
	INSTITUCIÓN EDUCATIVA LOS GÓMEZ <i>“Pensando en las futuras generaciones, construimos hoy; conocimiento, respeto y democracia”</i>	 CO-SC-CER352434
CÓDIGO DP-FO-09	PLAN DE APOYO	VERSIÓN: 4

FECHA: noviembre -2017

PERIODO: Quinto periodo

GRADO: sexto

DOCENTE: Samuel Cardona

AREA: tecnología

NOMBRE DEL ESTUDIANTE: _____

• **LOGRO O LOGROS NO ALCANZADOS DURANTE EL PERÍODO:**

- Aplicación y sistematización de estrategias para la solución de problemas tecnológicos e informáticos frente al medio ambiente.
- Identificación de delitos informáticos y funciones de acuerdo con los sistemas tecnológicos.
- Análisis y aplicación de las normas de seguridad que se deben tener en cuenta para el uso de algunos artefactos, productos y sistemas tecnológicos

• **PRESENTACIÓN DEL TRABAJO:**

El taller debe entregarse, en las fechas establecidas, en hojas de block (limpio y ordenado) a mano y prepararse para la socialización o sustentación en forma oral o escrita según fechas asignadas. Se calificara de la siguiente manera:

Presentación: 30%

Sustentación: 70%


TALLER A DESARROLLAR:

1. Lectura de texto
2. Responder las preguntas alusivas a la lectura

Lectura:

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.



No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello,

	INSTITUCIÓN EDUCATIVA LOS GÓMEZ <i>“Pensando en las futuras generaciones, construimos hoy; conocimiento, respeto y democracia”</i>	 CO-SC-CER352434
CÓDIGO DP-FO-09	PLAN DE APOYO	VERSIÓN: 4

durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

- **Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.** *El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- **Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.** *El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*
- **Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.** *El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.*
- **Artículo 269D: DAÑO INFORMÁTICO.** *El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- **Artículo 269E: USO DE SOFTWARE MALICIOSO.** *El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- **Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.** *El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
- **Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.** *El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.*

	INSTITUCIÓN EDUCATIVA LOS GÓMEZ <i>“Pensando en las futuras generaciones, construimos hoy; conocimiento, respeto y democracia”</i>	 CO-SC-CER352434
CÓDIGO DP-FO-09	PLAN DE APOYO	VERSIÓN: 4

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006.

SEGURIDAD INFORMÁTICA

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos.

Seguridad con respecto a la naturaleza de la amenaza

Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

- * Seguridad lógica: aplicaciones para seguridad, herramientas informáticas.
- * Seguridad física: mantenimiento eléctrico, anti-incendio, humedad.

Amenazas a un sistema informático

Amenazas a la seguridad de un sistema informático o computadora:

- * Programas malignos: virus, espías, troyanos, gusanos, phishing, spamming.
- * Siniestros: robos, incendio, humedad. pueden provocar pérdida de información.
- * Intrusos: piratas informáticos pueden acceder remotamente (si está conectado a una red) o físicamente a un sistema para provocar daños.
- * Operadores: los propios operadores de un sistema pueden debilitar y ser amenaza a la seguridad de un sistema no sólo por boicot, también por falta de capacitación o de interés.

Implementación de barreras de seguridad

Técnicas, aplicaciones y dispositivos para la seguridad informática:

- * Utilización de aplicaciones de protección: cortafuegos, antivirus, antiespías.
- * Encriptación de la información y uso de contraseñas.
- * Capacitación a los usuarios de un sistema.
- * Capacitación a la población general sobre las nuevas tecnologías y las amenazas que pueden traer. Ver analfabetismo informático.

I. cuestionario a responder.

	<p>INSTITUCIÓN EDUCATIVA LOS GÓMEZ <i>“Pensando en las futuras generaciones, construimos hoy; conocimiento, respeto y democracia”</i></p>	 CO-SC-CER352434
CÓDIGO DP-FO-09	PLAN DE APOYO	VERSIÓN: 4

1. A que hace referencia la ley 1273 del 2009.
2. Que delitos se pueden considerar delitos informáticos.
3. A que hace referencia el artículo 269 en cada uno de sus ítems.
4. A que hace referencia el delito llamado “phishing”
5. Que se entiende por seguridad informática.
6. Se puede lograr un ciento por ciento de sistema de informático seguro.
7. Como se puede dividir la seguridad informática de acuerdo a la amenaza.
8. Como se puede subdividir la seguridad informática por amenaza.
9. Que barreras de seguridad se pueden implementar para la seguridad informática.
10. Realiza un mapa conceptual de las diferentes amenazas informáticas.
11. Cuáles de los anteriores sistemas de seguridad te han causado mayores molestias.
12. Investiga a que hace referencia la IP en un computador. **BIBLIOGRAFÍA**

La tecnología y el medio ambiente: Desde los tiempos prehistóricos las personas han obtenido recursos para cazar, protegerse, etc., de la naturaleza. La naturaleza es capaz de renovar muchos recursos naturales si se consumen a un ritmo adecuado, pero otros recursos no pueden renovarse. Por ejemplo, el petróleo y el carbón tardan en formarse millones de años. Sin embargo, desde la época de la Revolución Industrial, las personas hemos consumido la mayor parte de las reservas mundiales de estos combustibles fósiles.

Durante mucho tiempo las necesidades industriales y tecnológicas se han satisfecho sin prestar atención a los posibles daños causados al medio ambiente. Ahora parece que al menos se conocen estos daños; sólo falta poner los medios a nuestro alcance para evitarlos.

Problemas medioambientales provocados por las actividades tecnológicas

Las actividades humanas, desde la obtención de una materia prima, hasta el desecho de los residuos generados tras la obtención de un producto tecnológico, pueden tener consecuencias nefastas para la conservación del medio ambiente. Algunos ejemplos son la desertización, el impacto medioambiental de las obras tecnológicas, la contaminación producida en la obtención y tratamiento de muchas materias primas o de fuentes de energía y los residuos generados en muchas actividades industriales.

Impacto ambiental directo: La ejecución de obras públicas (carreteras, pantanos, etc.) y las explotaciones mineras modifican el ecosistema en el que habitan muchas especies animales y vegetales. Estas obras pueden separar las poblaciones de ambos lados de la carretera, vía férrea, etc.

Desertización: Cada año aumenta la superficie desértica del planeta. Esto da lugar a un empobrecimiento general del suelo, lo que perjudica las actividades agrícolas y ganaderas de la región afectada.

	<p>INSTITUCIÓN EDUCATIVA LOS GÓMEZ <i>“Pensando en las futuras generaciones, construimos hoy; conocimiento, respeto y democracia”</i></p>	 CO-SC-CER352434
CÓDIGO DP-FO-09	PLAN DE APOYO	VERSIÓN: 4

Contaminación: Quizá sea el efecto más apreciable. El incremento en el consumo de energía ha hecho que aumenten considerablemente las proporciones de determinados gases (dióxido de carbono, óxidos de azufre, etc.) en la atmósfera, sobre todo cerca de las áreas industrializadas. Algunas consecuencias de la contaminación del aire son el calentamiento global del planeta debido al efecto invernadero o la disminución en el grosor de la capa de ozono.

Generación de residuos. Determinadas actividades tecnológicas generan residuos muy

Contaminantes que resultan difíciles de eliminar, como algunos materiales plásticos o los residuos nucleares.

Los accidentes de petroleros tienen unas consecuencias nefastas para el entorno marino en el que tienen lugar. Las mareas negras producidas pueden dañar considerablemente a las

La tecnología al servicio del medio ambiente

La ciencia y la tecnología pueden servir para ayudar a la conservación del medio ambiente. Algunos ejemplos son la predicción de incendios forestales, el reciclaje de determinados materiales o la utilización de fuentes de energía alternativas.

La predicción y la extinción de incendios forestales se llevan a cabo mediante satélites artificiales. Los modernos métodos de detección permiten advertir la presencia de incendios poco tiempo después de producirse.

- El reciclaje de determinados productos, como el vidrio, el papel, etc., puede evitar la sobreexplotación de algunas materias primas (madera, etc.).
- Las fuentes de energía renovables, como la energía solar, la eólica o la geotérmica no se agotan y, en general, contaminan menos que las fuentes no renovables, como el carbón o el petróleo.

Es decir la tecnología en general, en la que está incluidas tecnologías de la informática, las comunicaciones, y la industria en general, no han escatimado esfuerzo para poder desarrollarse rápidamente, pero en la mayoría de los casos, a costa del deterioro del medio ambiente en los que estamos incluidos nosotros como seres humanos.

Con esto, la naturaleza está enfermando de muerte y nosotros con ella. Pero si comenzamos a tomar conciencia sobre lo que está sucediendo o de lo que estamos dejando de hacer para protegerla, en la actualidad nosotros tenemos una gran variedad de herramientas tecnológicas que pueden facilitar los esfuerzos ecológicos.

Al final solo puedo decir que si ponemos al servicio de la naturaleza toda la tecnología existente, ejm los satélites, podemos realizar una monitorización de nuestra querida madre tierra, y trabajar para protegerla.

	<p>INSTITUCIÓN EDUCATIVA LOS GÓMEZ <i>“Pensando en las futuras generaciones, construimos hoy; conocimiento, respeto y democracia”</i></p>	 CO-SC-CER352434
CÓDIGO DP-FO-09	PLAN DE APOYO	VERSIÓN: 4

Una de las características que diferencian al hombre como ser racional o como "homo sapiens" de los demás seres de la creación, es su capacidad de lograr inventos. Desde los comienzos de la aparición del hombre, éste se ha esforzado por realizar elementos que hagan más fáciles algunas tareas, o que resuelvan problemáticas que se les presentaban y a las que había que buscarles una solución.

Los primeros inventos fueron elementos realizados en piedra, toscos y rústicos, los que fueron evolucionando a través de los tiempos.

La invención más grande -según mi punto de vista- que ha logrado el hombre desde sus comienzos, antes de la documentación histórica, es el sistema de signos para comunicarse: el lenguaje.

2 cuestionarios a responder.

- 1-Responder las preguntas alusivas a la lectura
2. Que acciones debes hacer para cuidar el medio ambiente?
3. Como incide la tecnología en el medio ambiente?
4. Cuál es el impacto de la tecnología en el medio ambiente?
5. Como ayuda la tecnología al servicio Del medio ambiente?
6. Que recomendaciones les harías a las personas para obtener el 7equilibrio entre tecnología y medio ambiente?
8. ¿Porque el hombre resuelve hacer inventos?
8. ¿Que motiva al hombre a descubrir o inventar objetos?
10. ¿Para la humanidad son importantes los inventos y/o los descubrimientos? ¿Por qué.