deductivo: Se extrajeron las regularidades, particularmente las referidas a los requerimientos teóricos y metodológicos exigidos a la propuesta de un sistema de actividades, que permitiera sensibilizar a los alumnos sobre la necesidad de su preparación en la seguridad informática, ya que la inducción es una forma de razonamiento por medio de la cual se pasa del conocimiento de casos particulares, al conocimiento más general y la deducción es una forma de razonamiento mediante el cual se pasa de un conocimiento general a otro de menor nivel de generalidad.

Histórico-lógico: Se seleccionó este método con el objetivo de poder estudiar la trayectoria real del fenómeno en el transcurso de su historia, en este caso se empleó para conocer los antecedentes del desarrollo de la seguridad informática y sobre la elaboración de un sistema de actividades así como los conocimientos teóricos que se poseen de esta problemática, mediante lo lógico se despoja el histórico de todo aquello que se repite, es decir, de los elementos secundarios, superficiales e irrelevantes, convirtiendo así la historia en un conocimiento lógico.

Enfoque de sistema: Permitió establecer comparaciones que tienen relaciones de jerarquización, dependencia, subordinación y coordinación entre las actividades que componen el sistema de actividades.

Como métodos del nivel empírico se utilizaron:

1-Prueba pedagógica: Se empleará para constatar el conocimiento de los alumnos del primer subgrupo del 7mo A en la seguridad informática en la ESBU Carlos J. Findlay de la provincia de Ciego de Ávila.

2- Observación: Esta se empleó para determinar los conocimientos en la seguridad informática de los alumnos del primer subgrupo del 7mo A de la ESBU Carlos J. Findlay de la provincia de Ciego de Ávila. Se utilizó para diagnosticar la realidad.

3- Entrevista: Se utilizó para determinar los conocimientos, habilidades y motivaciones que poseen los alumnos del primer subgrupo del 7mo A de la ESBU Carlos J. Findlay de la provincia de Ciego de Ávila en cuanto la seguridad informática, así como las formas o vías que utiliza para prepararse.

4- Encuesta: Se realizó para determinar los conocimientos, habilidades, motivaciones y actitudes que poseen los alumnos del primer subgrupo del 7mo A de la ESBU Calos J. Findlay de la provincia de Ciego de Ávila del municipio Primero de Enero de la provincia de Ciego de Ávila referido a la seguridad informática.

5- Pre-experimento: Posibilitó constatar la validez del sistema de actividades mediante su puesta en práctica.

6- Triangulación: Se utilizó en el procesamiento de los datos desde distintos ángulos en los instrumentos aplicados, documentos y métodos para compararlos y contrastarlos entre sí.

Además se utilizaron métodos estadísticos-matemáticos: De la estadística se utilizó la estadística descriptiva y del matemático el procedimiento análisis porcentual para el procesamiento de toda la información cuantitativa de la investigación, con el propósito de determinar tendencias a partir de la aplicación de determinados instrumentos y técnicas, presentando los datos en tablas y gráficos.

DESARROLLO

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA Y METODOLÓGICA QUE SUSTENTAN LA SEGURIDAD INFORMÁTICA Y LA PREPARACIÓN DE LA SEGURIDAD INFORMÁTICA DEL PRIMER SUBGRUPO DEL 7MO A EN LA ESBU CARLOS J. FINLAY DEL MUNICIPIO PRIMERO DE ENERO DE LA PROVINCIA DE CIEGO DE AVILA.

1.1 Antecedentes históricos del proceso de la seguridad informática en la ESBU.

Desde hace aproximadamente 50 años, después de la Segunda Guerra Mundial, tomó auge la tecnología que prácticamente generó el actual significado de la palabra "computación". Su origen lingüístico proviene del latín "computare", cuyo sentido se interpreta conceptualmente "con el pensamiento", y que tomó el significado de "contar o calcular algo con números", según lo define el diccionario de la Real Academia de la Lengua Española.

La palabra "informática" es un neologismo por contracción de las palabras "información" y "automática". Para entender el término seguridad informática es importante conocer sobre el de seguridad jurídica, que es un principio del Derecho universalmente reconocido en todas y cada uno de las esferas Estatales y Administrativas. Se entiende como la certeza o verdadera práctica del Derecho y todos los elementos que en ella se encierran o encuadran; representa la seguridad y certeza de quien conoce o puede conocer lo previsto en una norma, ley o reglamento, así como todo lo que está prohibido, mandado y permitido por la Administración respecto de uno para con los demás y de los demás para con uno.

Este concepto preciso sobre la seguridad, establece la primacía de la Ley frente a otras normas de menor jerarquía, las cuales van siendo reconocidas por su propia naturaleza como ser la Constitución Política del Estado, al ser la Ley Suprema del Ordenamiento Jurídico de un Estado, luego en menor jerarquía están las Leyes, luego los Decretos y los mismos van descendiendo

hasta llegar a disposiciones o reglamentaciones intra institucionales que regulan y reglamentan la actividad institucional.

La Seguridad es una necesidad básica dirigida a la prevención de la vida y las posesiones, es tan antigua como ella. Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, Cesar han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción, reducción de fallos y pérdidas han traído nuevos enfoques a los sistemas de seguridad.

La seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, el teórico (Fayol, Henry, 1919), identifica la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Con la aparición de las computadoras, esta mentalidad se mantuvo. Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que no se pueden incurrir y las respectivas medidas, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y en última instancia, en cada uno de sus trabajadores. En el grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio. Es en este proceso, donde se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de

aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, guardias fuertemente armados, trampas, vigilancia, entre otros.

Uno de los pioneros en el tema de la seguridad informática fue James P. Anderson, quien en el año1980 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.

A finales de la década del 80 e inicios de la del 90, comienzan a proliferar en el país varios virus informáticos y programas malignos, los que llegan por diferentes vías con la consiguiente afectación de máquinas y sistemas. Por ello, surge la necesidad de enfrentar un nuevo reto en la informática: el logro de la seguridad y protección de los recursos informativos en los centros educacionales.

A principio de los 90, el relativo abandono del modelo organizativo-institucional inspirado en los soviéticos, hizo que el gran centro de diseño de sistemas del fenecido Comité Estatal de Abastecimientos, provisto de un capital humano considerable, se viese obligado a rediseñarse, a encontrar una nueva misión y nuevos objetivos de trabajo. Era esa la institución ideal para la lucha contra los virus y para el logro de la seguridad informativa. Se crea entonces la empresa Segurmática, consultora de seguridad y protección informática.

Teniendo en cuenta lo anterior, se editan textos legales que ofrecen apoyo a este objetivo, como son el Reglamento de Seguridad Informática, emitido por el Ministerio del Interior en 1996, el cual estipula que todos los ministerios y organismos centrales de la Administración Central del Estado, así como empresas y otras instituciones de Educación. Deben analizar, confeccionar, aplicar planes de seguridad informática y de contingencia; para reducir el riesgo de afectaciones a los recursos informativos, por la acción de catástrofes naturales o artificiales, de fraudes, de errores humanos, de los propios programas malignos o de otra naturaleza.

Otro reglamento complementario al anterior, fue emitido por el Ministerio de la Industria Sideromecánica y Electrónica (que en los primeros años de la década del 90, había asimilado las funciones del extinto INSAC, en relación con la computación, la informática y la electrónica). El resto de los ministerios, de las empresas, corporaciones, emitieron reglamentos específicos para la protección y seguridad de los recursos informativos.

La seguridad informática en Cuba ha transitado por tres etapas de desarrollo, en correspondencia de cómo ha evolucionado a nivel internacional y nacional los avances de las TIC y el desarrollo de la sociedad, estas etapas son:

1ra Etapa: Desde 1980 hasta la década de 90. Se caracteriza por ver los aspectos de la seguridad informática relacionados con seguridad en las puertas de accesos a las TIC, y custodios bien armados, con el objetivo de disminuir las vulnerabilidades físicas, confidencialidad de los datos y las amenazas externas, Se controlaba o resguardaba esencialmente la información clasificada y sensible.

2da Etapa: Desde 1990 hasta 1999. Se caracteriza por ver en un sentido más amplio los temas de la seguridad informática, con respecto a la etapa anterior, se parte de los aspectos de detección de los incidentes y su corrección. Se incluyen en los análisis elementos como las vulnerabilidades electrónicas, confidencialidad de los datos, disponibilidad e Integridad, amenazas internas y externas. Se controlaba o resguardaba esencialmente la información clasificada y sensible.

3ra Etapa: Desde el año 2000 hasta la fecha, se caracteriza la seguridad informática como aspectos de prevención y gestión; se realiza conscientemente el análisis de riesgos, vulnerabilidades, validación de seguridad en la red, la respuesta a incidentes y recuperación.

Hoy se constata que la seguridad informática hay que verla con un enfoque integral y en sistema; donde se incluyen un conjunto de acciones desde el punto de vista soluciones técnicas, organizativas, legales y educativas al

problema; con el fin de minimizar los riesgos y los costos (dinero, tiempo, recursos) que acarrean la pérdida, la modificación y la propagación no deseada de información de alto valor para su poseedor.

La Seguridad Informática, como fenómeno complejo que abarca no sólo las economías de todos los países del mundo, sino que trasciende a la política, a la cultura, a los valores, a la moral e inclusive a las creencias religiosas y abarca prácticamente a todos los sectores de la sociedad. Favorece a que la seguridad informática adquiriera en la actualidad un gran auge a nivel internacional.

Se debe analizar, confeccionar y aplicar planes de seguridad informática, 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 naturalezas sobre esa base legal se inició el trabajo, pero era necesario encontrar una organización técnicamente fuerte que asimilara la responsabilidad de la lucha contra los programas malignos.

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

Hoy día, no existen sistemas completamente seguros, por lo que se hace necesarios buscar los aspectos vulnerables; por tanto, crear conciencia a los directores, docentes y alumnos de la necesidad de la seguridad, puesto que la

mayor cantidad de ataques se produce por usuarios de las propias instituciones. Los usuarios deben conocer las políticas de seguridad con el fin de interiorizar las implicaciones que su desconocimiento ocasionaría. Es por ello, que se hace necesario un proceso de preparación de los técnicos de laboratorio de Computación en el uso y desarrollo de la seguridad informática, la cual plantea nuevas exigencias.

1.2 Fundamentos teóricos del proceso de la seguridad informática para el 7mo grado dentro del proceso de enseñanza aprendizaje.

Cuba ha tenido un avance vertiginoso en el uso y utilización de las tecnologías de la informática, realidad que se ha acrecentado luego de la política de informatización de la sociedad vinculada a la Batalla de Ideas. Para dar cabal cumplimiento a esta realidad ha incorporado paulatinamente los principios que a escala mundial rigen esta disciplina, promulgando legislaciones y lanzando estrategias acordes a las características propias del país donde no ha faltado el considerar importante; es vital para la seguridad e integridad nacional el dominio de las tecnologías de la informática y la seguridad asociadas a ellas.

Se considera que la seguridad informática es en esencia la actividad preventiva que se realiza en la escuela sin la cual, el Estado como figura principal de la actividad económica cubana, no podría controlar los problemas que surgen en un universo tan complejo como el informático. Las violaciones son diversas, variadas y dentro de ellos están: los casos en los que se encuentran involucradas las tecnologías de las informaciones y las comunicaciones. Al igual que muchos otros contravenciones, que surgen, se desarrollan en el colectivo laboral e intervienen trabajadores, funcionarios, dirigentes por lo que es imposible llegar a esclarecerlos si no se toman y garantizan las acciones de seguridad, suficientes para impedirlo.

El uso creciente y la confianza en los computadores en todo el mundo han hecho surgir una preocupación legítima con respecto a la seguridad informática. Los computadores se han extendido en ambientes comerciales, educativo, gubernamentales, militares e incluso en los hogares. Grandes

cantidades de datos vitales sensibles se están confiando y almacenado cada vez más en computadores.

La seguridad, no solo requiere un sistema de protección apropiado, sino también considerar el entorno externo en el que el sistema opera. Los problemas de seguridad son esencialmente de administración, no problemas del sistema operativo. La información almacenada en el sistema, así como los recursos físicos del sistema de computación, tienen que protegerse contra acceso no autorizado, destrucción o alteración mal intencionado y la introducción accidental de inconsistencia.

Se asumen los fundamentos teóricos de Leblanch; 2008, en la que expresa que la seguridad informática está inmersa en el proceso de una cultura informática, que como fenómeno complejo abarca no sólo las economías de todos los países del mundo y sino que trasciende a la política, la cultura, los valores, la moral e inclusive a las creencias religiosas y abarca prácticamente a todos los sectores de la sociedad. Todo lo antes expresado favorece a que la seguridad informática adquiriera en la actualidad un gran auge a nivel internacional. A continuación se ofrece el encargo social de la seguridad informática asumido en la investigación.

La Seguridad informática consiste en asegurar que los recursos del sistema de información (Software, hardware y datos) de una organización sean utilizados de la manera como se planeó. Hoy en día, los sistemas informáticos son herramientas muy útiles en el sistema educativo. Básicamente, en ellos, aparecen todos los software educativos a utilizar en la docencia y otros programas educativos; así como documentos que procesa la escuela; pero son susceptibles de amenazas.

Por tal razón, la evaluación y control de la seguridad informática se encarga de evaluar si se están cumpliendo con las medidas de control para minimizar los riesgos que conlleva la utilización de sistemas informáticos. Según las fuentes de amenazas, estos riesgos se clasifican en Seguridad Lógica y Seguridad Física. El activo más importante de una escuela es la información; por ello, es

necesario contar con planes y políticas para protegerla. Para minimizar los riesgos se debe verificar de planes y políticas de seguridad para la protección de uno de los activos más importantes de la institución: la Información. Todo proceso se debe atender de manera cuidadosa la planificación, ejecución, evaluación y control de la seguridad informática.

El control a la seguridad informática es una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar-evaluar la planificación, el control, la eficacia, la seguridad y la adecuación de la informática en la escuela.

Es importante conocer cómo desarrollar y ejecutar la implantación de un Sistema de Seguridad. Desarrollar un Sistema de Seguridad implica: planear, organizar, coordinar dirigir y controlar las actividades relacionadas a mantener. Además de garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la escuela.

Rebeca Ávila; 2009, ofrece los objetivos de la seguridad informática, las cuales se asumen en la investigación, entre los que se destaca, mantener la protección contra la divulgación no autorizada de la información, la destrucción o alteración no autorizada de la información y la manipulación no autorizada de los recursos informáticos. Como funciones asociadas a ella están las de:
REGULACION: Capacidad de establecer las normas, preceptos, reglamentos y otros tipos de medidas jurídicas.
CONTROL: Facultad de verificar la adopción y el cumplimiento de lo regulado.
PREVENCION: Acciones que se realizan con el fin de minimizar los riesgos. Es la forma más eficaz y la vía más elemental para garantizar la seguridad durante el empleo de las TIC.
DETECCION: Conocimiento de la materialización de una amenaza.
ENFRENTAMIENTO: Acciones de respuesta.

La seguridad informática no solo se orienta hacia las actividades intencionales o premeditadas, sino que debe ocuparse también de los inconvenientes, pérdidas ocasionadas por causas accidentales, tanto naturales, como las que

son producto de actividades laborales o sociales, que generalmente exceden a las afectaciones originadas por las actividades delictivas.

Por su parte Anderson y Ávila; 2009, fundamentan que la seguridad informática tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información, lo cual se comparte en la investigación. Expresan que es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias. Para ello, deben utilizarse métodos formales de análisis de riesgos que lo garanticen. Se refieren a estos tres aspectos básicos que a criterio de la autora, son esenciales para el crecimiento de la entidad, el cumplimiento de la legalidad vigente y la imagen de la propia escuela:

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

Es importante conocer las posibles amenazas y riesgos en la seguridad informática, abordado por Del Valle; 2006, la cual se comporte en la investigación, pues permite que el trabajo del director de ESBU Carlos J. Finlay del municipio primero de enero de la provincia de Ciego de Ávila pueda tener éxito al respecto, si sucede lo contrario es algo catastrófico o sea todo un fracaso de los sistemas de seguridad. Aunque los activos están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas siempre existirán en los centros educacionales y están relacionadas a causas que representan riesgos, las cuales pueden ser:

• Causas naturales o no naturales.
• Causas internas o externas.

A criterio personal la seguridad informática, es una serie de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

Ávila; 2009, explica que el proceso de la seguridad informática depende de implantar una política de seguridad, la cual depende de una buena estrategia de divulgación entre los usuarios, una libre disposición de su contenido a todos los involucrados para aumentar el nivel de seguridad y compromiso de cada uno, campañas, entrenamientos, charlas de divulgación, sistemas de aprendizaje y otros mecanismos adoptados para hacer de la seguridad un elemento común a todos, los cuales se asumen en la investigación.

Se comparte las ventajas de las políticas de seguridad, que ofrece Ávila; 2009, dentro del proceso de seguridad informática en la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila, donde plantea que permite establecer los derechos de acceso con base en las funciones de cada persona, la orientación de los usuarios con relación a la disciplina necesaria para evitar violaciones de seguridad, establece exigencias que pretenden evitar que la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila sea perjudicada en casos de quiebra de seguridad, la realización de investigaciones de delitos por computadora y convierte en el primer paso para transformar la seguridad en un esfuerzo común.

Puede declararse que es común encontrar separada la seguridad física y seguridad lógica. Entendiendo la seguridad física aquella que se relaciona normalmente con temas de políticas de seguridad, normativas, planes de contingencia, la protección física de los datos, gestión de la seguridad, accesos, auditoria, leyes. En cambio la seguridad lógica está más orientada hacia la protección de la información en su mismo medio, ya sea generación, almacenamiento y transmisión; usando en este caso por lo general herramientas, técnicas y esquemas propios de la criptografía. Se considera que

no está muy clara la delimitación entre una y la otra, ambas se complementan y una no puede plantearse sin la otra. Lo que sí está aceptado por todos es que hoy, la seguridad informática es una especialidad emergente donde convergen un alto número de disciplinas y temas muy específicos.

Se entiende que la seguridad informática ha sido un tema complicado porque cada organización es distinta y no hay un acuerdo sobre la mejor manera de organizar la seguridad informática en un organismo pero en la sociedad cubana los procesos de informatización obligan a un excesivo desembolso de moneda libremente convertible para la adquisición de la tecnología de comunicaciones, millares de microcomputadoras personales, equipos periféricos y otros aditamentos.

Este costoso equipamiento está en manos de alumnos y trabajadores, desde la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila, oficinas, hogares, unidades de servicios y hasta los más encumbrados centros de investigación científica. Es un ambicioso programa sobre el que se trabaja desde hace años y la economía nacional lo asimila progresivamente por sus bondades en cuanto al mejoramiento de los servicios, organización y humanización de las fuentes productivas, para la investigación e incluso para elevar el nivel y la calidad de vida de los ciudadanos.

Por las urgencias propias del desarrollo, el 9 de julio de 2007 el Comité Ejecutivo del Consejo de Ministros tomó el acuerdo 6058, donde determinó que los organismos de la Administración Central del Estado adoptaran las medidas necesarias para el fortalecimiento de la seguridad de las tecnologías de la información en sus respectivos sistemas, en correspondencia con el esfuerzo que viene realizando el país en el desarrollo acelerado de la informática, para lo cual asegurarán, controlarán y exigirán en su ámbito de competencia. Se decidió el establecimiento de niveles de seguridad informática apropiados; la elaboración, aprobación, puesta en vigor y cumplimiento de los planes de seguridad informática. Por lo que su permanente actualización, designación, preparación, control del personal responsabilizado por los sistemas informáticos y su seguridad.

Se regularizan acciones a realizar mediante el empleo de las tecnologías de la información, particularmente aquellas que impliquen afectaciones a terceras partes. Las tecnologías, sistemas que se adquieran o que se implementen garanticen el grado de seguridad requerido, la creación, ejecución de los procedimientos establecidos ante la ocurrencia de incidentes y violaciones de seguridad. En su inciso quinto, faculta al Ministerio de la Informática y las Comunicaciones para ejercer la inspección estatal a la seguridad de las tecnologías de la información y establecer las regulaciones correspondientes, así como las normas para la prestación de servicios de Seguridad informática a terceros.

El complemento a todo el esfuerzo nacional es la Resolución 127, de 2007, en la que el Ministro de la Informática y las Comunicaciones, resolvió aprobar y poner en vigor el Reglamento para las tecnologías de la información, que regulariza el funcionamiento del sistema informático en el país.

La seguridad es hoy día una profesión compleja con funciones especializadas. Dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad física, seguridad ambiental, seguridad nuclear, seguridad lógica, entre otras. Para dar una respuesta satisfactoria es necesario eliminar la incertidumbre en el concepto, en esta investigación se asume que la seguridad es la calidad de algo seguro, y que algo seguro es algo libre de todo daño y riesgo.

Hoy en día, existen diferentes definiciones de Seguridad Informática tales como:
La seguridad informática puede ser definida, básicamente, como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información. Departamento de Sistemas y Computación Instituto Tecnológico de Morelia, México 2008.

Es muy común encontrar documentos donde la seguridad informática viene separada en dos apartados: seguridad física y seguridad lógica. Entendiendo la seguridad física aquella que se relaciona normalmente con temas de políticas

de seguridad, normativas, planes de contingencia, la protección física de los datos, gestión de la seguridad, accesos, auditoria, leyes. En cambio la seguridad lógica está más orientada hacia la protección de la información en su mismo medio, ya sea generación, almacenamiento y transmisión, usando en este caso por lo general herramientas, técnicas y esquemas propios de la criptografía.

La seguridad informática es un tema de gran importancia debido al desarrollo que han alcanzado las tecnologías y la dependencia de los que con ellas laboran. Puede definirse como el conjunto de reglas, planes y acciones que permiten asegurar la información contenida en un sistema computacional o la capacidad de mantener intacta y protegida la información de sistemas informáticos, permitiendo asegurar que los recursos del sistema de información generalmente (material informático o programas) de una organización sean utilizados de manera que no sea fácil de acceder por cualquier persona que no se encuentre acreditada.

Se determina como definición de seguridad Informática un enfoque integral y en sistema, donde se incluyen un conjunto de acciones desde el punto de vista soluciones técnicas, organizativas, legales y educativas al problema, con el fin de minimizar los riesgos y los costos (dinero, tiempo, recursos) que acarrean la pérdida, la modificación y la propagación no deseada de información de alto valor para su poseedor. Que en su esencia se denomina una de otra.

1.3 La preparación elemental en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila.

La secundaria tiene carácter obligatorio y universal, con beneficio para todos los alumnos, partiendo del principio de que a la más joven generación hay que enseñarla, atenderla y educarla. Su fin es contribuir a la formación integral del escolar, fomentando desde los primeros grados, la interiorización de los conocimientos y orientaciones valorativas, que se reflejan gradualmente en los

sentimientos, formas de pensar y comportamiento, que se corresponden con los valores e ideales de la Revolución Socialista.

La utilización de la computación como medio de enseñanza en esta enseñanza abre nuevos caminos para la dirección del proceso docente educativo, a la vez que garantiza el vínculo del mismo con el entorno tecnológico en que se desarrolla la sociedad.

En el desarrollo de la Informática Educativa en Cuba, la utilización de la computación en la enseñanza ha constituido un objetivo priorizado. A partir de 1984, con la asignación por el Gobierno Cubano de un fondo financiero significativo, se logró adquirir volúmenes crecientes de microcomputadoras, que posibilita un proceso amplio y acelerado en el caso de esta tecnología en los diferentes niveles de educación.

El uso de las Tecnologías Informáticas se convierte en una indispensable herramienta para elevar la calidad del proceso docente de enseñanza aprendizaje. El programa de Informática Educativa del Ministerio de Educación (MINED) en el área de la docencia, contempla la introducción de la computación como objeto de estudio dentro de los planes y programas en todos los niveles, así como la introducción progresiva del software educativo como medio de enseñanza en todos los niveles de educación. El estado cubano ha invertido cuantiosos recursos humanos y materiales en establecer el Programa de Informática en la Secundaria Básica.

A la educación se le ha designado socialmente la función de transmitir y generar los conocimientos. A través de la investigación, el avance de la ciencia y el desarrollo tecnológico, la educación ha estado empleando las nuevas tecnologías de la información y la comunicación para apoyar la labor docente, acceder a un número mayor de personas, además de acortar las distancias, como el Internet que ha globalizado el mundo.

En el desarrollo de la Informática Educativa en Cuba, la utilización de la computación en la enseñanza ha constituido un objetivo priorizado. A partir de

1984, con la asignación por el Gobierno Cubano de un fondo financiero significativo, se logró adquirir volúmenes crecientes de microcomputadoras, que posibilita un proceso amplio y acelerado en el caso de esta tecnología en los diferentes niveles de educación.

El uso de las Tecnologías Informáticas se convierte en una indispensable herramienta para elevar la calidad del proceso docente de enseñanza aprendizaje. El programa de Informática Educativa del MINED en el área de la docencia, contempla la introducción de la computación como objeto de estudio dentro de los planes y programas en todos los niveles, así como la introducción progresiva del software educativo como medio de enseñanza en todos los niveles de educación.

Por las urgencias propias del desarrollo, el nueve de julio de 2007 el Comité Ejecutivo del Consejo de Ministros tomó el acuerdo 6058, donde determinó que los organismos de la Administración Central del Estado adoptaran las medidas necesarias para el fortalecimiento de la seguridad de las tecnologías de la información en sus respectivos sistemas, en correspondencia con el esfuerzo que viene realizando el país en el desarrollo acelerado de la informática, para lo cual asegurarán, controlarán y exigirán en su ámbito de competencia.

Se decidió el establecimiento de niveles de seguridad informática apropiados; la elaboración, aprobación, puesta en vigor y cumplimiento de los planes de seguridad informática y su permanente actualización y la designación, preparación y control del personal responsabilizado por los sistemas informáticos y su seguridad. También regularizó las acciones que se realicen mediante el empleo de las tecnologías de la información, particularmente aquellas que impliquen afectaciones a terceras partes; que las tecnologías y sistemas que se adquieran o que se implementen garanticen el grado de seguridad requerido, la creación y ejecución de los procedimientos establecidos ante la ocurrencia de incidentes y violaciones de seguridad.

El estudiante recibe diferentes contenidos, se considera que lo que se le imparte a los alumnos en estos grados forma parte de la seguridad informática,

pues conociendo las partes de la computadora, como manipularla y el trabajo con programas que aparecen en ella poseen los alumnos una preparación elemental en este tema, pero entiende que ya se puede conocer otros contenidos que como usuario fundamental de la tecnología pudiera contribuir de manera más efectiva y dinámica en el proceso de seguridad informática que se desarrolla en la Secundaria Básica.

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

- En 7mo se continúan desarrollando habilidades intelectuales a partir del uso de los software educativos y el procesador de textos, se resuelven problemas prácticos relacionados con las asignaturas del grado escolar que cursan los alumnos al utilizar la computadora como herramienta y medio de enseñanza para la búsqueda, utilización de información y la creación de presentaciones de PowerPoint que apoyen sus trabajos prácticos. Entre los objetivos se persigue que cuiden y conserven de forma organizada su puesto de trabajo. En el trabajo con el procesador de texto se traba con la barra de dibuja para trabajar WordArt, autoformas, colores, la barra de imagen para trabajar contrastes y recortar imágenes. Al trabajar con el PowerPoint se crean diseños para presentaciones que den respuesta a los problemas y trabajos prácticos orientados. Redactar textos y editarlos. Insertar y transformar imágenes en diapositivas, animar imágenes y textos en correspondencia con los contenidos del grado, utilizar el contenido e imágenes de los software educativos en presentaciones de PowerPoint. Se pretende que los alumnos posean habilidades informáticas, generales e intelectuales para accionar con los softwares educativos, procesadores de textos u otros documentos que necesite. Aplicar conocimientos y habilidades informáticas en la elaboración de trabajos prácticos a partir del desarrollo curricular del nivel. Resolver problemas prácticos relacionados con las asignaturas del grado escolar que cursan, al utilizar la computadora como herramienta y medio de enseñanza para la búsqueda, utilización de información y la creación de modelos de

presentaciones que apoyen sus trabajos prácticos de forma integral. Cuidar y conservar de forma organizada su puesto de trabajo.

En este capítulo se realizó la fundamentación histórica, teórica y la preparación elemental del proceso de la seguridad informática en la Secundaria Básica que posibilita profundizar en los conocimientos al respecto, teniendo en cuenta dentro de los fundamentos teóricos los puntos de vista filosóficos, psicopedagógicos y sociológicos que sustentan la investigación.

CAPÍTULO 2: SISTEMA DE ACTIVIDADES PARA LA PREPARACIÓN ELEMENTAL EN LA SEGURIDAD INFORMÁTICA DE LOS ALUMNOS DEL PRIMER SUBGRUPO DEL 7MO A EN LA ESBU CARLOS J. FINLAY DEL MUNICIPIO PRIMERO DE ENERO.

Con el diagnóstico del estado inicial de la preparación de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero, en cuanto a la seguridad informática, se fundamenta el sistema de actividades desde el punto de vista filosófico, sociológico, psicológico, y pedagógico, se manifiestan sus características, desde el planteamiento del objetivo general, la descripción de cada una de las actividades y la forma de implementación que se sugiere.

2.1 Diagnóstico de la preparación elemental en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero.

Como paso previo, en el diseño del sistema de actividades para la preparación en la seguridad informática de los alumnos del primer subgrupo del 7mo A en de la ESBU Carlos J. Finlay del municipio Primero de Enero, se realizó un diagnóstico para conocer el estado real de su preparación.

El diagnóstico abarcó a 15 alumnos del primer subgrupo del 7mo A en de la ESBU Carlos J. Finlay del municipio Primero de Enero. Los instrumentos aplicados fueron los siguientes:

- Guía de observación.

- Entrevista.
- Encuesta.

Al aplicar la guía de observación con el objetivo de determinar los conocimientos en la seguridad informática de los alumnos del primer subgrupo del 7mo A, se pudo comprobar que:

- Emplean la tecnología diariamente. El laboratorio permanece con estudiantes todo el día.
- Las computadoras del escuela casi siempre poseen polvo.
- Los alumnos del primer subgrupo del 7mo A en no plasman su firma en el registro de acceso a las tecnologías.

Al realizar la entrevista a los 15 alumnos del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero dirigida a determinar los conocimientos y motivaciones que poseen los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila en cuanto la seguridad informática, se pudo determinar que: (Anexo X)

- El 17.64%, solo 3 alumnos, expresan que la seguridad informática es el cuidado y protección que hay que tener con los medios informáticos, el por ciento restante no emite criterio algunos.
- El 35.29% de los alumnos (6) expresan que un virus informático es algo dañino para las computadoras, el resto emite criterios que nada tiene que ver con el tema.
- El 35,29%, 6 de los alumnos, expresan que para contribuir a la buena seguridad informática de su escuela tienen que saber lo que tienen que hacer.

El resultado del instrumento aplicado demuestra que existen insuficiencias en la preparación elemental de los alumnos en la seguridad informática. Se corrobora que los alumnos presentan limitaciones en el conocimiento de lo que es la seguridad informática y la forma que pueden contribuir a ella.

Al realizar la encuesta con el objetivo de determinar los conocimientos que poseen los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay de la provincia de Ciego de Ávila en cuanto la seguridad informática, se pudo corroborar que: (Anexo 2)

- El 23,52%, 4 estudiantes, refieren que sí saben lo que es la seguridad informática.
- El 41.17%, 7 estudiantes, refieren conocer lo que es un virus informático.
- El 94,11%, 16 estudiantes, señalan que su maestro no le ha hablado sobre seguridad informática.
- El 100% señala que sí le gustaría conocer lo que es la seguridad informática. (total muestra)

Estos elementos entre otros, fundamentan la necesidad de establecer un sistema de actividades para contribuir en la seguridad informática a los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero, que les permita motivarlos, obtener conocimientos sobre la seguridad informática, así como desarrollar habilidades que les facilite obtener una preparación elemental en el tema.

2.2 Fundamentos teóricos y metodológicos del sistema de actividades para la preparación en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero.

Se han detectado dificultades en la preparación en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero, relacionada con la falta de dominio sobre la teoría de la seguridad informática y el qué hacer para contribuir a su buen funcionamiento, que se manifiesta en las limitaciones en cuanto a los conocimientos para su desempeño en la labor como alumno, el diagnóstico que recoge el estado inicial de su preparación permitió constatar, además, sus potencialidades, las que se tuvo en cuenta para la elaboración del sistema de actividades.

El sistema de actividades se fundamenta sobre la base de la filosofía marxista, el dominio del materialismo dialéctico-histórico permite analizar científicamente los fenómenos naturales y sociales, así como adquirir el conocimiento de las leyes y principios que rigen el sistema educacional cubano. La teoría

psicológica marxista concede un papel fundamental a la orientación en la formación de la psiquis humana. Ello ha sido aplicado de forma específica a la actividad cognoscitiva del hombre. La concepción acerca del sistema de actividades para la preparación de los monitores para el desarrollo de la seguridad informática, asume los postulados esenciales del Enfoque Histórico-cultural acerca de la personalidad, su formación y desarrollo.

El sistema de actividades para la preparación elemental en la Seguridad informática de los alumnos primer subgrupo del 7mo A en la ESBU Cralos J. Finlay del municipio Primero de Enero, un elemento esencial lo constituye el fundamento sociológico, pues revela al alumno como agente social, se considera que la contribución a la misma depende de los conocimientos que poseen.

En esta investigación se asumen algunas generalidades epistemológicas de la Teoría de la Actividad de Leontiev, basada en el enfoque Histórico-Cultural de Vygotsky.

Para Leontiev (2001, 2005) la actividad, permite al hombre relacionarse con el mundo para adaptarse a él y para poder transformarlo. Determinó que el objetivo y el motivo son los componentes principales de la actividad. Se precisan las acciones y operaciones como componentes de la actividad. Toda acción se descompone en varias operaciones con determinada lógica y consecutividad. Las operaciones son los procedimientos, la forma de realización de la acción de acuerdo con las condiciones, dándole a la acción una forma de proceso continuo. Estos fundamentos psicológicos se contextualizan en este trabajo a través de las acciones y operaciones propuestas en el sistema de actividades.

En la elaboración del sistema de actividades se tomó en cuenta que el sistema como resultado científico-pedagógico significa que es: “Una construcción analítica más o menos teórica que sustenta la modificación de la estructura de determinado sistema pedagógico real (aspectos o sectores de la realidad) y/o

la creación de uno nuevo, cuya finalidad es obtener resultados superiores en determinada actividad". Lorence González, J. (2004).

Desde el punto de vista pedagógico, la preparación en la seguridad informática asume la relación entre formación, instrucción, desarrollo y educación; la relación teoría práctica; y la relación, entre los componentes personales y personalizados del proceso docente-educativo con la finalidad de la formación de una personalidad integral.

Principios generales de la propuesta

- La propuesta responde al propósito de la preparación elemental en la seguridad informática.
- La consideración de las necesidades e intereses de los alumnos en el diseño del sistema de actividades, su preparación en torno a los objetivos, contenidos, métodos, ejecución y control.
- La interactividad comunicativa como premisa del intercambio, presupone el vínculo directo y sistemático entre las personas involucradas en la organización de este proceso.

La concepción del sistema de actividades se apoya en:

- Objetivos del modelo en los contenidos del modo de actuación de los alumnos.
- La interrelación de los factores involucrados en este proceso.
- Problemas resultantes del diagnóstico aplicado.

El sistema de actividades se diseña considerando los siguientes elementos:
Objetivo: Establecer una relación armónica entre todas las actividades a realizar en el proceso de desarrollo de la creatividad, evitar reiteraciones innecesarias y determinar la meta a lograr con el conjunto de actividades.
Contenido:

- Determinación de los tipos de actividades a realizar y su contenido específico.
- Precisión de los responsables y ejecutantes de cada actividad.

Métodos y Medios: El desarrollo de la actividad se determina según su tipología.

Se propiciará en cada caso un ambiente comunicativo e interactivo y un impacto emocional para el enriquecimiento espiritual, potenciando la máxima vinculación práctica.

Control y Evaluación: son funciones a tener en cuenta antes, durante y después de la realización de cada actividad.

Orientaciones metodológicas: Se propiciará en cada caso un ambiente comunicativo e interactivo y un impacto emocional para el enriquecimiento espiritual, potenciando la máxima vinculación práctica. Todas las actividades están concebidas para su realización en el tiempo de máquina de los alumnos.

Tiempo: Se otorga un tiempo que sea flexible para el cumplimiento de cada una de las actividades.

El carácter sistémico del sistema de actividades se fundamenta también en la concepción de su diseño, ejecución, control y evaluación con arreglo a objetivos integradores, diversificación de las formas y espacios para las actividades y el seguimiento continuo a la calidad de las acciones y su efectividad educativa. Se aprecia entre sus componentes principales: diagnóstico, objetivo y acciones de la planeación e instrumentación.

Dentro del principio de jerarquía el sistema superior de integración lo constituye el objetivo con su carácter rector, revelando el resultado del diagnóstico y pronosticando el resultado a alcanzar.

La estructura de sistema, entendida como el modo de organización e interacción entre los componentes y donde algunos adquieren una mayor jerarquía y otros se subordinan, permite que a partir del diagnóstico se determine el objetivo y que la proyección de las actividades contenidas en el

sistema responda a éste, existiendo una interdependencia entre cada actividad.

Características del sistema de actividades:

Objetividad: Porque toda la proyección está concebida a partir de los resultados del diagnóstico realizado a los alumnos en su contexto de actuación.

Desarrollo: Demuestra que el cambio y la transformación conscientes, posibilitarán el surgimiento de cualidades superiores que superarán las anteriores, o sea, ocurrirá en el proceso pedagógico un desarrollo en espiral, de lo simple a lo complejo, que le permitirá transitar por las diferentes etapas de preparación, mediante un proceso continuo, permanente, y evolutivo. Su progresión depende de su práctica sistemática.

Trabajo colectivo: Porque tiene como premisa esencial el trabajo colectivo que parte de la unidad de criterio y de acción, en el trabajo directo con los alumnos.

Flexibilidad: Porque puede rediseñarse permanentemente, en dependencia de las características.

Actualización: El sistema tiene en cuenta las principales concepciones pedagógicas y didácticas sobre el trabajo con los alumnos del segundo ciclo.

Intencionalidad: Por estar dirigido a la preparación elemental en la seguridad informática.

Capacidad evaluativa: Cada actividad permite ser evaluada, al estar concebidos los métodos, los instrumentos y las técnicas para el control de su efectividad.

Totalidad: El sistema contempla la muestra de la investigación.

Centralización: En las actividades del sistema la interacción rige al resto de las interacciones, tiene un papel rector. Existe una relación principal o conjunto de relaciones principales que le permiten al sistema cumplir con su función.

Complejidad: El sistema de actividades está organizado, ordenado de acuerdo con los indicadores, teniendo relación una con otras.

Jerarquización: Las actividades del sistema se ordenan de acuerdo con un principio a partir del cual se establecen cuáles son los subsistemas y cuáles los elementos.

Adaptabilidad: El sistema de actividades tiene la propiedad de modificar sus estados, procesos o características de acuerdo con las modificaciones que sufre el contexto.

Integración: Un cambio producido en cualquiera de sus subsistemas produce cambios en los demás y en el sistema como un todo.

Las exigencias que deben tenerse en cuenta al aplicar el sistema de actividades, son las siguientes:
Preparación previa del facilitador: Es imprescindible que el aplicador esté preparado con anterioridad para que la puesta en práctica del proyecto sea efectiva.

Disposición de todos los participantes: El cumplimiento de esta exigencia es fundamental porque garantiza el éxito de las actividades que se desarrollarán como parte del sistema y de la aplicación creativa en la utilización de medios, técnicas y procedimientos, a partir del conocimiento exhaustivo que debe poseer del objeto de transformación.

Condiciones higiénicas para su aplicación: Parte del éxito de la aplicación de este sistema está en el respeto y cumplimiento del sistema de actividades concebido para su cumplimiento y en las que debe primar un ambiente afectivo entre todos los participantes.

Aseguramiento material: Para aplicar el sistema de actividades se considera necesario que los elementos que forman parte del aseguramiento material

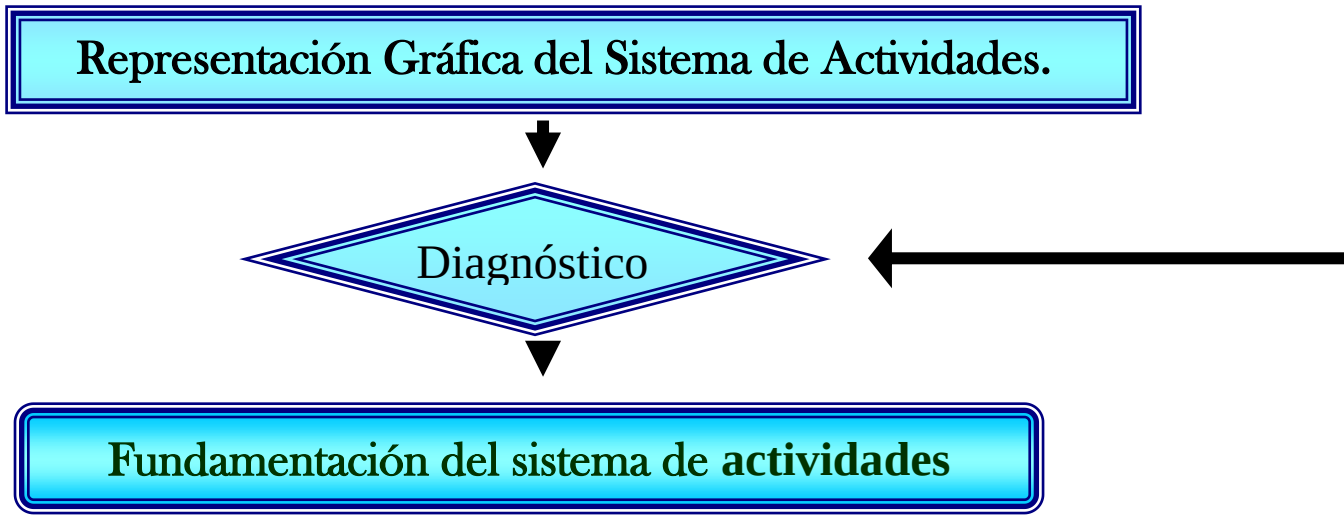
como: medios, los materiales de trabajo, los materiales de apoyo y la propuesta de actividades para la aplicación del sistema, estén previamente garantizados.

Para el sistema de actividades se tomó en consideración el enfoque integral, sistemático y sistémico de los componentes del proceso docente-educativo.

Esta concepción concibe su intencionalidad, ya que se propone con el objetivo de preparar de manera elemental en la seguridad informática a los alumnos, su capacidad referencial responde a los objetivos de la Secundaria Básica.

Su grado de amplitud está presente en cada actividad debido a que tienen concebida la meta a que aspira cada una de ella y la relación entre cada una de las actividades propuestas, además la aproximación analítica al objeto se manifiesta al reconocer las necesidades de cada una de los monitores y a partir de ahí se propuso el mismo. Se tuvo en cuenta su flexibilidad; para operar cualquier cambio o amplitud de las propuestas que se le quiera realizar, su aplicabilidad debido a que puede ser aplicado en cualquier escuela que posea laboratorio de Computación. Fue importante su carácter sistémico e integrador, este se expresa en las relaciones de coordinación, subordinación y jerarquización que se establece entre las actividades que lo componen. Su carácter integrador se concreta en la unidad de estudio.

En el diseño se incluyen objetivos y principios generales de este sistema de actividades con un enfoque colectivo a fin de organizar la labor del alumno.



Objetivo del sistema de actividades

Actividades

¿Qué debo saber?

¿Qué no se debe hacer?

¿Cómo tener mi PC saludable?

¿Qué es la Seguridad Informática?

¿Cómo cuidar el laboratorio?

¿Qué conocimientos tendré?

¿Cómo puedo ayudar?

¿Cómo se utiliza?

¿Será importante?

Implementación del sistema de actividades

Evaluación

2.3 Sistema de actividades para la preparación elemental en la seguridad informática de los alumnos primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero.

El sistema de actividades para la preparación elemental en la seguridad informática de los alumnos primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero se formula en relación directa con los componentes de la didáctica, lo cual se plantea a partir de la siguiente estructura: título, objetivo de la actividad, contenidos, recursos necesarios para la actividad. (Medios), acciones metodológicas. (Métodos), resultados esperados.

Sobre esta precisión teórica se puede presentar el sistema de actividades como se muestra a continuación.

***Actividad 1*:** Conversatorio.

Título: ¿Qué es la Seguridad Informática?

Objetivo: Analizar los elementos teóricos sobre lo que es la seguridad informática.

Contenido:

- ¿Qué es la seguridad informática? Importancia de la seguridad informática.
- Responsable de la seguridad informática.
- Resolución 127/2007.
- Usuarios de la tecnología.

Recursos necesarios para la actividad

Computadora

Acciones metodológicas

Es necesario que se centre la atención en lo que es la seguridad informática y que los alumnos del primer subgrupo del 7mo A forman parte de los usuarios de la tecnología como lo establece la resolución 127/2007, se realizará de manera sencilla, haciendo énfasis en lo que le corresponde al alumno cumplir dicha resolución. Además se le explica las responsabilidades que tienen los alumnos con el cuidado, uso y conservación de las computadoras.

Resultados esperados: Que los alumnos sepan lo que es la seguridad informática y la responsabilidad que tienen ante su uso.

***Actividad 2*:** Charla.

Título: ¿Cómo tener mi PC saludable?

Objetivo: Evaluar la importancia de la limpieza externa e interna de la computadora.

Contenido:

- El gran enemigo de la PC.
- Errores debidos a la suciedad del equipo.
- Los dos enemigos principales de la PC: el polvillo y la nicotina.
- ¡Peligro por humedad!
- **¡**Peligro por calor!
- Polvo en las computadoras ¿Realmente hace daño?

Recursos necesarios para la Actividad:

- Laboratorio de Computación.
- Computadora.

Acciones metodológicas:

El facilitador presentará la importancia de la limpieza de las computadoras a partir de explicar los daños que ocasiona el polvo y otros componentes de la computadora. Es importante enfatizar en la importancia de que los alumnos del primer subgrupo del 7mo A contribuyan con la limpieza externa de la computadora.

Resultados esperados:

- Contribuir al cuidado y limpieza de las computadoras y del laboratorio.
- Obtener conocimientos del daño que ocasiona el polvo para las computadoras.

Se deben solicitar a los participantes, sugerencias o actividades a considerar como objeto de transformación y perfeccionamiento constante del sistema de actividades. Puede hacerse de manera escrita y anónima, lo cual facilitará el flujo de información y la mayoría de criterios en un tiempo mínimo.

Como se conoce la charla: Motiva al oyente. Capta su atención. Despierta su interés y entusiasmo, se establece una comunicación personal con cada oyente y se dialoga con él. Lo involucra hasta tal punto, que lo invita a pensar juntos. Parte de una situación vivencial, trasluce calor humano. Para ello se apela a la experiencia del oyente, para que sienta el palpitar del corazón y no los razonamientos fríos del cerebro. El nivel del lenguaje es claro, sencillo y descriptivo. Usa metáforas y comparaciones. Da muchos ejemplos. La charla informa de manera entretenida.

***Actividad 3*:** Debate.

Título: ¿Qué no se debe hacer?

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

Contenido:

- Norma de ética en el laboratorio de Computación.
- Aspectos que pueden constituir violaciones de la seguridad informática.

Recursos necesarios para la actividad:

Laboratorio de Computación.

Diapositiva en PowerPoint.

Acciones metodológicas:

Este debate estará dirigido a que los alumnos del primer subgrupo del 7mo A aporten sus impresiones de lo que no se puede hacer en el laboratorio de computación según sus consideraciones y se le introduce el término de violación de la seguridad informática.

Se pretende crear espacios de diálogo entre iguales. Las interpretaciones surgen a partir de la comunicación intersubjetiva que se establece entre las personas que participan en ella.

Resultados esperados:

- Contribuyan a la seguridad informática del laboratorio.

Actividad 4: Mesa redonda.

Título: ¿Cómo puedo ayudar?

Objetivo: Valorar la forma de contribuir a la seguridad informática del laboratorio.

Contenido:

- Formas o vías en las que puede contribuir el alumno a la seguridad informática en el centro.

Recursos necesarios para la actividad:

Local o aula.

Acciones metodológicas:

Esta actividad se concibe como práctica pues en ella cada participante expondrá sus criterios de cómo puede contribuir a la seguridad informática de su escuela.

Se aplicará un PNI para tener seguridad de la aceptación de la propuesta del sistema de actividades.

Resultados esperados:

- Correcta aplicación de la seguridad informática por parte de los alumnos.

Actividad 5: Taller 1.

Título: ¿Cómo cuidar el laboratorio?

Objetivo: Profundizar en los registros de controles que deben existir en el laboratorio de Computación.

Contenido:

- ❖ Registros de la seguridad informática.
- ❖ Importancia del control en el laboratorio de Computación.

Se aplicará un PNI para tener seguridad de la aceptación de la propuesta del sistema de actividades.

Recursos necesarios para la actividad:

- ♦ Registros de la seguridad informática del centro.

Acciones metodológicas:

El desarrollo de la actividad se concibe para que los alumnos conozcan que ellos deben llenar el registro de acceso al local siempre que entran al mismo fuera del turno de clase de la asignatura y la importancia que tiene esos controles para la seguridad informática de la Secundaria Básica.

Resultados esperados:

- Interiorizar la importancia del control en el laboratorio de Computación.
- Actualización sistemática del registro de acceso a la tecnología.

Actividad 6: Taller 2

Título: ¿Qué debo hacer?

Objetivo: Determinar lo que es un virus, antivirus y la importancia de vacunar una computadora y la forma de hacerlo.

Contenido:

- ¿Qué es un virus?
- ¿Qué es un antivirus? Algunos tipos de antivirus.
- Forma de vacunar una computadora y su actualización.

Recursos necesarios para la Actividad:

- Computadoras, antivirus.

Acciones metodológicas:

El desarrollo de la actividad se concibe en un taller para el conocimiento de lo que es un virus, antivirus, tipos de antivirus, formas de vacunar una computadora. Es importante ejemplificar con el antivirus instalado en el municipio en las escuelas del territorio, en este caso se ejemplificará con el Kaspersky.

Resultados esperados:

- Elevación de los conocimientos de los alumnos en la seguridad informática.
- Vacunen las computadoras del centro de manera sistemática.

Actividad 7: Charla

Título: ¿Qué conocimientos tendré?

Objetivo: Evaluar la importancia de la seguridad de la computadora.

Contenido:

- El gran enemigo de la PC.
- Los dos enemigos principales de la PC: el polvillo y la nicotina.
- Polvo en las computadoras ¿Realmente hace daño?
- Peligro por calor.
- Importancia del control en el laboratorio de Computación.

Recursos necesarios para la Actividad:

- Laboratorio de Computación.
- Computadora.

Acciones metodológicas:

El facilitador presentará la importancia de la seguridad de las computadoras a partir de explicar los daños que ocasiona el polvo y otros componentes de la computadora. Es importante enfatizar en la importancia de que los alumnos contribuyan con la limpieza externa de la computadora.

Resultados esperados:

- Contribuir al cuidado y seguridad de las computadoras del laboratorio.
- Obtener conocimientos del daño que ocasiona el polvo para las computadoras.

Se deben solicitar a los participantes, sugerencias o actividades a considerar como objeto de transformación y perfeccionamiento constante del sistema de actividades. Puede hacerse de manera escrita y anónima, lo cual facilitará el flujo de información y la mayoría de criterios en un tiempo mínimo.

Como se conoce la charla: Motiva al oyente. Capta su atención. Despierta su interés y entusiasmo, se establece una comunicación personal con cada oyente y se dialoga con él. Lo involucra hasta tal punto, que lo invita a pensar juntos. Parte de una situación vivencial, trasluce calor humano. Para ello se apela a la experiencia del oyente, para que sienta el palpitar del corazón y no los razonamientos fríos del cerebro. El nivel del lenguaje es claro, sencillo y descriptivo. Usa metáforas y comparaciones. Da muchos ejemplos. La charla informa de manera entretenida

***Actividad 8*:** Conversatorio.

Título: ¿Cómo se utiliza?

Objetivo: Analizar los elementos teóricos de la utilización sobre lo que es la seguridad informática.

Contenido:

- ¿Cómo se utiliza la seguridad informática? ¿Qué es la seguridad informática?
- Responsable de la seguridad informática.
- Resolución 127/2007.
- Usuarios de la tecnología.

Recursos necesarios para la actividad

Computadora

Acciones metodológicas

Es necesario que se centre la atención en lo que es la seguridad informática y que los alumnos forman parte de los usuarios de la tecnología como lo establece la resolución 127/2007, se realizará de manera sencilla, haciendo énfasis en lo que le corresponde al alumno cumplir dicha resolución. Además se le explica las responsabilidades que tienen los alumnos con el cuidado, uso y conservación de las computadoras.

Resultados esperados: Que los alumnos sepan lo que es la seguridad informática y la responsabilidad que tienen ante su uso.

***Actividad 9*:** Conversatorio.

Título: ¿Será importante?

Objetivo: Analizar los elementos teóricos sobre lo importante que es la seguridad informática.

Contenido:

- ¿Qué es la seguridad informática? Importancia de la seguridad informática.
- Responsable de la seguridad informática.

Recursos necesarios para la actividad

Computadora

Acciones metodológicas

Es necesario que se centre la atención en lo que es la importancia de la seguridad informática y que los alumnos forman parte de los usuarios de la tecnología como lo establece la resolución 127/2007, se realizará de manera sencilla, haciendo énfasis en lo que le corresponde al alumno cumplir dicha resolución. Además se le explica las responsabilidades que tienen los alumnos con el cuidado, uso y conservación de las computadoras.

Resultados esperados: Que los alumnos sepan lo que es la seguridad informática y su importancia y la responsabilidad que tienen ante su uso.

2.4 Evaluación de la efectividad del sistema de actividades para la preparación elemental en la seguridad informática de los alumnos del

primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero.

Los estudios preliminares sobre la problemática y la práctica pedagógica se determinaron indicadores que permitieron evaluar el nivel de preparación en la seguridad informática de los alumnos de la ESBU Carlos J. Finlay del municipio Primero de Enero antes y después de aplicado el sistema de actividades propuesto.

Determinación de los indicadores para la evaluación del sistema de actividades**.**

- **Indicador 1:** Conocimientos de lo que es la seguridad informática.
- **Indicador 2:** Conocimientos de cómo tener mi PC saludable.
- **Indicador 3:** Conocimientos de lo que los alumnos deben saber para contribuir a la seguridad informática en el centro.
- **Indicador 4:** Formas en que se prepara para contribuir a la seguridad informática en el centro.
- **Indicador 5:** Habilidades que posee para tener mi PC saludable.
- **Indicador 6:** Disposición que posee para contribuir a la seguridad informática en su escuela.
- **Indicador 7:** Motivación por prepararse de manera elemental en el tema de la seguridad informática.

Resultado del pre-experimento:

Para la evaluación experimental se empleó el experimento pedagógico en su variante de pre-experimento, con una muestra de 17 alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero. La selección es intencional y se tuvo en cuenta que son estudiantes que le gusta la asignatura y pueden contribuir al desarrollo de la seguridad informática en la escuela.

Teniendo en cuenta el objetivo de la investigación se identifican dos variables a controlar: la preparación elemental en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio

Primero de Enero y el sistema de actividades para la preparación elemental en la seguridad informática.

El pre-experimento se desarrolló en los siguientes momentos.

1. Constatación inicial (pre-test).
2. Introducción del sistema de actividades.
3. Constatación final (post-test).

Para la implementación en la práctica educativa del sistema de actividades elaboradas y para comprobar su efectividad en la preparación elemental en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero, se elaboraron y se procesaron varios instrumentos que conforman el pre-test y el post-test, entrevista (Anexo 4), encuesta (Anexo 5)

Constatación inicial.

En la constatación inicial se procedió a realizar el pre-test para determinar el estado de capacitación inicial que tenían los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero sobre la seguridad informática, mediante la aplicación de los instrumentos ya mencionados anteriormente y la evaluación de los indicadores teniendo en cuenta los índices declarados en el **(Anexo 6).**

Una vez realizado el análisis de estos resultados la autora considera que:

Al aplicar la entrevista a los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay sobre la seguridad informática con el objetivo de determinar los conocimientos y habilidades que poseen los alumnos de la ESBU Carlos J. Finlay del municipio Primero de Enero referido a la seguridad informática, así como las formas o vías que utiliza para prepararse. Se pudo comprobar que existe desconocimiento por parte de los alumnos de lo que es la seguridad, solo dos alumnos expresaron algunos criterios aceptables de lo que era la seguridad informático, asociándolo en todos los casos al cuidado al robo de las mismas.

A la pregunta de cómo podían tener mi PC saludable, el 100% de los alumnos tienen dificultad en realizar esta operación.

Se aplicó una encuesta con el objetivo de determinar los conocimientos, habilidades, motivaciones y actitudes que poseen los alumnos de la ESBU Carlos J. Finlay del municipio Primero de Enero referido a la seguridad informática. En la misma se pudo comprobar el desconocimiento por parte de los alumnos de cómo contribuir a la seguridad informática en el centro.

Se comprobó que no se prepara a los alumnos desde el centro en el tema de la seguridad informática. Los alumnos tienen dificultad en qué es la seguridad informática, elemento de esencial importancia para contribuir a la seguridad informática en el centro.

El 100% de los alumnos están dispuestos a contribuir a la seguridad informática en el centro y desean además que los preparen en este tema.

Por lo que los indicadores quedan evaluados de la siguiente manera:
El indicador 1 quedó evaluado de Bajo, pues solo 2 alumnos que representa el 11.76% expresaron de manera muy sencilla lo que era la seguridad informática.
El indicador 2 quedó evaluado de Bajo, pues ninguno de los alumnos explicó cómo pueden tener mi PC saludable.
El indicador 3 quedó evaluado de Bajo, pues 3 alumnos que representa el 17,64% señalan que sí conocen lo que deben saber para contribuir a la seguridad informática en el centro.
El indicador 4 quedó evaluado de Bajo, pues 4 alumnos que representa el 23.52% señalan al menos una de las opciones que se les presentan para prepararse en el tema de la seguridad informática.
El indicador 5 quedó evaluado de Bajo, pues ninguno de los alumnos sabe cómo puedo tener mi PC saludable.
El indicador 6 quedó evaluado de Alto, pues el 100% de los alumnos están dispuestos a contribuir con la seguridad informática en el centro.
El indicador 7 quedó evaluado de Alto, pues el 100% de los alumnos desean que los preparen en el tema de la seguridad informática.

Insuficiencias derivadas de la constatación inicial.

- Son insuficientes los métodos, vías y procedimientos que emplea el centro para preparar a los alumnos en el tema de la seguridad informática.
- Falta de conocimientos de lo que es la seguridad informática.
- Débil desarrollo de habilidades que le permita a los alumnos contribuir al desarrollo de la seguridad informática en el centro.

Estas limitaciones se reflejan en la falta de conocimientos lo que conducen a que los alumnos que son los principales usuarios de la tecnología desconozcan la forma de contribuir a la seguridad informática para que puedan cumplir y hacer cumplir la misma. Sin embargo se constata las siguientes potencialidades: Los alumnos del primer subgrupo del 7mo A desean que los preparen en el tema de la seguridad informática y además se muestran dispuestos a contribuir a la seguridad informática en el centro. Los resultados anteriormente expresados reafirman la necesidad de buscar vías que propicien la preparación elemental de los alumnos en la seguridad informática.

Después de analizado el comportamiento de los indicadores de forma general, se puede inferir que en la constatación inicial se observan dificultades que limitan el efectivo desempeño de los alumnos del primer subgrupo del 7mo A en la seguridad informática de su escuela.

Introducción del sistema de actividades para la preparación de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero.

La constatación inicial se procedió a la aplicación de las actividades propuestas en el sistema de actividades, donde se realizan primeramente las dirigidas a crear las condiciones previas y el aseguramiento para su ejecución. Se efectúa el análisis del diagnóstico que posibilita el ajuste y selección de los contenidos. Se desarrolla tres conversatorios, dos charlas, dos talleres, una mesa redonda, para proporcionar y prácticos sobre la seguridad informática.

La autopreparación orientada antes, durante y después de los talleres se vinculó con la atención diferenciada, lo que facilitó la observación del actuar de los alumnos en las propias actividades desarrolladas.

Constatación final. (Post-test)

Al aplicar la entrevista a los alumnos sobre la seguridad informática con el objetivo de determinar los conocimientos y habilidades que poseen los mismos, así como las formas o vías que utilizan para prepararse, se pudo comprobar que el 94,11%, 16 de los alumnos de la muestra perteneciente ESBU Carlos J. Finlay del municipio Primero de Enero expresaron de manera correcta lo que es la seguridad informática.

Conocimientos sobre lo que es la seguridad informática	
Antes	**Después**
12%	**94,11%**

Existe conocimiento de la forma en cómo tener mi PC saludable, pues el 88,23% de los alumnos (15) explicaron de forma correcta cómo tener mi PC saludable.

Se aplicó una encuesta con el objetivo de determinar los conocimientos, habilidades, motivaciones y actitudes que poseen los alumnos del primer subgrupo del 7mo A de la ESBU Carlos J. Finlay del municipio Primero de Enero referido a la seguridad informática. En la misma se pudo comprobar que el 94,11% de los alumnos (16) saben cómo contribuir a la seguridad informática en el centro.

Se está preparando a los alumnos de manera elemental en la seguridad informática pues 15 alumnos, 88,23%, señalan de tres a cuatro opciones para prepararse en el tema antes señalado.

El 100% de los alumnos saben qué es la seguridad informática y continúan dispuesto a contribuir a la seguridad informática de su escuela y a que se les prepare en este tema.

Por lo que los indicadores quedan evaluados de la siguiente manera:

El indicador 1, quedó evaluado de Alto, pues 16 alumnos que representa el 94,11% expresaron de manera correcta lo que es la seguridad informática.
El indicador 2, quedó evaluado de Medio, pues 15 alumnos que representa el 88,23% explicaron de forma correcta cómo tener mi PC saludable.
El indicador 3, quedó evaluado de Alto, pues 16 alumnos que representa el 94,11% señalan que sí conocen lo que deben saber contribuir a la seguridad informática en el centro.
El indicador 4, quedó evaluado de Medio, pues 15 alumnos que representa el 88,23% señalan una, dos y tres opciones indistintamente para prepararse en el tema de la seguridad informática.
El indicador 5, quedó evaluado de Alto, pues el 100% de los alumnos saben cómo tener mi PC saludable.
El indicador 6, quedó evaluado de Alto, pues el 100% de los alumnos están dispuestos a contribuir a la seguridad informática en el centro.
El indicador 7, quedó evaluado de Alto, pues el 100% de los alumnos desean que lo preparen en el tema de la seguridad informática.

Potencialidades detectadas en los alumnos del primer subgrupo del 7mo A

- Conocen lo que es la seguridad informática.
- Poseen habilidades de cómo tener mi PC saludable.
- Están dispuesto a que se les prepare y a contribuir a la seguridad informática de en el centro.
- Los alumnos poseen dominio de elementos teóricos relacionados con la seguridad informática.
- Los alumnos contribuyen a la seguridad informática.
- Existe un diseño para la preparación elemental de los alumnos por parte de la escuela, para que puedan contribuir a la seguridad informática.

En el capítulo se pudieron determinar las necesidades de preparación de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay del municipio Primero de Enero en cuanto a la seguridad informática. A partir de ella se elaboró un sistema de actividades dirigida a la preparación elemental en la seguridad informática, al aplicarse se constató un estadío superior de preparación por parte de los alumnos, que permitió ponerlo en condiciones de contribuir a la seguridad informática en su escuela.

CONCLUSIONES

El análisis de la teoría revela que la preparación de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay en cuanto a la seguridad informática, constituye una necesidad para el sistema educativo cubano, ya que los mismos representan el mayor por ciento de los usuarios que acceden a la tecnología.

El diagnóstico del estado de la preparación elemental en la seguridad informática de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J.

Finlay, revela que es insuficiente el conocimiento que poseen sobre este tema, por lo que su contribución al correcto desarrollo de la misma en la escuela es limitado, produciendo en varios casos violaciones por desconocimiento del contenido que ella tiene implícita. La situación anterior condiciona la necesidad de abordar esta preparación a través de un sistema de actividades, que permita perfeccionar la preparación elemental en la seguridad informática en estos alumnos.

Proponer un sistema de actividades para la preparación elemental de los alumnos del primer subgrupo del 7mo A en la ESBU Carlos J. Finlay en cuanto a la seguridad informática, es una condición para propiciar esta elaboración. En ella se presentan contenidos sobre seguridad informática que hasta el momento no se habían empleado el en proceso docente educativo de la Educación Secundaria Básica.

El sistema de actividades diseñado demostró su efectividad en cuanto a la seguridad informática, al aplicarse se constató un estadío superior de preparación por parte de los alumnos, que permitió ponerlo en condiciones de contribuir a la misma en su escuela.

RECOMENDACIONES

Derivar otras actividades dirigidas a la Seguridad Informática para el desempeño de sus funciones, en las instituciones educacionales desde el proceso de enseñanza aprendizaje o extra curricular.

BIBLIOGRAFÍA

ADDINE FERNÁNDEZ, F. Diseño Curricular/ Fátima Addine Fernández [et. al.].-- La Habana: Instituto Pedagógico Latinoamericano y Caribeño, 1998 (material mimeografiado).

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

AMOROSO FERNÁNDEZ, YARINA. El Delito Informático, Conferencia Magistral Diplomado de Criminalística. La Habana. Cuba. 2002.

ANDERSON, JAMES P. Amenazas de seguridad informática de seguimiento y vigilancia. En http://www.sciencedirect.com/science.

ARAUJO GONZÁLEZ, R. Lecciones de Filosofía Marxista- Leninista/Rafael Araujo González [et. Al.]. _ La Habana: Ed. Pueblo y Educación, 1992.

ARREGOITIA LÓPEZ, SIURIA. Los llamados delitos informáticos; su regulación penal en cuba. En http//informática-juriidca.com

AÑORGA MORALES, J. Glosario de términos de Educación Avanzada. [CD ROM] La Habana; 2000.

ÁVILA ÁLVAREZ, REBECA. Sitio Web SegInf para perfeccionar el Sistema de Seguridad informática en las Direcciones Municipales de Educación. Tesis de Maestría en Ciencias de la Educación / Rebeca Ávila Álvarez. __ IPLAC. Las Tunas, 2009.

BIDOT, JOSÉ. "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.

_____. La seguridad Informática. Conferencia magistral, Diplomado de Criminalística. La Habana. Cuba, 2002.

BLANCO ENCINOSA, Lázaro J. "Apuntes para una historia de la Informática en Cuba.

BLANCO PÉREZ, ANTONIO. Filosofía de la Educación / Antonio Blanco Pérez _ Ciudad de la Habana: Ed. Pueblo y Educación, 2003.

_____. Introducción a la Sociología de la Educación / Antonio Blanco Pérez. _ La Habana: Ed. Pueblo y Educación, 2001.

CUBA FERNÁNDEZ, SANTIAGO. El proceso de las computadoras. Editora política. La Habana. Cuba 1993.

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

CASTRO RUZ, FIDEL. Discurso prenunciado por el comandante en jefe Fidel Castro Ruz en el Acto por los 15 años de los Joven Club de Computación, 7 de marzo de 2006.

_____. El robo de cerebros. Reflexiones. Periódico Granma. 17 de julio de 2007. La Habana. Cuba. 2007.

COLECTIVO DE AUTORES. Metodología de la investigación Educacional. Editorial Pueblo y Educación. La Habana. Cuba. 2002.

COLECTIVO DE AUTORES. Los detectives y la prevención de la criminalidad informática. Editora política. La Habana. Cuba. 2006.

COLECTIVO DE AUTORES. Plataforma Política para la Red del MINED. La Habana. Cuba. 2006.

CORDOVÉS RODRÍGUEZ, ENRIQUE. La prevención en los delitos informáticos. Ponencia. II taller Informática. La Habana. Cuba 2002.

Compendio de Pedagogía, La Habana: Editorial Pueblo y Educación, 2002.

CUÉLLAR, A. Nociones de Psicología General/ Antonio Cuéllar y Gerardo Roloff.__ Habana: Ed. Pueblo y Educación, 1977.

CHIRINO RAMOS, MARÍA V. Guías de Estudio 3er año. Metodología de la Investigación Educativa / MSc. María Victoria Chirino Ramos. _ Ciudad de la Habana: Ed Pueblo y educación. 2003.

DE ARMAS RAMÍREZ, NERELY. Caracterización y diseño de los resultados científicos como aportes de la investigación educativa. Curso 85 pre-evento Pedagogía 03 / Nerely de Armas Ramírez, José M. Perdomo Vázquez, Josefa Lorence González.--ISP.” Félix Varela”, Villa Clara, 2002.

DEL VALLE ALVAREZ, ACISCLO. Introducción a la Seguridad Informática/ Acisclo del Valle Álvarez [et.al.].__ Ciego de Ávila: Instituto Superior Pedagógico Manuel ascunce Domenech”, 2006 (material digital).

DOMÍNGUEZ MENDEJA, MAYLÉN. Bibliotecología y nuevas tendencias de la información, una era por definir a las puertas del nuevo milenio. La Habana. Cuba. 2003.

GABRIELA BRUNO, KARINA. Delitos Informáticos; necesidad de tipificación en el código penal. En http://falsificaciones.htm/yahoo.com.

GARCÍA BATISTA, GILBERTO. Compendio de Pedagogía / Gilberto García Batista. __ Ciudad de La Habana: Ed. Pueblo y Educación, 2003.

GARCÍA HERRERA, PEDRO. Incidencia del delito Informático. Trabajo de diploma, ISMI. La Habana. Cuba. 2002.

GARCÍA PIERRAT, GONZALO. Retos de las nuevas tecnologías. Un mundo diferente. Ponencia. Oficina de Seguridad para las Redes Informáticas. La Habana. Cuba. 2007.

GARNIER GALÁN JUAN C. La información y su papel en la Seguridad Nacional de la Información. La Habana. Cuba. 2006.

GONZÁLEZ MAURA, V. Psicología para educadores/ Viviana González Maura, Doris Castellano Simons.__ La Habana: Ed. Pueblo y Educación, 1995.

GRIJALBO. -- Gran Diccionario Enciclopédico Ilustrado. __México: El Grijalbo, 2000.

LEBLANCH PEÑA, ISABEL. "Sitio Web Educativo para desarrollar una cultura en Seguridad Informática en los Institutos Politécnicos de Informática de la Educación Técnica y Profesional". Tesis en opción al grado de Máster en Ciencias de la Educación. La Habana. 2008

MANSON MARCELO. Legislación sobre delitos informáticos en Argentina. En: http://www.segu-info.com.ar.

MENESES ESTRADA, AMAURY. Principales indicadores de vigilancia en interés de la seguridad informática.

XIII Edición de la Especialidad en Seguridad y Defensa Nacional. La Habana. Cuba. 2008.

NÚÑEZ PONCES, JULIO. Los delitos informáticos. En: http://publicaciones.derecho.org/redi/No.15_-_Octubre_de_1999.

PLA LOPEZ, RAMON. Concepción integradora para la Planificación, Control y Evaluación del trabajo de los Docentes a partir de sus funciones.

RAMIÓ AGUIRRE, JORGE: Desarrollo de la Seguridad Informática en España, su Incidencia en la Enseñanza Universitaria y CriptoRed". España. 1995.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RIBALTA, M, ALEJANDRO. Las Tecnologías de la Información y las Comunicaciones (TIC) en el Sistema Nacional de Educación y en la formación de docentes en la República de Cuba. VII Taller Internacional

Planeamiento, Administración y Supervisión Educativa. IPLAC: La Habana. Cuba. 2004.

RODRÍGUEZ CUERVO, ALEJANDRO M. Acercamiento al surgimiento y desarrollo de la seguridad informática. En http://www.rimed.cu

RODRÍGUEZ FERNÁNDEZ, ELZABET. La Seguridad Informática: Condición indispensable para la preservación de las Tecnologías de la Información en la provincia de Las Tunas. Tesis en opción al grado de Máster en Ciencias Jurídicas. Las Tunas. Cuba. 2006.

TELLEZ VALDÉS, JULIO. Derecho Informático. Segunda Edición. Editorial McGraw-Hill. México. 1997.

UNJC. Relatoría del III Congreso sobre Derecho e Informática, La Habana. Cuba. 2003.

VALDÉS DOMÍNGUEZ, MARTA. Los Delitos Informáticos a la luz del Siglo XXI. Revista Betsime. La revista del empresario cubano. La Habana. Cuba. 2006.

VALDÉS MENÉNDEZ RAMIRO. Informatización de la sociedad cubana I y II partes. En la Revista GIGA, Nro. 3 y 4 de 1997. La Habana. Cuba. 1997.

VIGOTSKY, L. S. Pensamiento y Lenguaje / Lev S. Vigotsky. _ Ciudad de La Habana: Ed. Pueblo y Educación, 1998.

_____. Obras Completas V/ L. S. Vigotsky, La Habana: Editorial Pueblo y Educación, 1989.

ZALDIVAR VÁZQUEZ, JESÚS A. La seguridad Informática y el Delito. Ponencia TECNICRIM. p27. 2000. La Habana. Cuba. 2000

ZERGUERA RAMOS, PABLO. Seguridad Informática. Ponencia digital. Segurmática. La Habana. Cuba. 2007.

ANEXO 1

GUÍA DE OBSERVACIÓN

Objeto de la observación: Medir los conocimientos que poseen los alumnos en cuanto a la seguridad informática.

Objetivos de la observación: Determinar los conocimientos en la seguridad informática de los alumnos.

Cantidad de observadores: 1

Tiempo total y frecuencia de las observaciones: 1 mes.

Tipo de observación: Participante.

Lugar en que se realiza la observación: Laboratorio de Computación de la ESBU Carlos J. Finlay del municipio Primero de Enero.

Aspectos a observar en la unidad de investigación:

- Empleo de las tecnologías.
- Cuidado de las tecnologías.
- Uso del registro de acceso a las tecnologías.
- Actualización del plan de seguridad informático.

ANEXO 2

ENTREVISTA A LOS ALUMNOS

Objetivo: Determinar los conocimientos, habilidades y motivaciones que poseen los alumnos de la ESBU Carlos J. Finlay en cuanto la seguridad informática.

Consigna: Estudiante, necesitamos su colaboración en la realización de la siguiente entrevista.

1. ¿Qué entiendes por seguridad informática?
2. ¿Qué es un virus informático?
3. ¿Cómo puedes contribuir a que exista en el centro una buena seguridad informática?

ANEXO 3

ENCUESTA A LOS ALUMNOS

Objetivo: Determinar los conocimientos, habilidades y motivaciones que poseen los alumnos de la ESBU Carlos J. Finlay en cuanto la seguridad informática.

Consigna: Estimado Estudiante, necesitamos su colaboración en el llenado de este instrumento, solicitamos que nos exprese con sinceridad su opinión sobre este tema.

1. ¿Sabes lo que es la seguridad informática?

__Si ___No

2. ¿Conoces lo que es un virus informático?

__Si ___No

2. ¿Te ha hablado tu maestro de Computación sobre la seguridad informática?

__Si ___No

3. ¿Te gustaría conocer lo que es la seguridad informática?

__Si ___No

ANEXO 4

ENTREVISTA A LOS ALUMNOS

Objetivo: Determinar los conocimientos y habilidades que poseen los alumnos de la ESBU Carlos J. Finlay del municipio Primero de Enero referido a la seguridad informática, así como las formas o vías que utiliza para prepararse.

Consigna: Alumnos, necesitamos su colaboración, solicitamos que exprese con sinceridad su opinión sobre este tema.

1. Expresa qué es para ti la seguridad informática.
2. Explica cómo puedes tener mi PC saludable.

ANEXO 5

ENCUESTA A LOS ALUMNOS DURANTE EL DESARROLLO DEL (PRE-TEST Y EL POS-TEST)

Objetivo: Determinar los conocimientos, habilidades, motivaciones y actitudes que poseen los alumnos de la ESBU Carlos J. Finlay del municipio Primero de Enero referido a la seguridad informática.

Consigna: Estimado alumno, necesitamos su colaboración en el llenado de este instrumento, solicitamos que nos exprese con sinceridad su opinión sobre este tema.

1. Conoces qué debes hacer para contribuir a la seguridad informática en el centro.

___Sí ___ No

2. Señala con una x las formas en qué te preparas en el tema de la seguridad informática.

__ Tiempo de máquina.

__ Clase de Computación.

__ Charlas.

__ Conversatorios.

3. ¿Sabes cómo tener mi PC saludable?

___Sí ___ No

4. ¿Estás dispuesto a contribuir a la seguridad informática en el centro.

?

___Sí ___ No

5. ¿Deseas que te preparen en el tema de la seguridad informática?

___Sí ___ No

ANEXO 6

METODOLOGIA PARA LA EVALUACION DE LOS INDICADORES

El indicador 1 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos expresan correctamente lo que es la seguridad informática.

Medio: Si entre el 89% y el 59% de los alumnos expresan correctamente lo que es la seguridad informática.

Bajo: Si entre el 58% y el 1% de los alumnos expresan correctamente lo que es la seguridad informática, o si no expresan lo que es la seguridad informática.

El indicador 2 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos explican cómo pueden tener mi PC saludable.

Medio: Si entre el 89% y el 59% de los alumnos explican cómo pueden tener mi PC saludable.

Bajo: Si entre el 58% y el 1% de los alumnos explican cómo pueden tener mi PC saludable, o no explican cómo pueden tener mi PC saludable.

El indicador 3 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos señalan que sí conocen lo que deben saber para contribuir a la seguridad informática en. el centro.

Medio: Si entre el 89% y el 59% de los alumnos señalan que sí conocen lo que deben saber para contribuir a la seguridad informática en el centro.

Bajo: Si entre el 58% y el 1% de los alumnos señalan que sí conocen lo que deben saber para contribuir a la seguridad informática en el centro, o señalan que no conocen lo que deben saber para contribuir a la seguridad informática en el centro.

El indicador 4 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos señalan con una x a las cuatro opciones que se les presentan para prepararse en el tema de la seguridad informática.

Medio: Si entre el 89% y el 59% de los alumnos señalan con una x, tres, dos opciones o al menos una que se les presentan para prepararse en el tema de la seguridad informática.

Bajo: Si entre el 58% y el 1% de los alumnos no señalan ninguna de las opciones que se les presentan para prepararse en el tema de la seguridad informática.

El indicador 5 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos señalan con sí saben tener mi PC saludable.

Medio: Si entre el 89% y el 59% de los alumnos señalan con sí saben tener mi PC saludable.

Bajo: Si entre el 58% y el 1% de los alumnos señalan con sí saben tener mi PC saludable, o el 100% o menos señalan que no saben tener mi PC saludable.

El indicador 6 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos están dispuestos a contribuir a la seguridad informática en el centro.

Medio: Si entre el 89% y el 59% de los alumnos están dispuestos a contribuir a la seguridad informática en el centro.

Bajo: Si entre el 58% y el 1% de los alumnos están dispuestos a contribuir a la seguridad informática en el centro o no lo están.

El indicador 7 será evaluado de:

Alto: Si entre el 100% y el 90% de los alumnos desean que lo preparen en el tema de la seguridad informática.

Medio: Si entre el 89% y el 59% de los alumnos desean que lo preparen en el tema de la seguridad informática.

Bajo: Si entre el 58% y el 1% de los alumnos desean que lo preparen en el tema de la seguridad informática o no desean que los prepare.

ANEXO 7

Mesa redonda

Título: ¿Cómo puedo ayudar?

Objetivo: Valorar la forma de contribuir a la seguridad informática del laboratorio.

Contenido:

Formas o vías en las que puede contribuir el alumno a la seguridad informática en el centro.

Tiempo previsto: 2 horas.

Desarrollo

Formas o vías en las que puede contribuir el alumno a la seguridad informática de su centro.

- Preparándose en el tema de la seguridad informática.
- Llenar con sus datos el registro de acceso al local.
- Cuidando la limpieza del local y computadoras.
- Proteger a las computadoras.
- Cómo tener mi PC saludable sistemáticamente las computadoras y los soportes externos que se pongan en ella.

Cumpliendo las normas de ética del laboratorio del centro.

ANEXO 8

Taller 1

Título: Cómo tener mi PC saludable.

Objetivo: Determinar lo que es un virus, antivirus y la importancia de cómo tener mi PC saludable y la forma de hacerlo.

Contenido: ¿Qué es un virus? ¿Qué es un antivirus? Algunos tipos de antivirus. Forma de tener mi PC saludable.

Tiempo previsto: 2 horas.

Desarrollo:

Un virus informático es un programa o software que se auto ejecuta y se propaga. Se adjunta a un programa o archivo de forma que pueda propagarse, infectando los ordenadores. Como los virus humanos, los virus de ordenador pueden propagarse en gran medida: algunos virus solo causan efectos ligeramente molestos mientras que otros pueden dañar tu hardware, software o archivos. Es importante observar que un virus no puede continuar su propagación sin la acción humana.

¿Cómo eliminar un virus informático?

Es fundamental contar con un antivirus correcto instalado y actualizado en el equipo para protegerse de ataques no deseados o software mal intencionado.

Los Antivirus: son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación.

Algunos tipos de antivirus. NOD 32, KASPERSKY, PANDA, SAV 32, AVIRA

Forma de tener mi PC saludable y su actualización.

Se da doble clic en el icono que representa el antivirus en la barra de tareas, en este caso el Kaspersky que es el que está establecido para el centro cubana, un clic en Análisis del ordenador y luego Análisis estándar para tener mi PC saludable completa y si se desea vacunar parte de ella en específico, dar clic en Análisis inteligente y escoger la unidad en riesgo y dar clic en Analizar. Cuando acabe de analizar o escanear la unidad deseada, dar clic en el menú Herramienta y seleccionar la opción Cuarentena.

Si existe algún virus, con un clic derecho, sale un menú contextual, donde se le da clic en eliminar de la cuarentena.

ANEXO 9

Taller 2

Título: Cómo cuido mi laboratorio.

Objetivo: Profundizar en los registros de controles que deben existir en el laboratorio de Computación.

Contenido:

- Registros de la seguridad informática.
- Importancia del control en el laboratorio de Computación.

Tiempo previsto: 2 horas.

Desarrollo:

Es importante que los alumnos sepan que en el laboratorio su profesor debe llevar como controles varios registros y que además en uno de ellos deben plasmar la firma todos los usuarios que acceden a la tecnología.

En el centro existirán los siguientes registros

Registro No. 1 Software Autorizado.

Registro No. 2 Mantenimientos a equipos y soportes.

Registro No. 3 Inspecciones

Registro No 4 Control de los soportes

Registro No 5 Registros de software de nueva adquisición.

Registro No 6 Registros de acceso a las áreas.

Registro No 7 Entrada, salida y movimiento de tecnologías de información.

Registro No 8 Incidencias de la Seguridad informática

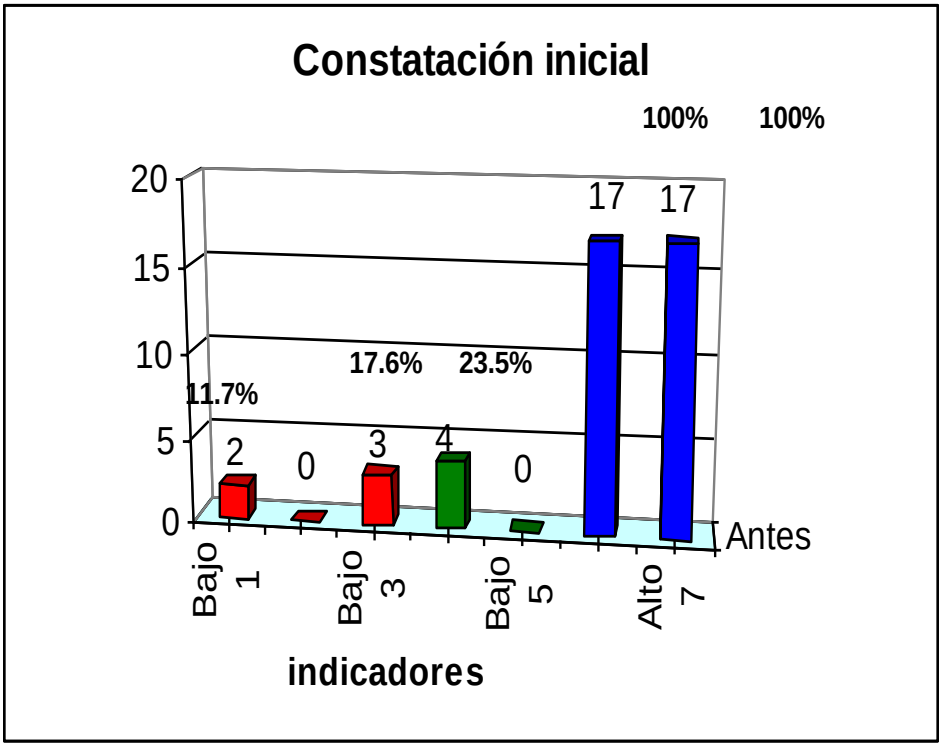
Registro No 9 Acceso a Los sistemas informáticos.

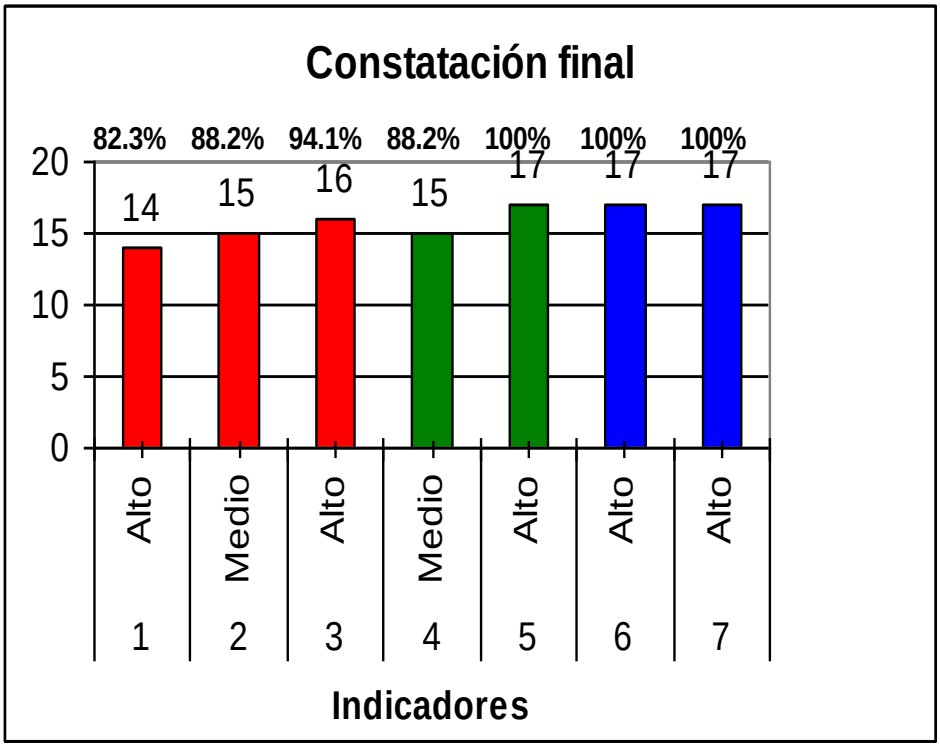
Registro No. 10-A Registro de Control de Acceso a Los sistemas informáticos fuera del Horario Laboral.

Importancia del control en el laboratorio de Computación.

Ante una incidencia en el laboratorio los controles aportaran datos importantes de los posibles usuarios que le han hecho daño a las computadoras o a la información que contiene la misma.

Anexos:


Constatación inicial
100%
100%
20
15
10
5
0
17
17
17.6%
23.5%
11.7%
2
0
3
4
0
Antes
Bajo
1
Bajo
3
Bajo
5
Alto
7
indicadores


Constatación final
82.3%
88.2%
94.1%
88.2%
100%
100%
100%
20
15
10
5
0
14
15
16
15
17
17
17
Alto
Medio
Alto
Medio
Alto
Alto
Alto
1
2
3
4
5
6
7
Indicadores