INSTITUTO TECNOLOGICO DE TLALNEPANTLA

NOMBRE: SALINAS OREGON

SOFIA

MATERIA: AUDITORIA EN

TECNOLOGIAS DE INFORMACION

PROFESOR: CRUZ VENEGAS

MARIA DEL CARMEN

GRUPO: T91

NUMERO DE CONTROL: 17251084

FECHA DE ENTREGA: JUEVES 3

DE MARZO DE 2022

ACTIVIDAD 1. ADJUNTAR ARCHIVO. CONTESTA EL SIGUIENTE CUESTIONARIO

1.- ¿Cuál es la diferencia entre Informática Jurídica y Derecho Informático?

la informática jurídica surge cuando se aplican los instrumentos informáticos a los fenómenos del derecho, se refiere a la informática como avanzado medio técnico que proporciona auxilio y servicio a las diversas actividades relacionadas con el derecho.

2.- ¿Cuáles son los derechos patrimoniales en el derecho de autor?

Los derechos patrimoniales de autor se denominan como tal, porque hacen parte del patrimonio del autor, por lo que se traducen en la facultad de beneficiarse y disponer de su obra y en ese sentido, se heredan, pueden hacer parte de la sociedad conyugal, son embargables, son transigibles y son renunciables. Estos se dividen en dos tipos, los derechos patrimoniales exclusivos, en los cuales el ejercerlos implica una autorización previa, y los de mera remuneración, en donde no se requiere autorización sino pago.

Son derechos exclusivos, entre otros, los siguientes:

- Reproducción: Crear copias físicas o digitales de la obra.
- Comunicación pública: Comunicar o poner a disposición del público la obra.
- Transformación: Crear otras obras a partir de la obra original, tales como la traducción o la adaptación.
- Distribución: Poner a disposición del público ejemplares de la obra mediante venta, alquiler, etc.

3.- ¿Qué es la multimedia?

Multimedia es cualquier combinación de texto, arte gráfico, sonido animación y video que llega a usted por computadora u otros medios electrónicos.

4.- ¿Qué es una estafa informática?

Se refiere al fraude realizado a través del uso de una computadora o del Internet. La piratería informática (hacking) es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial.

5.- Realice una clasificación de los contratos informáticos?

- Contrato informático de hosting.
- Contrato informático de outsourcing.
- Contratos informáticos sobre el software.
- Contratos informáticos de desarrollo de programas.
- Contrato de mantenimiento informático.

- Contrato de escrow.
- Contrato de auditoria informática.

6.- ¿Qué es el EDI?

EDI, que significa intercambio electrónico de datos, es la comunicación entre empresas de documentos comerciales entre empresas, en un formato estándar.

7.- ¿Cuál es la diferencia entre una tarjeta de crédito y una de débito?

En una tarjeta de débito, el pago se carga directamente en la cuenta corriente del titular. Así, solo permiten el cobro hasta el límite de los fondos de la cuenta. Con la tarjeta de crédito es posible pagar incluso si no se dispone de fondos, ya que es posible aplazar el cobro hasta el mes siguiente.

8.- ¿Cuál es la diferencia entre contratación informática y contratación

electrónica?

La diferencia existente entre la contratación electrónica y la contratación informática, es que en la primera se dan las contrataciones utilizando como medio las computadoras y demás medios electrónicos pertinentes, mientras que e la segunda las contrataciones se dan en relación a bienes y servicios informáticos.

Contratación electrónica:

- Contrato de arrendamiento financiero a través de un e-mail o correo electrónico.

Contratación informática:

- Un contrato de adhesión.

9.- ¿Qué es un documento electrónico?

Es aquel producido por una persona natural o jurídica en el ejercicio de sus funciones que contiene información generada, enviada, recibida y almacenada por medios electrónicos, la cual permanece en estos medios durante todo su ciclo de vida.

ACTIVIDAD 2. ADJUNTAR ARCHIVO INVESTIGAR 3 CASOS REALES DE FRAUDES INFORMÁTICOS Y PROPONER (MÍNIMO 3) CONTROLES PARA PREVENIRLOS.

1. Fallchill

Es un ***malware*** que fue detectado en varios equipos de una empresa de telecomunicaciones en la Ciudad de México. Entre sus capacidades están las siguientes:

- **Extraer información de los discos duros** de las computadoras donde se alojaba.
- **Iniciar y terminar procesos**.
- Intervenir cualquier archivo para **modificarlo, ejecutarlo, moverlo** o incluso eliminar elementos del sistema.
- Por último, es capaz de borrarse a sí mismo, y así **evitar dejar rastros** de su presencia, lo que dificulta su detección en las redes vulnerables.

CONTROL PARA PREVENIR:

- Ataque por Denegación de Servicio Distribuido (DDoS). Típicamente, el DDos es utilizado para atacar y volver inestable un servidor, impidiendo así que los usuarios legítimos accedan a él. Sin embargo, utilizado a la inversa puede ayudar a efectuar pruebas de penetración con el objetivo de identificar y eliminar vulnerabilidades o brechas en los sistemas, favoreciendo la prevención y control de riesgos informáticos.

- Software como Servicio (SaaS). Los SaaS ayudan a centralizar la información para un óptimo manejo y protección; además, aportan a la ciberseguridad en tanto que permiten mantener control sobre el área de Cumplimiento.

- Supervisar la interacción de las máquinas de manera en que, en el momento que se detecte una acción sospechosa en los equipos no pasar desapercibido y poner atención en el mismo, del mismo modo, mantener el equipo bajo contraseña o seguridad.

2. WannaCry

Tuvo alcance en más de 150 países, incluido México en 2017. Este programa **operaba mediante extorsiones**, ya que tenía la función de **"secuestrar"** información para luego "pedir pagos por su rescate"; este es el *modus operandi* típico de un ***ransomware*.**

Se calcula que el número de víctimas de este malware, hasta 2018, fue de al menos **200,000 a nivel global**; mientras que, en México, se estima que el 44% de las organizaciones fueron víctimas del secuestro de su información.

CONTROL PARA PREVENIR:

- Lo primordial es el cuidado de la información personal, es decir, no proporcionar datos delicados como nombre, teléfono, fechas de nacimiento o datos similares en plataformas de fácil acceso o de acceso público.
- Eliminar directamente los correos sospechosos, sin abrir los enlaces o archivos.
- Mantener activado el anti spam (filtra la entrada por correo electrónico) y el antivirus, actualizado con la versión más reciente.

3. Janeleiro

Por último, este **malware bancario** creado originalmente para atacar corporativos de bancos en Brasil, del cual fue creada una variante para atacar usuarios en México, y poder **robar su información bancaria y personal.**

Este virus es distribuido a través de correos electrónicos, que contienen enlaces que re direccionan a los usuarios ventanas emergentes con **formularios de banco apócrifos**; de esta forma **logran acceder y robar la información** bancaria.

CONTROL PARA PREVENIR:

- Eliminar directamente los correos sospechosos, sin abrir los enlaces o archivos.
- Si tenemos aplicaciones en el teléfono de banca móvil utilizar mecanismos de seguridad para hacer cualquier tipo de acción como token, claves, etc.

- Utilizar antivirus y tener cuidado con descargas peligrosas.