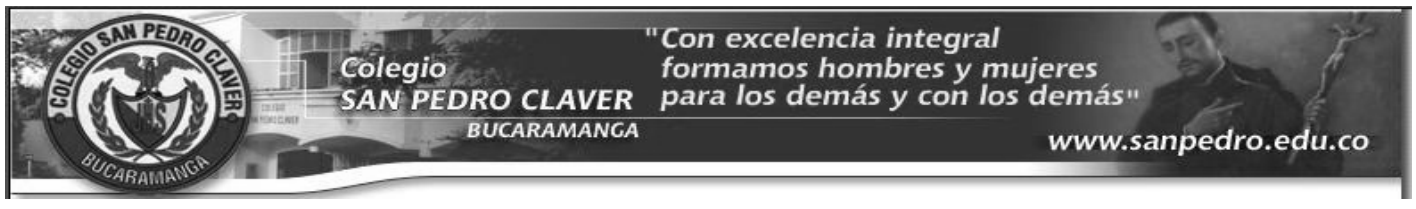

AREA DE EDUCACION EN TECNOLOGIA E INFORMATICA
SEXTO - 2010
Docente: John Bohórquez Jiménez

Claverian@ _____ Curso: _____ Fecha: _____

Guía 1: Ética de la Informática

Indicador 1: Reconoce las implicaciones éticas sobre el uso de la información y su influencia en el desarrollo de la humanidad.	

Criterio: Capacidad argumentativa.
Instrumento: Taller de aplicación Nº 1 **Fecha:**
Observaciones:

Indicador 2: Muestra recursividad y creatividad en el procesamiento de la información.	

Criterios: Creatividad, Trabajo colaborativo
Instrumento: Taller de aplicación Nº1 **Fecha:**
Observaciones:

ACTIVIDADES

1. Reúnase con dos (2) compañeros para analizar los casos sobre la ética informática que se encuentran al reverso de la hoja, donde se presentan situaciones de uso inadecuado de las Tics. En su hoja de trabajo de forma personal, tome nota de las ideas más importantes.
2. Participe en la puesta en común para que comparta con sus compañeros sus apreciaciones.
3. Lea el documento de apoyo "Delitos informáticos: mal uso de Tecnologías de Información y Comunicación", que será suministrado en archivo digital por el profesor y exprese por escrito su opinión.

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____

4. Desarrolle el Taller Nº 1 (Anexo 1: Ética Informática)
5. Participe en la puesta en común para que comparta con sus compañeros sus apreciaciones.
6. Atienda a la lectura que hará el profesor sobre "Delitos Informáticos en Colombia". Luego responda en su hoja de trabajo los siguientes cuestionamientos:
   - ¿Cómo influye la Ética informática en la autoestima de una persona?
   - ¿Será ético cargar a la WWW un video que no es de su propiedad?
   - ¿Conoce el castigo al que se somete una persona cuando comete un delito informático en Colombia?
   - Cuando utiliza cualquier medio de comunicación (verbal, escrito, virtual), ¿cómo vive o promueve la ética? Explique.
7. Reúnase con un compañero para elaborar un código ético tomando como base, por ejemplo, los diez mandamientos del Instituto de Ética e informática. Luego consígnenlo en una cartelera (que será ubicada en el laboratorio de informática 2) para promover el uso correcto de la tecnología en nuestro colegio y sociedad.

LOS DIEZ MANDAMIENTOS DE LA ÉTICA INFORMÁTICA

"No usarás un computador para dañar a otros.
No interferirás con el trabajo ajeno.
No indagarás en los archivos ajenos.
No utilizaras un computador para robar.
No utilizarás la informática para realizar fraudes.
No copiarás o utilizarás software que no hayas comprado.
No utilizarás los recursos informáticos ajenos sin la debida autorización.
No te apropiarás de los derechos intelectuales de otros.
Deberás evaluar las consecuencias sociales de cualquier código que desarrolles.
Siempre utilizarás los computadores de manera de que respetes los derechos de los demás".

ALGUNOS CASOS DE ESTUDIO SOBRE DELITOS INFORMATICOS

Zinn, Herbert, Shadowhack.
Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de «Shadowhawk», fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenía 16 y 17 cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen.

Poulsen Kevin, Dark Dante.
Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de «Dark Dante» en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar america na. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.
Siguió el mismo camino que Kevin Mitnick, pero es más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a «ganar» un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue.
Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional.
Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente «reformado». Que dicho sea de paso, es el mayor tiempo de estancia en la cárcel que ha comparecido un hacker.

Murphy Ian, Captain Zap.
En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba «Captain Zap», gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.
En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como «Captain Zap,».
Mostró la necesidad de hacer más clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenía acceso a órdenes de mercancías, archivos y documentos del gobierno. «Nosotros usamos los a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados» Explico Murphy. «El violar accesos nos resultaba muy divertido». La Banda de hackers fue finalmente puesta a disposición de la ley». Con cargos de robo de propiedad, Murphy fue multado por US $1000 y sentenciado a 2 ½ años de prueba.

Morris Robert.
En noviembre de 1988, Morris lanzo un programa «gusano» diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dólares. Se creó el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad.

TEXTO TOMADO DE **http://www.mailxmail.com/curso-delitos-informaticos/casos-impacto-delitos-informaticos**