

INSTITUTO NACIONAL DE JUAYUA

MATERIA: INFORMATICA 2021

PROFESOR: JAIRO JOSUE GARCIA MENDEZ

Guía de trabajo 3, 4 y 5

duración: 2 semanas

06/03/2021

UNIDAD UNO: La naturaleza de las TIC y elaboración de proyectos

Objetivo: identificar los delitos cibernéticos que se desarrollan en internet o requieren del uso de medios informáticos.

Indicación: realiza por medio de la información brindada por la guía las siguientes preguntas y ejercicios proporcionados por el docente.

ACTIVIDAD:

Guía 3

- ✚ Desarrolla la lectura y conoce e identifica los conceptos básicos.
- ✚ Lectura de la presentación de apoyo en PowerPoint.
- ✚ Subraya con marcador las palabras que no conoces su significado y búscalo en la web.
- ✚ Ver los enlaces Link que aparecen en cada uno de los temas representado por cortometraje.

Guía 4

- ✚ Responde el cuestionario de ciberdelitos.

Guía 5

“Tarea virtual desde casa”

- ✚ Realizar una presentación en Microsoft Power Point o una video presentación, en la aplicación de tu preferencia de todos los temas de ciberdelitos.
- ✚ Si no tiene acceso a una computadora hacer la presentación en pedazos de cartulina, esquemas, páginas de papel bond o en el cuaderno de forma clara y ordenada.
- ✚ Puedes informarte en otros sitios web para fortalecer conocimientos.
- ✚ Puedes transcribir la información resumida en tu cuaderno, para sustentar la temática.

Ultimo día de entrega: lunes 22 de marzo 2021

Guía #3

Delitos cibernéticos, ¿qué son?

En este sentido, los delitos cibernéticos son todos aquellos actos o hechos que, estando tipificados como delitos, se desarrollan en internet o requieren del uso de medios informáticos para ser realizados.

Una parte muy importante de los «delitos de toda la vida» también pueden ser delitos cibernéticos desde el preciso instante que se tienen lugar en internet, haciendo uso de internet y/o empleando hardware o software para ello.

¿CUÁLES SON LOS CIBERDELITOS MÁS COMUNES?

Qué es el ciberacoso

El ciberacoso es el acoso que tiene lugar en dispositivos digitales, como teléfonos celulares, computadoras y tabletas. El ciberacoso puede ocurrir mediante mensajes de texto, textos y aplicaciones, o bien por Internet en las redes sociales, foros o juegos donde las personas pueden ver, participar o compartir contenido. El ciberacoso incluye enviar, publicar o compartir contenido negativo, perjudicial, falso, o cruel sobre otra persona. Esto puede incluir compartir información personal o privada sobre alguien más, provocándole humillación o vergüenza. Algunos acosos por Internet pasan a ser un comportamiento ilegal o criminal.

Los lugares más comunes donde ocurre el ciberacoso son:

Redes sociales, como Facebook, Instagram, Snapchat y Twitter

SMS (servicio de mensajes cortos), también conocidos como mensajes de texto, enviados a través de dispositivos

Mensajería instantánea (a través de dispositivos, servicios de proveedores de email, aplicaciones y funciones de mensajería de las redes sociales) email

Video de youtube: <https://www.youtube.com/watch?v=tVAjyNzYq0>

Cyberbullying.

El ciberacoso es el uso de los medios telemáticos para ejercer el acoso psicológico entre iguales. No se trata aquí del acoso de índole estrictamente sexual.

Estamos ante un caso de cyberbullying cuando un menor atormenta, amenaza, hostiga, humilla o molesta a otro mediante internet, teléfono móvil, consolas de juegos u otras tecnologías telemáticas.

Según el Estudio sobre hábitos seguros en el uso de las TIC por los menores, publicado por INTECO en marzo de 2009, el cyberbullying se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

Video de youtube: <https://www.youtube.com/watch?v=-yOZ-QgZXBc>

Revenge Porn.

Este delito está estrechamente ligado al sexting, una mala práctica muy extendida entre menores de edad. El Revenge Porn (o porno vengativo) es el contenido sexual explícito que se publica en internet sin el consentimiento del individuo que aparece representado. Mucho de este material es producido por la propia víctima y enviado al infractor a través de canales como Whatsapp.

La pornografía vengativa, al someter a la víctima en una situación de exposición no consentida de su sexualidad, se considera como violencia sexual, aunque no sea física, sino psicológica.

Video youtube : https://www.youtube.com/watch?v=s_O1FIEc1xk

Grooming.

Se trata de una serie de conductas y acciones emprendidas por un adulto con el objetivo de ganarse la confianza de un menor de edad, creando una conexión emocional con el fin de disminuir las inhibiciones del menor y poder abusar sexualmente de él.

En algunos casos se puede buscar la introducción del menor a la prostitución infantil o a la producción de material pornográfico.

Video de youtube: <https://www.youtube.com/watch?v=Pa2ttVRA-xU>

Pharming.

Es la explotación de una vulnerabilidad en el software de los servidores DNS (o en el de los equipos del propio usuario) que permite al atacante redirigir un nombre de dominio a otra computadora distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para el nombre de este dominio.

Video de youtube: <https://www.youtube.com/watch?v=Mr-osgLJ0N4>

Phishing.

O suplantación de identidad es el modelo de abuso informático que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. El ciberdelincuente, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.

Video de youtube: <https://www.youtube.com/watch?v=3jJVIsHlzW0>

Sextortion la red elegida por las organizaciones internacionales es Facebook, a través de un perfil falso o Fake comienza un chat que ofrece una videollamada erótica e invita a los participantes a mostrarse con poca ropa, cuándo lo logra se corta la cámara y comienza la extorsión acompañada por frases del tipo "si no querés que se vea este video tenés que depositar cierta suma de dinero en la siguiente cuenta" por lo general son transacciones económicas a países inusuales.

Video youtube: <https://www.youtube.com/watch?v=sVqeJXhF6OA>

¿en qué consiste el sexting?

Las primeras referencias del sexting provienen de los países anglosajones. El término sexting proviene del "sex" sexo; y "texting" envío de mensajes de texto por SMS desde teléfonos móviles o smartphones.

Hoy en día, resulta evidente que con la proliferación de aplicaciones, redes sociales y demás mecanismos de transmisión de documentos e imágenes desde cualquier dispositivo, el concepto se amplía en toda acción de difusión o publicación de contenidos (principalmente fotos o vídeos) de tipo sexual generado de manera voluntaria por su autor a través de cualquier dispositivo tecnológico, sin el consentimiento de la persona afectada.

Pero ¿qué conductas constituyen el delito de sexting?

El artículo 197.7 del Código Penal recoge esta nueva figura delictiva en los siguientes términos:

"Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona".

Así la conducta típica viene delimitada por los verbos difundir, revelar y ceder; verbos que hacen referencia a la transmisión de contenido íntimo que afecte gravemente la intimidad de la persona afectada; más allá de los límites consentidos ente el primer emisor y la persona que comete la acción típica.

Como elementos del delito tenemos:

Difundir, revelar y ceder fotos, imágenes o cualquier material de contenido íntimo sin autorización de la persona afectada.

Dicho contenido debe afectar gravemente la intimidad personal de la persona.

Dichos contenidos los ha obtenido el autor con la anuencia de la persona afectada.

Son contenidos captados en el domicilio de la víctima o en cualquier lugar donde exista una previsión de intimidad.

Video de youtube: <https://www.youtube.com/watch?v=UIKpHkKEy5U>
<https://www.youtube.com/watch?v=qjVRDI5YMPA>



Los Delitos Cibernéticos en El Salvador

El uso del internet y de las tecnologías de la información es una vía directa para cometer delitos cibernéticos.

En muchos países no existe regulación relativa a las tecnologías de la información y de las comunicaciones. Como resultado, esto crea una falsa sensación de anonimato e impunidad, por lo que facilita que las personas piensen que su actuar no es detectable, y mucho menos perseguible.

Casos de delitos cibernéticos

El uso del internet y las tecnologías de la información son parte del día a día, y su abuso también. Innumerables extorsiones se cometen valiéndose de celulares, a través de aplicaciones para "chatear" que precisan del internet. Igualmente, entre los adolescentes, agresiones físicas son documentadas y difundidas por medio de las redes sociales. Se cometen delitos contra el honor e imagen de las personas al creer que existen límites a su libertad de expresión en la web.

La lista de los posibles delitos va desde el Hurto de la Identidad, hasta Violación de Signos Distintivos y la Obtención y Transferencia de Información de Carácter Confidencial.

Ley contra delitos cibernéticos en El Salvador

La Ley Especial Contra Delitos Informáticos y Conexos vigente en El Salvador, es de los primeros intentos del país de sancionar a aquellos que cometen delitos cibernéticos. Con su aprobación, dicha ley establece sanciones meramente penales, por lo que es importante conocer aquellas conductas indicadas en esa ley como ilegales, por ejemplo:

- Estafas electrónicas
- Manipulación de registros públicos o privados
- Acoso
- Accesos indebidos a sistemas informáticos
- Interferencia de sistemas informáticos, etc.

El Salvador no se ve desafectado por las implicaciones legales del uso de las tecnologías de la información y las comunicaciones. La regulación de crímenes cibernéticos es un avance para el desarrollo del Derecho de las Nuevas Tecnologías.

Indicación:

Investigar las siguientes interrogantes.

1. ¿Qué es un delito?

2. ¿Qué es un delito cibernético o delito informático?

3. ¿Quién comete delitos informáticos?

4. ¿Cuáles son los delitos informáticos previstos en la legislación penal mexicana?

5. ¿En cuáles legislaciones especiales se encuentran previstos delitos informáticos?

6. ¿Qué es el delito de revelación de secretos?

7. ¿Qué es el delito acceso ilícito a sistemas y equipos de informática?

8. ¿Qué es el delito contra la identidad de privacidad de la información sexual?

9. ¿Se considera como delito afectar un programa de cómputo o software?

10. ¿En qué consiste el delito de engaño telefónico?

11. ¿En qué consiste el delito de extorsión telefónica?

12. ¿A qué se refiere la falsificación de títulos o documentos crediticios?

13. ¿En qué consiste el delito de alteración o manipulación de medios de identificación electrónica?

14. ¿En qué consiste el delito de pornografía?

15. ¿Cuál es el delito de acoso sexual a través de medios informáticos?

16. ¿En qué consiste el delito de difusión de imágenes falsificadas de personas?

17. ¿Cuáles conductas son tipificadas como delitos cibernéticos en la Ley de Instituciones de Crédito?

18. ¿En qué consiste el delito de suplantación de identidad según la legislación penal?

19. ¿Qué es un phishing?

20. ¿Qué es el ciberodio?

21. ¿Qué es la pornografía infantil?

22. ¿Qué es el fraude?

23. ¿Qué es el chantaje?

Guía #5

“Tarea virtual desde casa”

- ✚ Realizar una presentación en Microsoft Power Point o una video presentación, en la aplicación de tu preferencia de todos los temas de ciberdelitos.
- ✚ Si no tiene acceso a una computadora hacer la presentación en pedazos de cartulina, esquemas, páginas de papel bond o en el cuaderno de forma clara y ordenada.
- ✚ Puedes informarte en otros sitios web para fortalecer conocimientos.
- ✚ Puedes transcribir la información resumida en tu cuaderno, para sustentar la temática.

Información opcional docente:

Materia: informática

Nombre: Prof. Jairo Josue García Méndez

Correo: jairojosue27@gmail.com (entrega de tareas)

Consultas a mi número y WhatsApp: 78125907

Horario de atención en línea y virtual: 8:00 am a 8:00 pm (instalar la aplicación Meet o Zoom)

Atención presencial con medidas de Bioseguridad por medio de acuerdo previo.