INSTITUCIÓN EDUCATIVA FEDERICO SIERRA ARANGO
Resoluciones Deptales. 15814 de 30/10/2002 – 9495 de 3/12/2001
NIT: 811039779-1 DANE: 105088001750
Bello - Antioquia

GUÍA N°3: SOFTWARE (DELITOS INFORMÁTICOS)

TECNOLOGÍA E INFORMÁTICA PERIODO DOS (2) SEMANAS (5 Y 6)
AREA: Tecnología e Informática.
GRUPO: 8°1 - 8°2 – 8°3
INDICADORES DE DESEMPEÑO • **Explico, con ejemplos, conceptos propios del conocimiento tecnológico tales como tecnología, procesos, productos, sistemas, servicios, artefactos, herramientas, materiales, técnica, fabricación y producción. (Conocer qué son los delitos informáticos y que normas té pueden proteger.)** •
RESPONSABLES: Adriana Ortega y Nancy Esthela Salazar Mosquera
OBSERVACIONES: • Realizar la lectura, que abarca el tema: *Delitos informáticos*, haga su lectura a conciencia y disfrútela. • Desarrolle la actividad que se encuentra finalizando la lectura ingresando al enlace que está asignado en la plataforma. • Esta actividad se entrega por medio de la plataforma CLASSROOM. • El trabajo se debe realizar y entregar de forma individual. • Si algún estudiante no cuenta con la herramienta sugeridas, realice la actividad en el cuaderno de tecnología, bien organizado, ordenado, coherente y claro. Luego de forma física entregue en la IEFESA; si puede enviarlo por medio de imágenes a la plataforma Classroom hágalo • La fecha límite para entregar el trabajo es el 14 de mayo del año 2021 hasta las 12:00 M.

DELITOS INFORMÁTICOS

Recordando un poco la historia, al ser humano actual le ha sucedido lo mismo que a nuestros antepasados prehistóricos cuando fabricaron el primer cuchillo. Tuvo un gran alivio en sus labores diarias, se sintió feliz, porque ya contaba con una herramienta que le ayudaría en sus tareas cotidianas de supervivencia. Pero no faltó quien usara esta herramienta con otras intenciones en contra de sus congéneres y terminara cometiendo delitos que, seguramente, en su momento no se llamaron así, aunque sí se entendían como actos en contra de la supervivencia de los demás. Con los sistemas informáticos ha ocurrido algo similar a lo observado en la historia. El hombre vive cada vez más interesado y condicionado por la informática, debido a su vertiginoso desarrollo y a la enorme influencia que ha alcanzado en muchas de las actividades diarias de las personas y las organizaciones. Pocas personas, en la actualidad, pueden abstraerse del contacto directo o indirecto con un sistema de cómputo, lo cual muestra de distintas maneras el poder y alcance de la tecnología informática en las sociedades del mundo. Así como la tecnología y su desarrollo han incidido en prácticamente todas las actividades del ser humano a lo largo de su historia, en la actualidad, la dependencia tecnológica ha venido concentrándose cada vez más en el fenómeno de la tecnología informática, la información y la comunicación.

Con efecto retardado, se descubrió luego que ese desarrollo venía acompañado de distintos y también novedosos riesgos.

Los antecedentes de los delitos informáticos van a la par del desarrollo de las tecnologías de la información. Con el desarrollo de la tecnología, la sociedad se ha visto en un panorama de avance y desarrollo en todas sus áreas; por desgracia, la delincuencia también se ha beneficiado de esto. Entre los beneficios que ofrece el uso de redes de comunicación a los delincuentes se encuentran: la

Fuente:
https://www.dinero.com/pais/articulo/formulan-pliego-de-cargos-contra-elizabeth-loaiza-por-publicidad-enganosa/286003
https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/
https://dialnet.unirioja.es/descarga/articulo/248204.pdf
https://dialnet.unirioja.es/descarga/articulo/3643404.pdf
http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Adriana.ortega@virtul.edu.co
E-mail: Nancy.salazar@virtual.edu.co
312 7088768

capacidad de cometer delitos en y desde cualquier parte del planeta, velocidad, gran cantidad de víctimas potenciales y anonimato, entre otros. Uno de los primeros y más importantes ataques en la historia de Internet se remonta a CREEPER en 1971, escrito por el ingeniero Bob Thomas, es considerado el primer virus informático que afecto a una computadora el cual mostraba un mensaje en los equipos infectados, el cual, si no causaba daño alguno, fue la base para el desarrollo de ataques posteriores con pérdidas multimillonarias. Se puede definir el delito informático como: "*El acto en el cual interviene un sistema de cómputo como utensilio en la producción de un hecho criminológico, en donde se atenta contra los derechos y libertades de los ciudadanos.*"

SUPLANTACIÓN DE IDENTIDAD

Fuente:
https://www.dinero.com/pais/articulo/formulan-pliego-de-cargos-contra-elizabeth-loaiza-por-publicidad-enganosa/286003
https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/
https://dialnet.unirioja.es/descarga/articulo/248204.pdf
https://dialnet.unirioja.es/descarga/articulo/3643404.pdf
http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Adriana.ortega@virtul.edu.co
E-mail: Nancy.salazar@virtual.edu.co
312 7088768

NORMATIVIDAD SOBRE DELITOS INFORMÁTICOS

Código penal colombiano

LEY 1273/09 (Protección de la información y de los datos)

	Se comete cuando	Pena
269 A Acceso abusivo a un sistema informático	Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 B Obstaculización ilegítima de sistema informático o red de telecomunicación	Bloquean en forma ilegal un sistema o impiden su ingreso, igualmente, el acceso a cuentas de correo electrónico de otras personas, sin el debido consentimiento.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 C Interceptación ilícita de datos informáticos	Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.	Prisión de 36 a 72 meses vigentes
269 D Daños informáticos	Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 E Uso de software malicioso	Cuando se producen, adquieren, distribuyen, envían, introducen o extraen del país software o programas de computador que produce daños en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 F Violación de datos personales	Sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
269 G Suplantación de sitios *web* para capturar datos personales	Crean una página similar a la de una entidad y envía correos (spam o engaños), como ofertas de empleo y personas inocentemente, suministran información personal y claves bancarias, y el delincuente informático ordena transferencias de dinero a terceros.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes

Auditoría de sistemas frente a los delitos informáticos, DI

Fuente:
https://www.dinero.com/pais/articulo/formulan-pliego-de-cargos-contra-elizabeth-loaiza-por-publicidad-enganosa/286003
https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/
https://dialnet.unirioja.es/descarga/articulo/248204.pdf
https://dialnet.unirioja.es/descarga/articulo/3643404.pdf
http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Adriana.ortega@virtul.edu.co
E-mail: Nancy.salazar@virtual.edu.co
312 7088768

SITUACIÓN REAL (NOTICIA, MAYO 6 DE 2020)

Pliego de cargos contra Elizabeth Loaiza por publicidad engañosa

Este miércoles, la Superintendencia de Industria y Comercio (SIC) anunció que formulará pliego de cargos contra la modelo Elizabeth Loaiza por hacer publicidad engañosa a través de sus redes sociales, a través de la cual ofrecía pruebas rápidas de detección del coronavirus que no tenían aprobación por la autoridad sanitaria en el país.

Loaiza había anunciado en sus redes sociales el producto 'ProMed Covid 19 Rapid Test', asegurando que este contaba con el registro sanitario expedido por el Invima y que podían adquirirlo únicamente las gobernaciones, alcaldías, hospitales y clínicas.

Ante esto, la delegatura de protección al consumidor de la entidad adelantó una serie de averiguaciones sobre las publicaciones realizadas por la modelo e influenciadora en su cuenta de Instagram. En estas indagaciones, la delegatura encontró que se trataba de un producto al que se le atribuían bondades relacionadas con la detección rápida de la covid-19."Al parecer, estas condiciones objetivas no se ajustan a la realidad, lo cual podría construir publicidad engañosa y por tanto una vulneración a lo dispuesto en el Estatuto del Consumidor", explicó la Superindustria.

A raíz de esta situación, la SIC solicitó a Loaiza información sobre el origen del producto y los beneficios atribuidos al mismo, así como de la publicidad utilizada para tal fin. Dicha información no fue suministrada por la modelo, por lo cual la entidad también imputó cargos por el incumplimiento de esta orden.

Así mismo, la Superintendencia también tuvo en cuenta la alerta sanitaria expedida por el Invima en la que, además de advertir que las pruebas rápidas de detección del virus no son de venta libre, incluyó un listado de pruebas que se ofrecen en el mercado nacional sin contar con autorización por la autoridad, dentro de las cuales se encontraba el producto ofrecido por Loaiza. "En consecuencia, se solicitó información en relación con la publicación mencionada al Invima, la cual confirmó a esta autoridad que el producto mostrado en la publicidad de la cuenta de Elizabeth Loaiza no contaba con registro sanitario, ni autorización de importación para su comercialización", señaló la SIC.

De confirmarse la violación de las normas señaladas, la entidad aseguró que la modelo e influenciadora podría ser sancionada con una multa económica de hasta 2.000 salarios mínimos legales mensuales vigentes.

Fuente:
https://www.dinero.com/pais/articulo/formulan-pliego-de-cargos-contra-elizabeth-loaiza-por-publicidad-enganosa/286003
https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/
https://dialnet.unirioja.es/descarga/articulo/248204.pdf
https://dialnet.unirioja.es/descarga/articulo/3643404.pdf
http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Adriana.ortega@virtul.edu.co
E-mail: Nancy.salazar@virtual.edu.co
312 7088768

ACTIVIDAD N°1: FORMULARIO GOOGLE DELITOS INFORMÁTICOS

Componente (Martes de Pruebas)

1. Después de realizar la lectura, ingrese al siguiente enlace para que conteste las preguntas acerca de los delitos informáticos. Por favor marque los datos obligatorios que se le solicitan.
2. Si algún estudiante no cuenta con la herramienta sugeridas, realice la actividad en el cuaderno de tecnología, bien organizado, ordenado, coherente y claro. Luego de forma física entregue en la IEFESA; si puede enviarlo por medio de imágenes a la plataforma Classroom hágalo

Nombres y Apellidos:
Grado:
Fecha:

Responde la pregunta correcta

1. El uso de software malicioso consiste en
   A. La utilización de malware y software espías para captura de información
   B. El envío y recepción de información privada sobre posibles víctimas de desfalco
   C. La utilización de páginas web ficticias para estafas
   D. La programación de software de video juegos.
2. Como se pueden evitar o evadir las estafas en Redes Sociales:
   A. No tener redes sociales
   B. No compartir mi perfil en redes
   C. Verificar la valides de los perfiles
   D. Solo fiarme de los perfiles de famosos
3. Cuál de los siguientes YouTuber estuvo envuelto en estafas virtuales por ofrecer productos sin registro INVIMA.
   A. Liendra
   B. Elizabet Loaiza
   C. Ami Rodríguez
   D. Sofia Castro

Escoja las respuestas correctas

4. Qué puede usted hacer en caso de ser víctima de suplantación de identidad:
   A. Reportar el perfil en su red social.
   B. Revisar las políticas de seguridad de su red social
   C. Cambiar su contraseña de ingreso a su red social
   D. Convertir su perfil en privado.
   E.
5. ¿Cuáles son las técnicas o estrategias que utilizan los hackers para hacer suplantación de identidad?
   A. Malware
   B. Phishing
   C. URL Phishing
   D. Hackeo de cuenta

Fuente:
https://www.dinero.com/pais/articulo/formulan-pliego-de-cargos-contra-elizabeth-loaiza-por-publicidad-enganosa/286003
https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos
https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/
https://dialnet.unirioja.es/descarga/articulo/248204.pdf
https://dialnet.unirioja.es/descarga/articulo/3643404.pdf
http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Adriana.ortega@virtul.edu.co
E-mail: Nancy.salazar@virtual.edu.co
312 7088768