TECNOLOGICO NACIONAL DE MEXICO
INSTITUTO TECNOLOGICO DE TIJUANA

SEMESTRE 2022-1

ING INFORMATICA

TALLER DE LEGISLACION INFORMATICA

Portafolio de Evidencias

Garcia Vázquez Wesly

Docente: DANIELA ADRIANA SANCHEZ VIZCARRA

Índice

Introducción

En este trabajo veremos una recopilación de los trabajos realizados a lo largo del semestre, podemos encontrar en cada una de las actividades un resumen de lo visto en la unidad.

6. Temario

No.	Temas	Subtemas
1.	Introducción al derecho	1.1. Concepto y propósito del derecho. 1.2. Normas jurídicas, morales y sociales. Semejanzas y Diferencias. 1.3. Fuentes del derecho. 1.4. Clasificación del derecho.
2.	El derecho y la informática	2.1. La sociedad de la información. 2.2. Derecho informático. 2.3. Orígenes, concepto y clasificación del derecho informático. 2.4. Informática jurídica.
3.	Derecho de la información y de los datos personales	3.1. El derecho de la información. 3.2. Los problemas de su sistematización. 3.3. El régimen jurídico de la información en México. 3.4. Marco constitucional. 3.5. Libertad de expresión. 3.6. Derecho de petición. 3.7. Las telecomunicaciones.
4.	El derecho de la propiedad intelectual y las nuevas tecnologías de la información y comunicación	4.1. Protección jurídica de los programas de cómputo. 4.2. Implicaciones. 4.3. Criptografía. 4.4. Propiedad industrial y derechos de autor (Marcas, Patentes, Copyright, Copyleft). 4.5. Normatividad internacional.
5.	Los contratos informáticos	5.1. Concepto y elementos. 5.2. Clasificación de los contratos informáticos. 5.3. Características particulares de los contratos informáticos. 5.4. Partes de los contratos informáticos. 5.5. Fraudes en la comercialización de tecnologías de información y comunicación.
6.	Delitos informáticos	6.1. Concepto y características. 6.2. Clasificación de delitos informáticos. 6.3. Normatividad nacional. 6.4. Normatividad internacional.

Actividad Unidad 1

Norma	Características	Sanción	Ejemplo
Jurídicas	Reglas de conducta establecidos por una autoridad para regular la conducta humana	▪ Económica ▪ Privar de libertad ▪ Indemnización	• Robo y/o hurto de bienes • Estafas
Sociales	Permiten a la sociedad desarrollar una vida social más amena y cordial (cortesía) o, bien, conducirnos conforme a ciertas reglas establecidas para circunstancias y momentos determinados.	▪ Rechazo de la sociedad. ▪ No ser aceptado en un grupo social	• Tirar basura en la calle. • Mantener limpio la ciudad-
Morales	Conjunto de reglas que indica lo que está bien o mal, lo que debemos o no hacer en nuestra relación con la sociedad.	• Similitud con las sanciones de normas sociales. ▪ Ser señalado por los individuos de la sociedad o familia.	• Hablar mal de los demás. • Ser “Doble cara”.
Religiosas	Son reglas de conducta en las que se establece que está permitido y que está prohibido.	• Ser señalado por los altos cargos de la institución religiosa	• Romper Ayuno • Comer carne en cuaresma.

Actividad Unidad 2

Tipo de I. Jurídica	Finalidad	Ejemplo
Documentaria	Encontrar lo más rápida y pertinentemente posible la información que ha sido almacenada.	• Uso de base de datos • Información en la nube
Control y Gestión	Organizar y controlar la información jurídica de documentos, expedientes, libros. Etc.	• Uso de expedientes • Programas
Meta documentaria	Hace uso de la inteligencia artificial para el amplio uso del conocimiento especializado para resolver problemas como especialista humano.	• Servicios de IA para resolver casos jurídicos

Actividad Unidad 3

	Que establece
Articulo 6	La libertad de expresión como la facultad de toda persona de manifestar sus ideas, pensamientos u opiniones por cualquier medio no escrito.
Articulo 7	La libertad de imprenta supone la facultad del individuo de publicar ideas, escritos o imágenes por cualquier medio grafico
Articulo 8	Las autoridades públicas tienen la obligación de responder por escrito y en breve termino a las consultas escritas que les formulen de manera pacífica y respetuosa los particulares.
Articulo 30	las publicaciones de carácter religioso no podrán "oponerse a las leyes del país o a sus instituciones, ni agraviar, de cualquier forma, los símbolos patrios".

Actividad Unidad 4

País	Normativa o Ley	Porcentaje de Pirateria	Enlace articulo
Rusia	La Federación Rusa ha aprobado un decreto que elimina las compensaciones a sus ciudadanos y empresas por el uso de patentes de los estados incluidos en su lista de "países hostiles"	**95%**	**Enlace**
Alemania	Ley Federal de Protección de Datos: Aprobada el 30 de junio de 2017, vigente desde el 25 de mayo de 2018, y modificada por última vez por la Ley para adaptar la Ley de Protección de Datos al Reglamento (UE) 2016/679 (RGPD).	**20%**	**Enlace**
India	Las leyes cibernéticas en India han allanado el camino para el comercio electrónico y la gobernanza electrónica en el país al garantizar la máxima conectividad y los mínimos riesgos de ciberseguridad. Además, para mejorar el alcance y expandir el uso de medios digitales.	**91%**	**Enlace**

China	La Ley de Ciberseguridad fue aprobada inicialmente por el Congreso Nacional del Pueblo en noviembre de 2016. Reforma la gestión de datos y las regulaciones de uso de Internet en China e impone nuevos requisitos para la seguridad de redes y sistemas.	**94%**	**Enlace**
México	Ley federal del derecho de autor (LFDA) Publicada en el Diario Oficial de la Federación el día 24 de Diciembre de 1996 por el presidente Ernesto Zedillo Ponce de León, El objeto de la misma es la protección de las obras originales susceptibles a ser reproducidas o divulgadas por cualquier medio o forma**.**	**75.1%**	**Enlace**

Actividad Unidad 5

Contrato informático

Los contratos informáticos surgen ligados a la inminente comercialización de las computadoras.

En un principio, éstas se empleaban, según hemos dicho, en el ámbito científico y militar y después fueron incorporadas al ámbito de los negocios, lo cual originó su rápida comercialización y, por ende, la proliferación de contratos en materia informática, cuya redacción significó una notoria diferencia respecto a lo que podríamos considerar contratos clásicos en función de su alta tecnicidad.

Clasificación

Tipo de contrato informático	Contenido
Contrato de compra-venta de hardware	El bien informático es por su naturaleza un bien mueble, por fuerza material para que cumpla con el requisito de ser físicamente aprensible, característica que la informática exige para ser denominado hardware.
Contrato de arrendamiento de hardware	En este contrato, el arrendador o locador cede temporalmente un bien informático, una computadora o conjunto de computadoras como regla y/o uno o más suministros, periféricos o repuestos de computadoras como excepción en arrendamiento a favor de un arrendatario.
Contrato de mantenimiento de hardware	1. Contratos de mantenimiento preventivo: se realizan con el objetivo de evitar anomalías en el funcionamiento de los equipos y que no incluyen el servicio de las reparaciones necesarias. 2. Contratos de mantenimiento correctivo: surten sus efectos cuando los componentes del equipo presentan fallas o problemas de funcionamiento.
Contrato de leasing de hardware	El contrato de leasing o arrendamiento financiero se basa en la necesidad del empresario de obtener un crédito (materializado en maquinarias como herramientas de producción).

Actividad Unidad 6

Lazarus, los cibercriminales que roban y extorsionan para el Amado Líder de Corea del Norte

El grupo de 'hackers' que en 2017 secuestró ordenadores de todo el mundo con el virus WannaCry acaba de robar 625 millones de dólares en criptomonedas, el mayor golpe digital de la historia

El mes pasado se perpetró el mayor robo cibernético del que se tiene constancia. Alguien sustrajo criptomonedas (ethereum, la segunda más usada tras bitcoin) por valor de 625 millones de dólares (alrededor de 600 millones de euros) de una web relacionada con el videojuego *Axie Infinity*. Estados Unidos no tardó en relacionar el ataque con el grupo Lazarus, unos ciberdelincuentes de Corea del Norte muy conocidos entre los expertos en ciberseguridad. La consultora especializada en *blockchain* Chainalysis estima que estos *hackers* norcoreanos podrían haberse adueñado el año pasado de otros 400 millones en activos digitales a través de varios ataques dirigidos a plataformas de criptomonedas.

Muchos países, como China, Irán o EE UU, patrocinan extraoficialmente a equipos de *hackers* para que realicen sabotajes o consigan información de valor. El caso de Pyongyang es distinto: utiliza a su grupo de expertos informáticos para hacer dinero. El Amado y Respetado Líder (esa es una de las formas oficiales de referirse a Kim Jong-un) lo ve como una vía para sobrevivir a las duras sanciones internacionales a las que está sometido el régimen.

Calificar a Lazarus de simples rateros digitales sería menospreciarlos. Su hoja de servicios está al alcance de muy pocos. EE UU y Reino Unido, así como Microsoft, les atribuyen el lanzamiento en 2017 de WannaCry 2.0, el mayor *ransomware* de la historia, que acaba de cumplir cinco años. Esta modalidad de virus informático secuestra los equipos infectados y los libera tras el pago de un rescate. Se calcula

que WannaCry afectó a unos 300.000 ordenadores de 150 países, incluyendo los del sistema de salud de Reino Unido, que quedó paralizado.

Un año antes, en 2016, Lazarus intentó robar 1.000 millones de dólares al Banco Central de Bangladesh con un sofisticado plan que incluía hacerse pasar por empleados de la entidad y lograr permisos para mover el dinero. El ataque se vio frustrado por un error de codificación, pero no antes de hacerse con 81 millones. El FBI lo consideró entonces el mayor ciberatraco de la historia. Existen sospechas también de que en 2018 robaron unos 530 millones de dólares en *tokens (*fichas digitales) del portal japonés de intercambio de criptomonedas Coincheck.

Hacer dinero para el Líder

Todo el dinero que gana Lazarus tiene un mismo destinatario: el régimen de Kim Jong-un. Lazarus es una rareza en el mundo de las amenazas persistentes avanzadas (APT en sus siglas inglesas), término con el que se conoce a los grupos organizados de *hackers* con mayores capacidades. Estos equipos, dirigidos y patrocinados extraoficialmente por gobiernos, se encuentran en la cúspide de la pirámide de los *hackers*. Están muy bien estructurados y jerarquizados —cuentan con departamentos y profesionales con roles muy definidos— y disponen de recursos económicos, lo que les permite elaborar ataques complejos, coordinados y veloces. Sobre el papel, solo los servicios secretos de las grandes potencias (EE UU, Rusia o Reino Unido) tienen más poder que las APT.

Debido a la propia naturaleza de internet, donde es sencillo pasar desapercibido, los ciberataques son muy difíciles de atribuir. “Las APT son rastreadas básicamente con pistas aportadas por los servicios de inteligencia y particularidades del código, pero hacer un buen análisis forense que determine la autoría puede llevar meses”, explica el *hacker* y analista de ciberseguridad Deepak Daswani. Por eso, los gobiernos usan las APT para sabotear, espiar o llevar a cabo acciones de inteligencia sin provocar incidentes diplomáticos.

“El de Lazarus es un caso único”, subraya Adam Meyers, responsable de inteligencia de CrowdStrike y experto en APT. “Otros grupos lanzan *ransomware*, como Rusia en Ucrania a través de Voodoo Bear, pero como tapadera para otros fines, sin interés alguno en ser pagados. Y si hacen dinero es para su propio beneficio, como las mafias. El objetivo de Lazarus es conseguir fondos para sostener un régimen asfixiado por las sanciones internacionales”, añade el analista tejano.

Fotograma del vídeo distribuido en marzo de este año por Pyongyang en el que Kim Jong-un dirige el lanzamiento de un misil balístico intercontinental.朝鮮通信社 **(AP)**

Lazarus es de hecho la palabra clave que se le dio a los *hackers* que operan desde Corea del Norte. El equipo de Meyers distingue cinco facciones diferenciadas dentro de ese paraguas, con objetivos y especializaciones bien definidas, pero que comparten hasta un repositorio de código al que recurren para preparar sus ataques. Dos de ellos, Stardust Cholima y Labyrinth Cholima, están exclusivamente dedicados a la monetización. “Creemos que Stardust Cholima pertenece a la Oficina 121, uno de los departamentos de la Oficina General de Reconocimiento”, nombre con el que se conoce a una de las agencias de espionaje norcoreanas. “Están muy enfocados en sistemas financieros, criptomonedas y nuevas tecnologías”.

El entramado de Lazarus también realiza acciones de sabotaje, en la línea de las APT de otros países. Los grupos de *hackers* de Corea del Norte fueron especialmente activos durante los meses de 2020 en los que las grandes farmacéuticas trabajaban frenéticamente para desarrollar una vacuna contra la covid. Trataron de entrar en los ordenadores de trabajadores de AstraZeneca, que junto con la Universidad de Oxford estaban en pleno desarrollo de uno de los remedios. Más tarde intentaron robar información de Pfizer, otro de los laboratorios volcados en la vacuna. Curiosamente, Corea del Norte es de los pocos países del mundo en los que la pandemia se mantuvo a raya (hasta hace unas semanas), por lo que sus intenciones podrían haber sido simplemente torpedear el proceso o vender secretos industriales.

Otro de sus golpes más sonados no perseguía fines económicos, sino venganza. Se desarrolló en 2014 y fue el primer aviso de que los norcoreanos no eran aficionados en el terreno digital. El objetivo fue Sony Entertainment, la productora de *La entrevista*, una película que fantasea con el asesinato de Kim Jong-un. Un mes antes de la fecha de estreno prevista, un grupo de *hackers* infectó los ordenadores de trabajadores de Sony. Consiguieron borrar datos sensibles de la compañía, publicaron detalles salariales y revelaron *emails* comprometedores de algunos de sus directivos. También amenazaron con atentados en las salas de cine

donde se exhibiera la cinta, lo que llevó a las grandes distribuidoras a retirarla de la cartelera.

El gran paso adelante de Kim Jong-un

Nadie creía que Corea del Norte sería capaz de convertirse en una potencia cibernética. Tampoco que pudiera desarrollar la bomba atómica. Pero consiguió ambas cosas. Lo segundo fue la obsesión de tres generaciones de dictadores; lo primero, un deseo expreso del actual.

Kim Jong-un dirige con mano de hierro uno de los países más aislados del mundo. Desde que en 2009 tomara el testigo de su padre, supo ver el potencial de la esfera digital tanto para espiar y sabotear a sus enemigos (EE UU y Corea del Sur) como para ganar un dinero que no puede conseguir a través del comercio. “El régimen norcoreano potencia activamente a los *hackers* de élite para incorporarlos a la Oficina 121″, escribe la australiana Anna Fifield en su libro *El gran sucesor* (Capitán Swing, 2021), en el que hace una radiografía de la hermética vida y carrera del nieto de Kim Il-sung. “Los estudiantes que muestran posibles aptitudes en este sentido, algunos de tan solo 11 años, son enviados a escuelas especiales y luego a la Universidad de Automatización de Pyongyang”, donde “a lo largo de cinco años se les enseña a *hackear* sistemas y a crear virus informáticos”.

Resulta llamativo, cuenta Fifield, que ya en 2018 los estudiantes norcoreanos obtuvieran regularmente los primeros puestos en las competiciones, o *hackatones*, organizadas por la empresa de *software* india CodeChef. Por lo que ha podido averiguar la periodista, buena conocedora del país debido a sus años en Tokio y Pekín como jefa de las oficinas del *Washington Post* y en Corea del Sur como corresponsal del *Financial Times*, los *hackers* norcoreanos gozan de una posición de respeto y una vida acomodada en un país en el que hasta los años noventa la gente moría literalmente de hambre.

Según cuenta Fifield a EL PAÍS, no tiene datos de que en los últimos años haya cambiado su estatus. Más bien al contrario: Kim Jong-un tiene claro que el cibercrimen es un negocio más, una respuesta a las sanciones internacionales. “El régimen participa en todo tipo de sectores que le puedan aportar divisas, como las pruebas farmacéuticas, el cultivo de opio o el tráfico de personas”, indica Meyers “El ciberespionaje y el cibercrimen son un vector más”. Si no puede ganar dinero comerciando, lo robará.

Referencia Electrónica

Pascual, M. G. (2022, May 23). Lazarus, los cibercriminales que roban y extorsionan para el Amado Líder de Corea del Norte. Ediciones EL PAÍS S.L. https://elpais.com/tecnologia/2022-05-23/lazarus-los-cibercriminales-que-roban-y-extorsionan-para-el-amado-lider-de-corea-del-norte.html

Conclusión

Esta materia me resulto de mucha importancia debido a que, como parte de nuestra formación universitaria, es de mucha relevancia el conocer los derechos, obligaciones en el ámbito jurídico informático, esto nos ayudara al momento de ejercer como ingenieros.