ACADEMIA DE
LA MAGISTRATURA

Manual Auto Instructivo

CURSO “DELITOS INFORMATICOS”

Elaborado por el
Dr. JHON SANCHEZ CHIRINOS

2016

Academia de la Magistratura

La Academia de la Magistratura es la institución oficial del Estado peruano, que tiene como finalidad la formación de aspirantes a la magistratura y el desarrollo de un sistema integral y continuo de capacitación, actualización, certificación y acreditación de los magistrados del Perú.

CONSEJO DIRECTIVO DE LA ACADEMIA DE LA MAGISTRATURA

Dr. Josué Pariona Pastrana
Presidente del Consejo Directivo

Dr. Zoraida Avalos Rivera
Vice- Presidenta del Consejo Directivo

Dr. Javier Arévalo Vela - Consejero

Dr. Ramiro Eduardo De Valdivia Cano- Consejero

Dr. Pablo Sánchez Velarde - Consejero

Dr. Sergio Iván Noguera Ramos - Consejero

Dr. Richard Alexander Villavicencio Saldaña –Consejero

Dra. Cecilia Cedrón Delgado - Director General

Dr. Bruno Novoa Campos - Director Académico

El presente material del Curso “DELITOS INFORMATICOS”, ha sido elaborado por el Dr. JHON SANCHEZ CHIRINOS.para la Academia de la Magistratura, en julio de 2016.

SILABO

NOMBRE DEL CURSO”DELITOS INFORMATICOS”

I. DATOS GENERALES

Programa Académico	:	Programa de Actualización y Perfeccionamiento
Horas Lectivas	:	74
Número de Créditos Académicos	:	03
Especialista que elaboró el material	:	JHON SANCHEZ CHIRINOS

II. PRESENTACIÓN

El presente curso, pone a disposición de los discentes, material de capacitación dentro del marco de la investigación y procesamiento de los delitos informáticos por parte de las instituciones involucradas en el sector justicia, las que a la fecha no cuentan con acervo documentario que permita un adecuado análisis de los tipos penales incorporados en la legislación nacional e internacional.

Los delitos informáticos atendiendo al medio que emplean, es decir, uso de nuevas tecnologías de la información y comunicación aprovechando la vulnerabilidad de los sistemas informáticos y de los usuarios, presentan cifras en crecimiento tal como lo demuestra el observatorio de la criminalidad del Ministerio Público, los mismos que resultan en procesos judiciales y refleja la necesidad de especialización por parte de jueces y fiscales.

El presente curso realiza un desarrollo que parte de conocimientos técnicos fundamentales, análisis de modalidades delictivas usando las tecnologías de la comunicación, las políticas públicas, la tipificación del delito a nivel nacional e internacional así como una introducción a lo que constituye el análisis de evidencia digital por medio de la uso de las nuevas tecnologías, con un soporte legal adecuado que permita una investigación que incida en un debido proceso.

III. COMPETENCIAS A ALCANZAR

Para el presente curso se ha formulado la siguiente competencia:

Conocer, comprender, aplicar y argumentar la importancia de la investigación de los Delitos informáticos, desde una perspectiva técnico - legal para lo cual deberá analizar, evaluar y proponer soluciones con una visión multidisciplinaria con énfasis en la aplicación normativa. La asignatura contribuirá al desarrollo de competencias transversales tales como: Analizar e investigar problemas, iniciativa, innovación, aprendizaje autónomo, liderazgo, integración de conocimientos, orientación a resultados.

Capacidades Terminales:

- Identifica las distintas modalidades de delito informático, características, métodos de investigación, procedimientos que aseguren una adecuada cadena de custodia y el análisis multidisciplinario.

IV. ESTRUCTURA DE CONTENIDOS

UNIDAD I: CONOCIMIENTOS TECNICOS

Conceptuales	Procedimentales	Actitudinales
1. La Sociedad de la Información y la protección de los derechos. 2. Redes y Telecomunicaciones 3. Modalidades delictivas y tecnologías empleadas en los Delitos Informáticos	Para el desarrollo del Taller el discente dispondrá del material de estudio elaborado por el especialista, el mismo que contará con un marco teórico desarrollado específicamente para estos efectos, así como lecturas y casos oportunamente entregados.	Aprecia la importancia del conocimiento de la tecnología y su relación con el derecho.

Lecturas Obligatorias: 1. EL SECRETO DE LAS COMUNICACIONES CON ELABOGADO DEFENSOR EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN- INMACULADA LÓPEZ-BARAJAS PEREA.
Lecturas Sugeridas a) Topología e Infraestructura de Redes. b) Guía de Nombres de Dominio. c) Caso Esher vs Brasil. d) Informe Pandalabs 2015.

UNIDAD II: CONOCIMIENTOS LEGALES

Conceptuales	Procedimentales	Actitudinales
1. Análisis respecto a temas de seguridad de la información de la ley de protección de datos personales 29733 y su reglamento. 2. El Convenio de Budapest- Convenio sobre cibercriminalidad.	Para el desarrollo del Taller el discente dispondrá del material de estudio elaborado por el especialista, el mismo que contará con un marco teórico desarrollado específicamente para estos efectos, así como lecturas y casos oportunamente entregados.	Reflexiona sobre los temas de seguridad de la información.
Lecturas Obligatorias: 1.- Convenio sobre la Cibercriminalidad de Budapest. 2.- Ley 30071 y 30096 de Delitos Informáticos. 3.- Retención de datos y secreto profesional- Comisión de Derechos Humanos de Barcelona FBE 30 de enero 2015.		
Lecturas Sugeridas a) Norma Técnica Peruana ISO - IEC .- 27001-2014 b) Ley 29733 - Protección de Datos Personales y su reglamento.		

UNIDAD III: INFORMATICA FORENSE

Conceptuales	Procedimentales	Actitudinales
1. Análisis de evidencia digital y definición de informática forense.	Para el desarrollo del Taller el discente dispondrá del material de estudio elaborado por el especialista, el mismo que contará con un marco teórico desarrollado específicamente para estos efectos, así como lecturas y casos oportunamente entregados.	Aprecia la importancia del conocimiento de la evidencia digital y definición de informática forense.
Lecturas Obligatorias: 1.- La Cadena de Custodia Informático Forense. 2.- Análisis Forense Digital - Miguel López Delgado.		
Lecturas Sugeridas: a) Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 Dr. Santiago Acurio Del PinoDirector Nacional de Tecnología de la Información. b) Sentencia por Delito de Fraude Informático.		

V. MEDIOS Y MATERIALES.

- Material de lectura preparado por el docente
- Jurisprudencia seleccionada
- Lecturas recomendadas

VI. METODOLOGÍA Y SECUENCIA DE ESTUDIO.

La metodología del Curso "Delitos Informáticos es activa y participativa, basada en el método del caso, aprendiendo desde lo vivencial, a través de una práctica concreta de los casos planteados por el docente, promoviendo la conformación de grupos de estudios, análisis de textos y la resolución de los cuestionarios respectivos, todo esto para alcanzar las competencias esperadas en el curso.
Para el desarrollo del presente curso los discentes tendrán acceso al Aula Virtual de la Academia de la Magistratura, donde tendrán a su disposición todos los materiales utilizados, las diapositivas de las sesiones presenciales y lecturas obligatorias.

Se combina el aprendizaje a distancia con sesiones presenciales. Fase presencial: Interactiva; con las siguientes técnicas: exposición y preguntas,

lluvia de ideas, análisis de casos, debates, argumentación oral. Fase no presencial: Lectura auto instructiva y foro virtual.

VII. SISTEMA DE ACOMPAÑAMIENTO

Para el desarrollo de este curso, el discente cuenta con el acompañamiento del profesor especialista quien será el responsable de asesorarlo y orientarlo en los temas de estudio, a la vez que dinamizarán la construcción del aprendizaje. Así también, contarán con un coordinador quien estará en permanente contacto para atender los intereses, inquietudes y problemas sobre los diversos temas.

VIII. SISTEMA DE EVALUACIÓN

Se ha diseñado un sistema de evaluación permanente, de manera que el discente pueda ir reflexionando y cuestionando los diversos temas propuestos en el curso. Los componentes evaluativos serán informados oportunamente por el coordinador del curso.

IX. BIBLIOGRAFÍA

1) CABEZUDO Rodríguez, N. "La administración de justicia ante las nuevas tecnologías. Del entusiasmo a la desconfianza, pasando al olvido" Revista jurídica de Castilla y León, núm, 7, Octubre 2005, págs. 155-208.
2) Castells, Manuel, La era de la Información. 1998.
3) CLIMENT Barberá, J,. "La Justicia penal en Internet, Territorialidad y competencias penales", en VV.A.A., Internet y derecho penal, Consejo General del Poder Judicial, Madrid, 2001, págs. 645-663.
4) CONDE Ortiz, C. La protección de los datos personales, Un derecho autónomo con base en los conceptos de intimidad y privacidad, Dykinson, Madrid , 2005
5) CRUMP, C, "Data retention: Pryvacy, Anonymity, and Accountability Online", Stanford Law Review, núm 1, volumen 56, Octubre 2003, 7ágs.. 191-229.
6) DAVARA Rodríguez, M.A., La protección de datos de Europa: principios, derechos y procedimiento, Grupos Asnef Equifax, Madrid 1998.
7) Delgado López, L.M. y Martin Nájera, S., "La recogida y conservación de contenidos en la intervención de las comunicaciones telefónicas y telemáticas" Revista del Ministerio Fiscal, núm. 7, 2000, 7ágs.. 141-158.

8) GONZALES López, Juan José, Los datos de tráfico de las comunicaciones electrónicas en el proceso penal. Editorial La Ley , Madrid, 2011.
9) Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico2001-2002 de la UOC.
10) Linares Julio, et Alii. Autopistas Inteligentes, Fundesco 1995.
11) LOPEZ-BARAJAS Perea, Inmaculada, La Intervención de las comunicaciones electrónicas. Ed. La Ley, 1 edición, 2011. 349 p.
12) Misión para la Sociedad de la Información, Libro verde sobre la Sociedad de la Información en Portugal, 1997.
13) PARDINI, Aníbal, Derecho de Internet, Ediciones La Roca, Buenos Aires 2002.
14) YONEJI Matsuda, La Sociedad Informatizada como sociedad post-industrial, Tecnos 1994.

PRESENTACIÓN

La Academia de la Magistratura es la institución oficial del Estado Peruano que tiene como finalidad desarrollar un sistema integral y continuo de formación, capacitación, actualización, y perfeccionamiento de los magistrados del Poder Judicial y Ministerio Público.

La Academia de la Magistratura, a través de la Dirección Académica ejecuta el Curso "Delitos Informáticos" en el marco de actividades de las Sedes Desconcentradas. Para este fin, se ha previsto la elaboración del presente material, el mismo que ha sido elaborado por un especialista de la materia y sometido a un tratamiento didáctico desde un enfoque andragógico, a fin de facilitar el proceso de enseñanza y aprendizaje del discente de una manera sencilla y práctica.

El presente material se encuentra estructurado en tres unidades con los siguientes ejes temáticos: Conocimientos Técnicos, Conocimientos Legales y Informática Forense.

Asimismo, el discente tendrá acceso a un Aula Virtual, siendo el medio más importante que utilizará a lo largo del desarrollo del curso, a través de ella podrá acceder al material autoinstructivo, lecturas y un dossier de casos que le permita aplicar los conocimientos adquiridos.

En ese sentido, se espera que concluido el presente Curso el discente esté en mejores condiciones para Conocer, comprender, aplicar y argumentar la importancia de la investigación de los Delitos informáticos, desde una perspectiva técnico - legal para lo cual deberá analizar, evaluar y proponer soluciones con una visión multidisciplinaria con énfasis en la aplicación normativa. La asignatura contribuirá al desarrollo de competencias transversales tales como: Analizar e investigar problemas, iniciativa, innovación, aprendizaje autónomo, liderazgo, integración de conocimientos, orientación a resultados.

Dirección Académica

INTRODUCCIÓN

En los últimos 50 años hemos sido testigos de una elevada escala de la tecnología informática. El desarrollo de los sistemas informáticos produce, a su vez, el desarrollo de nuevas formas de comunicación entre los individuos.

Producto de todo el avance tecnológico, el Derecho también se ve inmerso en nuevas formas de actividades de diverso tipo, en las cuales la intervención de los sistemas informáticos para su realización es cada vez más común. Todo esto origina que surjan contratos que se celebran a través de un sistema operativo o que se realicen actos de comercio a través de la red. Estas conductas no siempre son lícitas, por lo que es necesaria su debida regulación para garantizar la participación de los usuarios en la red y para un correcto funcionamiento de los sistemas.

Es indudable, pues, que la informática produce cada día una intensa evolución en las distintas ramas del Derecho (Derecho Constitucional, Derecho Civil, Derecho comercial, Derecho Penal, etc.). Esta nueva realidad nos pone frente al desafío de encontrar fórmulas eficaces de aplicación del Derecho, en nuestro caso, del Derecho Penal, porque constituye también parte esencial del desarrollo tecnológico y comercial del mundo entero.

Como es sabido, el uso de sistemas informáticos forma desde hace mucho tiempo una pieza clave en la vida de cada individuo, el cual se ve sujeto a la necesidad de tener una computadora, una base de datos, la red, etc. Como medio para realizar diversas conductas en su vida diaria.

Mucho se habla de los grandes beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, sin embargo, el desarrollo tan amplio de la tecnología informática han aportado a la sociedad actual, sin embargo, el desarrollo tan amplio de la tecnología informática ofrece también un aspecto negativo, ya que

se han generado nuevas conductas antisociales y delictivas que se manifiestan en formas que no era posible imaginar en el siglo pasado. Los sistemas de computadoras ofrecen oportunidades nuevas y muy complejas de infringir la ley y han creado la posibilidad de cometer delitos tradicionales en formas no tan tradicionales.

Es innegable, pues que los avanzados cambios en la tecnología de los sistemas provocan una serie de cambios en la realidad social. Estos cambios, quiérase o no, repercuten en todas las personas que utilizan estos medios informáticos, ya sea por motivos laborales, como de entretenimiento.

La respuesta a esta necesidad de normar el entorno informático se ha puesto de manifiesto con iniciativas globales como El Convenio sobre la ciberdelincuencia fue firmado en Budapest el 23 de noviembre del 2001 y la más reciente normativa peruana de los delitos informáticos.

Parafraseando a Manuel Castells, en ocasión de un discurso del 2001, y hablando del "caos" positivo que Internet genera en la comunicación, dijo: "Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los trasgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces. La definición de la trasgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España"[1]

[1] "Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico2001-2002 de la UOC.

INDICE

UNIDAD I

CONOCIMIENTOS TECNICOS

PREGUN TAS GUÍA

1. ¿Cuáles son los riesgos que se presentan en el mundo respecto al uso de las nuevas tecnologías y que deberían promover los Estados para generar un verdadero impacto para mejorar la seguridad de la información?

2. ¿Qué información contiene los datos de tráfico y cuál es su importancia en la investigación de los delitos informáticos?

3. ¿Quién asigna las direcciones IP y qué importancia tiene esta en la investigación de delitos informáticos?

4. ¿Conociendo las capacidades con las que cuentan las modalidades delictivas en la red, cuáles de ellas servirían para la comisión de delitos informáticos a la luz de la legislación nacional?

PRIMER CAPÍTULO: LA SOCIEDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LOS DERECHOS

a) La Sociedad de la Información.

Partimos este capítulo por definir un concepto fundamental que engloba a muchos temas que desarrollaremos a lo largo de este curso con el fin de tener un panorama bastante claro de sus alcances, algunas definiciones esbozadas son las siguientes:

"…*Sociedad que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material…*". [2].

"…*Nuevo sistema tecnológico, económico y social, una economía en que el incremento de la productividad no depende del incremento cuantitativo de los factores de producción, capital, trabajo, recursos naturales, sino de la aplicación del conocimiento e información a la gestión, producción y distribución, tanto en los procesos como en los productos..*" [3]

"…*El término Sociedad de la información se refiere a una forma de desarrollo económico y social en el que la adquisición u diseminación de la información con vistas a la creación de conocimiento y a la satisfacción de las necesidades de las personas y de las organizaciones, juega un papel central en la actividad económica, en la creación de riqueza y en la definición de la calidad de vida y las prácticas culturales de los ciudadanos…*". [4]

"…*Las sociedades de la información se caracterizan por basarse en conocimiento y en los esfuerzos por convertir la información en conocimiento. Cuanto mayor es la cantidad de la información generada*

[2] Yoneji Matsuda, La Sociedad Informatizada como sociedad post-industrial, Tecnos 1994
[3] Manuel Castells, La era de la Información. 1998.
[4] Misión para la Sociedad de la Información, Libro verde sobre la Sociedad de la Información en Portugal, 1997.

por una sociedad, mayor es la necesidad de convertirla en conocimiento, Otra dimensión de tales sociedades es la velocidad con que tal información se genera, transmite y procesa. En la actualidad, la información puede obtenerse de manera prácticamente instantánea y, muchas veces a partir de la misma fuente que la produce, sin distinción de lugar…". [5]

A partir de estas definiciones y las múltiples que podemos encontrar en diversos foros internacionales, podemos definir algunos elementos característicos, como son:

- ✓ Se considera una etapa del desarrollo social.
- ✓ Se precisa de una capacidad de los ciudadanos, empresas y el mismo Estado a través de sus diversas instituciones, para obtener y compartir información, que atendiendo a los fines de las instituciones públicas comprenden las iniciativas por la transparencia y el acceso a la Información pública.
- ✓ La Accesibilidad de la información es también un rasgo característico, como lo permite ahora la Internet y los portales que apuntan a contenidos cada vez mas amigables para el público usuario, incluso rompiendo barreras de cualquier discapacidad.
- ✓ Disponibilidad de Contenidos de manera instantánea.

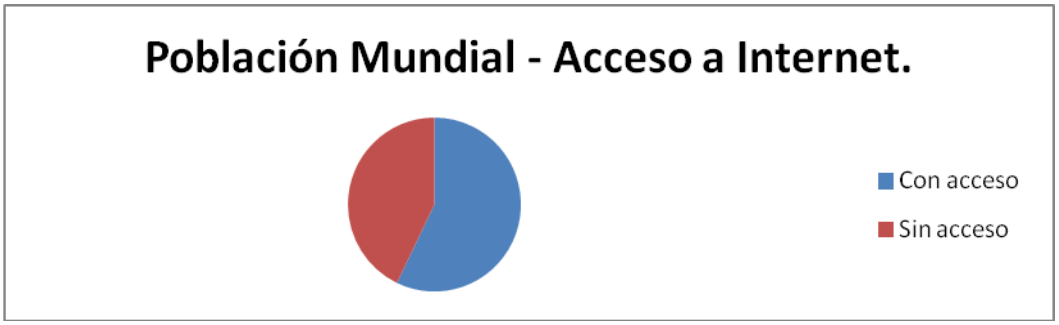
Es interesante notar de las estadísticas sobre el grado de penetración de las nuevas tecnologías en los ciudadanos, que la posibilidad de acceder a terminales móviles es mayor, incluso se habla que en el Perú la cantidad de equipos supera a la cantidad de habitantes, a Diciembre del 2015 en el mercado peruano había 34 millones 240 mil celulares los cuales ya consumen un promedio de S/. 27 soles mensuales, según el Organismo Supervisor de la Inversión Privada en Telecomunicaciones (Osiptel), asimismo el crecimiento del sector es de 7.4 por ciento entre el 2014 y 2015,

[5] Julio Linares et Alii. Autopistas Inteligentes, Fundesco 1995.

generando para los operadores móviles una ganancia S/8,885 millones en total[6].

En el caso de líneas fijas que en la actualidad están enlazadas los sistemas ADSL que transmiten datos y permiten el acceso a Internet a velocidades que permiten incluso la videoconferencia, se tiene que en el 2015 habían 2,97 millones de líneas fijas en servicio, esta cifra representaba el 2,3 % menos de los registrado a fines del 2014.

Asimismo en lo que respecta a Internet, la misma que a la fecha del presente material, cumple ya 47 años de creación, cuenta con 3 mil 424 millones de usuarios en el mundo. En el Perú, los internautas sobrepasan los 11 millones (37 por ciento de la población) con un promedio de 26 años de edad.



A nivel mundial 4 billones de personas de los 7 billones de habitantes no tienen acceso a Internet.

El 29% del total de usuarios en el Perú tiene un Smarthphone y el 11% una Tablet, asimismo analizando desde donde se realiza la conexión a internet se tiene que el 66% ingresa a través de computadoras de escritorio, 31% por Laptops, 30 % por Smartphones, 11.5% por celulares, 7% por tablets y 2 % por Smart Tv.

Al mismo tiempo, los avances en la tecnología y la digitalización están transformando las ciudades, economías y los medios de hacer negocios, lo

[6] http://larepublica.pe/impresa/economia/767312-cada-linea-movil-consume-un-promedio-de-s27-al-mes-informo-osiptel

que se considera actualmente la "Cuarta Revolución Industrial" , este entorno es adecuado para todos los actores involucrados con inimaginables soluciones para las mas preocupantes situaciones que el mundo necesita.

Estos cambios y la introducción de nuevos medios de comunicación a la fecha permiten también nuevas formas de contratación de personal y de la manera como es que desarrollamos nuestro trabajo, generando cambios importantes en la legislación.

Así como se da un crecimiento de medios de comunicación, también va en crecimiento un fenómeno importante que es la cyber dependencia, y la posibilidad que en la actualidad se tenga una nueva clasificación en cuanto a analfabetismo como lo es el digital.

Es importante también referir que la posibilidad de acceder a información y tener la posibilidad de compartirla y generarla, atendiendo a que información se produce, implica riesgos importantes para el ciudadano, con la proliferación de redes sociales gratuitas (Whatsapp, Facebook, Twitter, Instagram) que permiten desde la sola comunicación por voz , hasta las mas completas generar un álbum público de la vida, virtudes y problemas, que por estar ahora expuestos en redes públicas como lo es Internet y almacenadas en miles de servidores alrededor del mundo generan una especie de perpetuidad, en la que la posibilidad de recuperar dicha información es técnicamente posible, así como armar un perfil personal que es ya de interés de empresas que buscan en ellas tendencias de los consumidores, o de ciberdelincuentes que logran con solo este nivel de acceso a información poder ingresar a la intimidad y actividades habituales de cualquier potencial víctima.

Es en este entorno en que la colaboración entre países es importante para afrontar los nuevos riesgos que se producen en cada sector de la sociedad, como son:

a) Riegos de cyber seguridad.[7]

b) El intercambio de datos entre países.- ahora denominado "*El petróleo del siglo XXI*" [8] necesita marcos legales adecuados para que la economía realmente aproveche las ventajas de la digitalización, así como es necesario una adecuada protección a favor de los derechos fundamentales, la privacidad, transparencia, control de los mensajes encriptados, temas de propiedad intelectual, regímenes adecuados que controlen la transferencia de datos entre países y el impacto de la propiedad de los datos en la competitividad.

Finalmente concluimos que la posibilidad de acceder, así como el uso continuo y popular de las TICS y la adopción de las mismas en diversas actividades de la vida diaria, no es independiente o detonante para el crecimiento de la competitividad y la productividad tanto del sector empresarial como lo es la ciudadanía en general, para que este verdaderamente genere un impacto es necesario fortalecer desde el Estado mediante políticas públicas proyectos que permitan el fortalecimiento de las capacidades del recurso humano y alianzas del sector público y privado en apoyo al fomento de la creatividad tecnológica y redoblar esfuerzos para fomentar conciencia en seguridad de la información.

b) El Derecho al Secreto de las Comunicaciones.

El secreto de las comunicaciones es reconocido como una garantía constitucional en todas las constituciones y normas internacionales, como por ejemplo la Declaración Universal de los Derechos Humanos[9] en su artículo 12 al establecer que ***".nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y si reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias y ataques…"***

[7] http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf
[8] http://www.elfinanciero.com.mx/tech/big-data-se-convertira-en-el-petroleo-del-siglo-xxi.html
[9] http://www.un.org/es/documents/udhr/

El en Pacto Internacional de Derechos Civiles y Políticos[10] en su **artículo 17** dispone:

"…1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. …"

El alcance que ha tenido las nuevas tecnologías y su interrelación con los ciudadanos permite concluir que los ciudadanos han puesto en manos de terceros por del uso de servicios online gratuitos en su mayoría, una gran cantidad de información que tienen que ver con su vida privada, su familia, datos acerca de su domicilio, correspondencia, así como del seguimiento de sus actividades se puede obtener perfiles personales, sicológicos, tendencias, historia personal, enfermedades, relaciones personales, contactos, tendencia de sus contactos, opiniones a lo largo del tiempo entre otras que van de la mano con la posibilidad del desarrollo personal y económico del individuo, que requieren una adecuada protección.

La posibilidad de abrir gran cantidad de información no relevante para la investigación con contenido personalísimo del ciudadano debe de ser tratada de manera segura, mediante protocolos debidamente establecidos y con límites claros en cuanto a la información a ser desclasificada para un proceso penal.

En la actualidad el secreto de las comunicaciones no es solo una garantía de la libertad individual sino implica de manera trasversal múltiples derechos y libertades como la propiedad, la libertad de opinión, ideología, pensamiento, empresa, información médica, tal como lo ha señalado el Tribunal Constitucional español en la SSTC 281/2006[11] ,

[10] http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx
[11] https://www.boe.es/diario_boe/txt.php?id=BOE-T-2006-19899

56/2003[12] y 123/2002[13], constituye una **garantía de pluralismo y de la democracia.**

En el Perú el inciso 10) del artículo 2º de la Constitución protege el secreto y la inviolabilidad de la comunicación en todas sus formas o medios, como son el telefónico, el telegráfico o el informático, es decir, aquella comunicación que se mantiene a través de un determinado medio o soporte técnico.

El Tribunal Constitucional en la STC 01058-2004-AA/TC ha precisado que "*…toda persona tiene derecho a que sus comunicaciones y documentos privados sean adecuadamente protegidos, así como a que las mismas y los instrumentos que las contienen, no puedan ser abiertas, incautadas, interceptadas o intervenidas sino mediante mandamiento motivado del juez y con las garantías previstas en la ley…*".[14]

La Corte Interamericana de Derechos Humanos en la sentencia del Caso *Escher y otros vs. Brasil*[15], del 6 de julio de 2009, ha enfatizado que la "*..Convención Americana protege la confidencialidad e inviolabilidad de las comunicaciones frente a cualquier injerencia arbitraria o abusiva por parte del Estado o de particulares, razón por la cual tanto la vigilancia como la intervención, la grabación y la divulgación de esas comunicaciones quedan prohibidas, salvo en los casos previstos en ley y que se adecuen a los propósitos y objetivos de la Convención Americana…*".

El Tribunal Europeo de Derechos Humanos precisa que la vida privada es un término abierto no susceptible de una definición exhaustiva, que " *debe ser interpretado a la luz de las condiciones actuales de vida propias de la Sociedad de la Información en la que estamos inmersos para*

[12] http://hj.tribunalconstitucional.es/es/Resolucion/Show/4831
[13] https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/7._Sentencia_123-2002_de_20_de_mayo_de_2002._def.pdf
[14] Tribunal Constitucional en la STC 01058-2004-AA/TC
[15] http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

proteger al individuo de forma real y efectiva en aquellos ámbitos a los que se refiere…"[16]

El Derecho al secreto de las comunicaciones tiene una estrecha relación con el derecho a la intimidad y la confidencialidad tanto en el proceso de la comunicación como lo es del contenido de lo comunicado, lo lesivo en la lesión al derecho del secreto de las comunicaciones no es tanto el contenido de la misma, sino que un tercero intervenga en la comunicación sin autorización o revele su contenido, por lo que es posible atentar contra este derecho sin llegar necesariamente a la esfera íntima de la persona.

La titularidad del derecho puede serlo para personas como a la ficción persona jurídica, la interceptación por parte de las autoridades competentes esta bajo la respectiva autorización judicial bajo el análisis de criterios de proporcionalidad y análisis de la necesidad de una intervención inmediata para la prevención, averiguación del delito, descubrimiento de crimen organizado y obtención de pruebas.

La Sentencia del Tribunal Constitucional Español STC 123/2002[17] explica el ámbito de alcance del secreto de las comunicaciones, la misma que no solo cubre su contenido sino todos los aspectos de la misma, como la identidad de los interlocutores, la existencia de la comunicación, confidencialidad de las circunstancias o datos externos de la comunicación telefónica(datos técnicos), momento, duración, destino, independiente del carácter público o privado de la red de transmisión de la comunicación.

c) Protección de los datos de tráfico.

Es interesante empezar definiendo que se entiende por Datos de Tráfico.

16 http://ruc.udc.es/dspace/bitstream/handle/2183/9158/comunicacions_15_LopezBarajas_Perea_517530.pdf?sequence=1

17 http://hj.tribunalconstitucional.es/es/Resolucion/Show/4659

Gonzales López, J.J[18] lo define como "…*Las informaciones que se generan o tratan en el curso de una comunicación y difieren de su contenido material, entendiendo por tal aquella información cuya transmisión voluntaria por el emisor al receptor motiva la comunicación…*"

El Convenio 185 del Consejo de Europa, sobre Ciberdelincuencia[19], de 23 de Noviembre del 2001 define datos de tráfico en su artículo1.d) como todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, el tiempo, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

La importancia de la información que contiene estos denominados "Datos de Tráfico" es en cuanto en la técnica de investigación es importante acceder a los mismos puestos que se obtiene información de importancia para un futuro proceso penal, como lo es identificación de la dirección IP, proveedor de servicios de Internet, MAC o IMEI del equipo entre otras, con ello se puede identificar a otros miembros en caso de organizaciones criminales.

La delimitación de este concepto permitirá definir los limites en los cuales se llevará adelante una intervención, que puede realizarse tomando conocimiento de la conversación telefónica o por medio de cualquier red social, o la mera observación sin llegar a conocer el contenido de la conversación pero si de su existencia, sus interlocutores y de su duración.

El acceso a los datos de tráfico reviste importancia atendiendo a la proliferación de sistemas y programas que permiten la geolocalización por medio de equipos GPS[20] , en el Perú tenemos el Decreto Legislativo 1182

[18] Gonzales López J.J , Retención de datos de tráfico de las telecomunicaciones y proceso penal" , en VV.AA. , Estudios jurídicos sobre la Sociedad de la Información y nuevas tecnologías. Libro con motivo del XX Aniversario de la Facultad de Derecho, Servicio de Publicaciones de la Universidad de Burgos, Burgos 2005, pás, 275-394

[19] https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

[20] Sistema de Posicionamiento Global.

que "Regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado" el mismo que establece condiciones y procedimientos para acceder desde la fuente o proveedor de dichos servicios a información que permite la pronta localización de personas investigadas.

Asimismo la citada norma obliga a todas las empresas concesionarias de servicios públicos a almacenar por tres años toda la información de los datos derivados de las telecomunicaciones para que pueda ser consultada por la Policía.

Incluimos en el presente material para la reflexión la siguiente cita del Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informe de la Oficina del Alto Comisionado y del Secretario General[21]

"….En la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos. Como ha señalado el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, los avances tecnológicos entrañan que la eficacia de la vigilancia realizada por el Estado ya no se ve limitada por su magnitud o duración. La disminución de los costos de tecnología y almacenamiento de datos ha eliminado los inconvenientes financieros o prácticos de la vigilancia. El Estado no había tenido nunca la capacidad de que dispone actualmente para realizar actividades de vigilancia simultáneas, invasivas, con objetivos precisos y a gran escala[22] Es decir, las plataformas tecnológicas de las que depende crecientemente la vida política, económica y social a nivel mundial no solo son vulnerables a la vigilancia en masa, sino que en realidad pueden facilitarla.

[21] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_sp.doc

[22] http://www.creativecommons.uy/wp-content/uploads/2014/12/Declaraci%C3%B3n-10-de-diciembre 2014_Vigilancia-Seguridad-Privacidad.pdf

SEGUNDO CAPITULO: REDES Y TELECOMUNICACIONES.

a) Definición de Red de Telecomunicaciones.

A tenor de la norma especial tenemos la dada por el DECRETO SUPREMO Nº 039-2007-MTC[23] que establece la definición de Red de Telecomunicaciones como "… *La Infraestructura necesaria para la prestación de servicios públicos de Telecomunicaciones o instalación que establece una red de canales o circuitos para conducir señales de voz, audio, datos, textos, imágenes u otras señales de cualquier naturaleza, entre dos o más puntos definidos por medio de un conjunto de líneas físicas, enlaces radioeléctricos, ópticos o de cualquier otro tipo, así como por los dispositivos o equipos de conmutación asociados para tal efecto…*"[24]

b) Conectividad.

Es importante iniciar este módulo que contiene conocimientos técnicos básicos para el análisis técnico legal, definiendo lo que se entiende por "Conectividad", organismos internacionales (ONU, OCDE) refieren dicho término para describir los artefactos tecnológicos que proporcionan la conexión física a las infraestructuras de tecnologías de información y comunicación.

La conectividad implica equipamiento que permite la interacción entre la información en formato digital y el usuario final, la misma que pasa, atendiendo a la infraestructura de las redes que la soportan diversas vías y accesos directos entre los diferentes puntos de una red.

Los usuarios, los terminales por los cuales acceden a Internet y los servidores que almacenan y administran información, entre otros como los que proveen seguridad a la red, integran lo que denominamos red, la misma que está interconectada a las redes mundiales de la sociedad de la información donde se ramifican, sin un contexto de fronteras físicas

[23] http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_1335.pdf
[24] DECRETO SUPREMO Nº 039-2007-MTC

territoriales. Estar en la red es el primer paso para tener acceso al ciberespacio.

El Perú ocupa el puesto 34 en conectividad a nivel mundial, esto debido al creciente mercado de las telecomunicaciones, esto basado en el Informe de Conectividad Global del 2015[25] elaborado por la empresa Huawei, en donde proyectos importantes como la construcción de la red nacional de fibra óptica permiten a la fecha ofrecer al país de banda ancha, necesaria para una adecuada virtualización de las actividades productivas.

Asimismo y tal como referimos en páginas anteriores en el Perú la adquisición de smartphones aumentó en un 35 por ciento superando a países como Colombia que llegó a un 25 %.

A nivel global, Estados Unidos está a la cabeza, en temas de conectividad. seguido por Suecia, Singapur, Suiza, Reino Unido.

Un crecimiento en la **conectividad** global permite crear una plataforma de información y colaboración para empresas y gobiernos con el fin de identificar, impulsar y crear nuevas oportunidades en la **economía digita**l para construir un mundo mejor conectado.

c) Banda ancha.

El concepto de banda ancha fue empleado originalmente para designar las transmisiones en las que se utilizaban múltiples canales de forma simultánea, por oposición a *banda de base*, que aludía a la transmisión en un único canal en un momento dado, está relacionado generalmente con la velocidad de transmisión de datos, la velocidad de conexión a Internet.

La velocidad de conexión a Internet se mide en *kilobits* o *megabits* por segundo (kbit/s), a mayor velocidad mejor calidad con la que se descargan datos de la red, sea esta transmisiones multimedia, de voz, etc.

[25] **www.huawei.com/minisite/gci/en/**

Un 57% de la población de América Latina cuenta con cobertura de banda ancha y un 90% de la población latinoamericana (571 millones de personas) vive en zonas con cobertura de red 3G o 4G.

d) Topología de las redes:

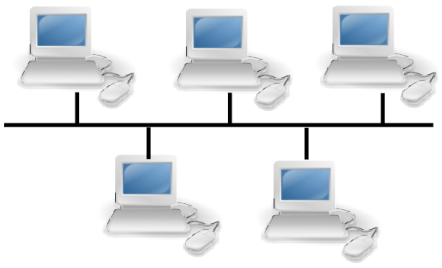
La topología de una red representa la disposición de los enlaces que conectan los nodos de una red, las redes pueden ser conformadas por diversas configuraciones y dependiendo de cómo es que se hayan conectado los nodos o terminales se establecerá el tipo.

- **La topología física** explica la configuración de cables, antenas, computadores y otros dispositivos en la red.

- **La topología lógica**, es un nivel mas abstracto, considerando el método como es que se desarrolla el flujo de información entre los nodos.

Atendiendo a la configuración física de la red tenemos:

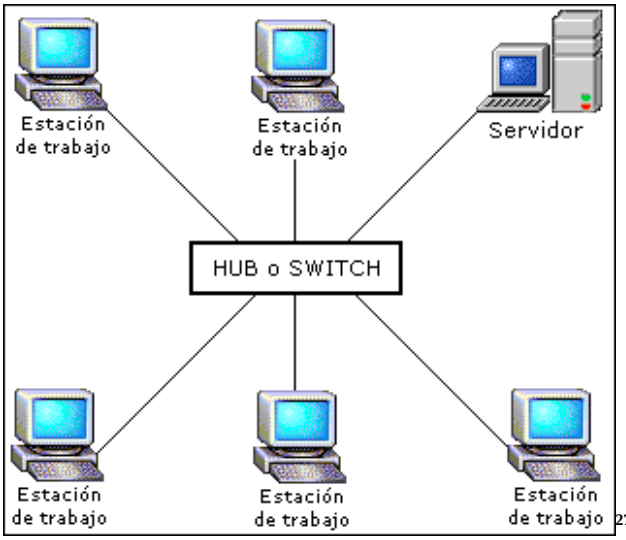
a) Bus o barra: todos los nodos están conectados a un cable común o que comparten, por ejemplo las redes Ethernet.



[26]

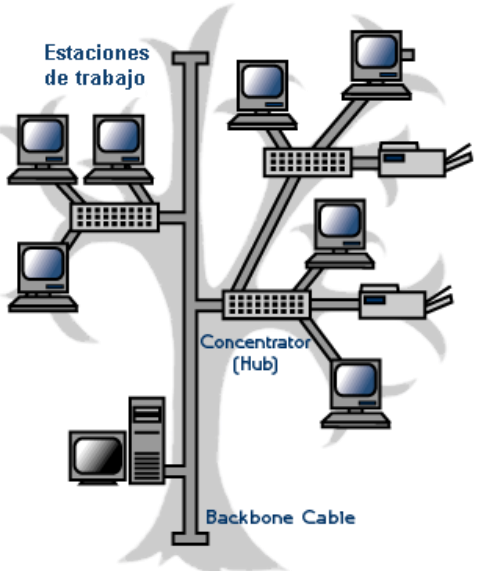
[26] http://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/

b) Estrella: Cada nodo se conecta directamente a un concentrador central, todos los datos pasan a través de ella antes de alcanzar a su destino , por ejemplo en redes Ethernet e inalámbricas WIFI.



[27]

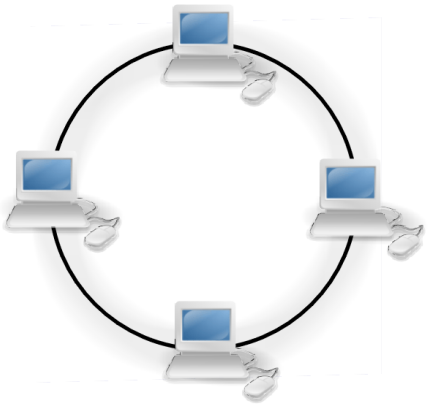
c) Árbol: Es una combinación entre las topologías Bus o Barra y la Estrella, una o varias redes estrella se conectan directamente a una dorsal denominada (BACKBONE)



[28]

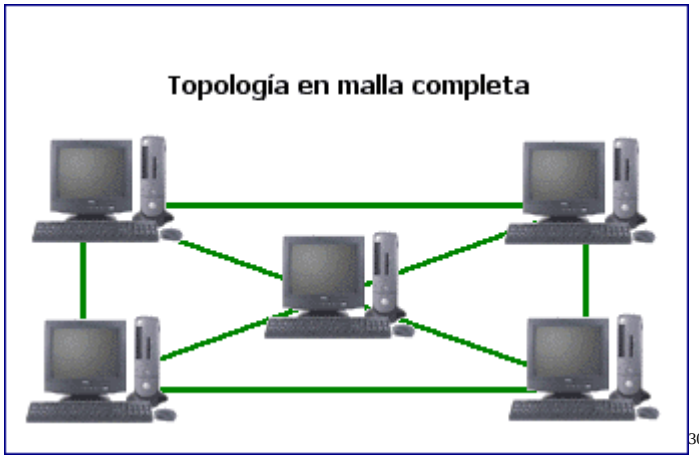
[27] http://topologias4conalep.blogspot.pe/p/topologia-en-estrella-y-estrella.html
[28] http://infor503redes.blogspot.pe/2014/12/topologia-de-arbol.html

d) Anillo: Todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta directamente a dos dispositivos vecinos, la infraestructura es tipo dorsal (Backbone) de fibra óptica.



[29]

e) Malla Completa: Enlace directo entre todos los pares de nodos de una red.



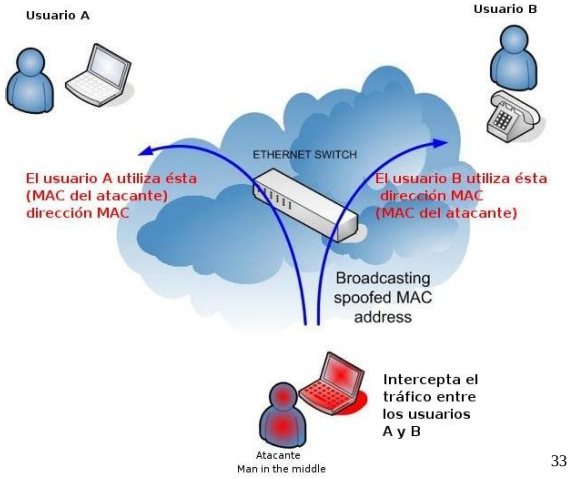
[30]

f) Malla Parcial: algunos nodos están organizados en malla completa, mientras otros se conectan a uno o dos nodos de la red.

[29] http://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/
[30] http://modul.galeon.com/aficiones1366341.html

g) Comunicación Inalámbrica.

En el caso de **comunicación inalámbrica** esta se desarrolla en dos sentidos por lo que es Bidireccional desde el punto de acceso (Access point), en el caso de sniffing[31] (monitoreo) pasivo o eavesdropping[32] (escucha subrepticia) la comunicación no sería bidireccional.



33

Ejemplo de ataque tipo eavesdropping (escucha subrepticia)

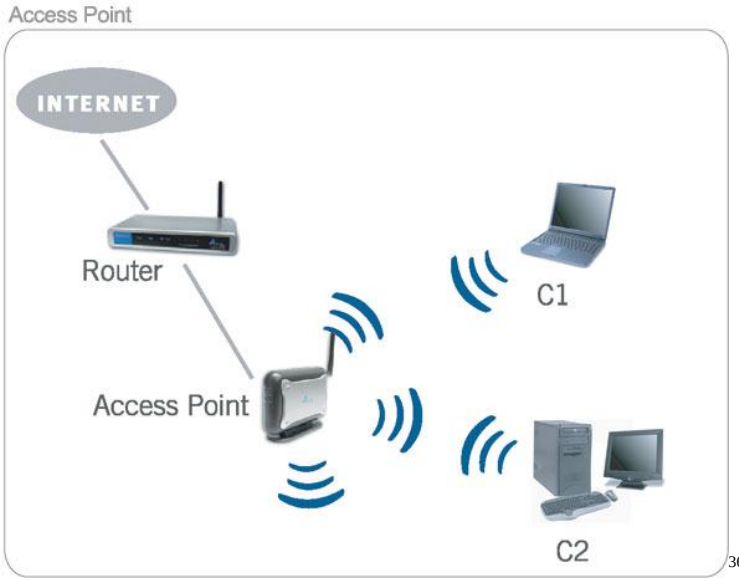
Los enrutadores (routers) inalámbricos tienen la función combinada de dar acceso y enrutar la información por IP.

34

[31] http://www.internetmania.net/int0/int93.htm
[32] http://blog.txipinet.com/2006/10/11/40-seguridad-en-voip-iii-captura-de-conversaciones-o-eavesdropping/
[33] http://blog.txipinet.com/2006/10/11/40-seguridad-en-voip-iii-captura-de-conversaciones-o-eavesdropping/
[34] https://sites.google.com/site/wiilkersite/otros-tipos-de-harware

En una red inalámbrica se pueden encontrar trabajando de manera conjunta equipos inalámbricos como puntos de acceso, esta facilidad lo dan ahora equipos con sistemas operativos Android[35], los que permiten compartir la señal de WIFI a cualquier dispositivo en su alcance.

Los puntos de acceso (Access Point) permiten captar la señal de los enrutadores, amplificándolas para dar mayor cobertura a la red, dependiendo del poder de las antenas insertas en la misma y la potencia del equipo.

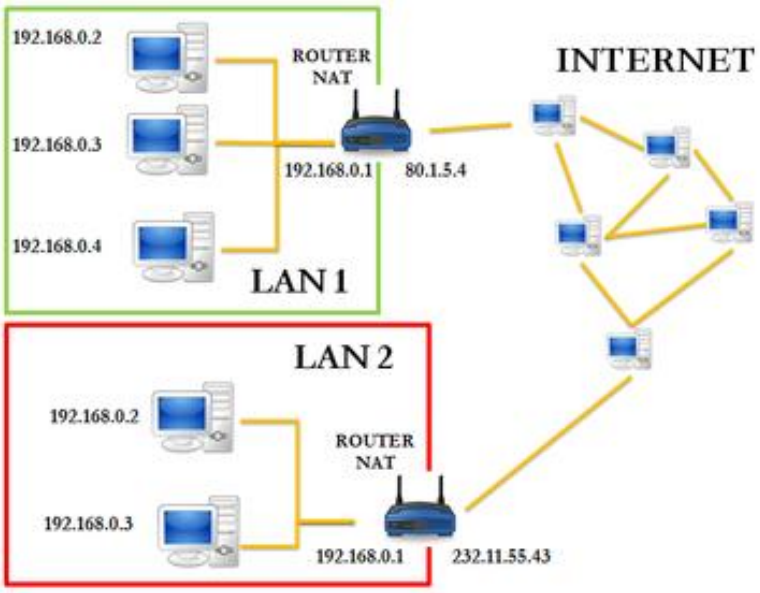


[36]

[35] https://www.android.com/
[36] http://fergs87.blogspot.pe/2012/10/access-point-vs-repetidor.html

Enmascaramiento: o NAT (Network Adress Traduction) permite comunicar terminales a una red externa como Internet, los paquetes de datos administrados por la red local interna con direcciones IP locales son pasados al Enrutador que modifica la información de la Dirección IP y el número de puerto enviándolas a Internet **con una dirección IP UNICA**, al recibir respuesta del host remoto, el enrutador devuelve la modificación realizada al paquete, para que llegue a la red interna y consecuentemente al equipo origen.

Los equipos de los clientes, se conectan a un punto de acceso mediante el nombre asignado, este procedimiento de identificación se le conoce como SSID Service Set Identifier (Identificador del Conjunto del Servicio).



[37]

e) PROTOCOLOS DE COMUNICACIÓN VÍA INTERNET.-

La comunicación por medio de las redes es mediante el denominado protocolo TCP / IP es un tipo de sistema codificador que permite a las computadoras describir datos electrónicamente.

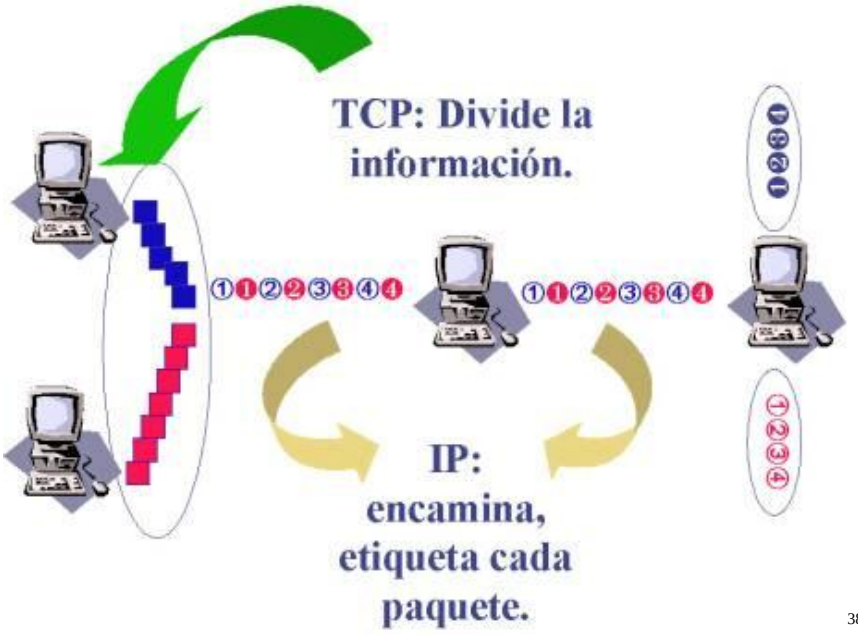
[37] https://aula-informatica-4a.wikispaces.com/T1-12.+Direcciones+reservadas

Dicho término describe dos partes: el protocolo de control de transmisión (Transmision control protocol TCP) y el protocolo de Internet (Internet Protocol: IP)

Cada terminal que accede a Internet interpreta dichos protocolos y los utiliza para el envío o recepción de datos a lo largo de la red.

El TCP/IP crea el paquete conector, un tipo de red que intenta lograr minimizar la perdida de datos que se envía por el cableado.

El TCP fragmente cada pieza de datos, agrupándolos en pequeños conjuntos denominados paquetes, los cuales son codificados electrónicamente.



[38]

El TCP/IP es una de las mas importantes de una lista de protocolos de Internet, existen protocolos de traslados de correos simples (simple mail transfer protocol : SNTP) , protocolos de transferencias de archivos (file

[38] http://tecnologiaedu.us.es/cursos/29/html/cursos/tema7/cont_2.2.htm

transfer protocol : FTP) y protocolos de transferencia de telnet (telnet transference protocol: TTP)

Ejemplo configuración TCP/IP

Dirección IP	192.168.0.15
Máscara de subred	255.255.255.0
Puerta de enlace	192.168.0.254
DNS preferido	80.58.0.33
DNS alternativo	80.58.32.97

[39]

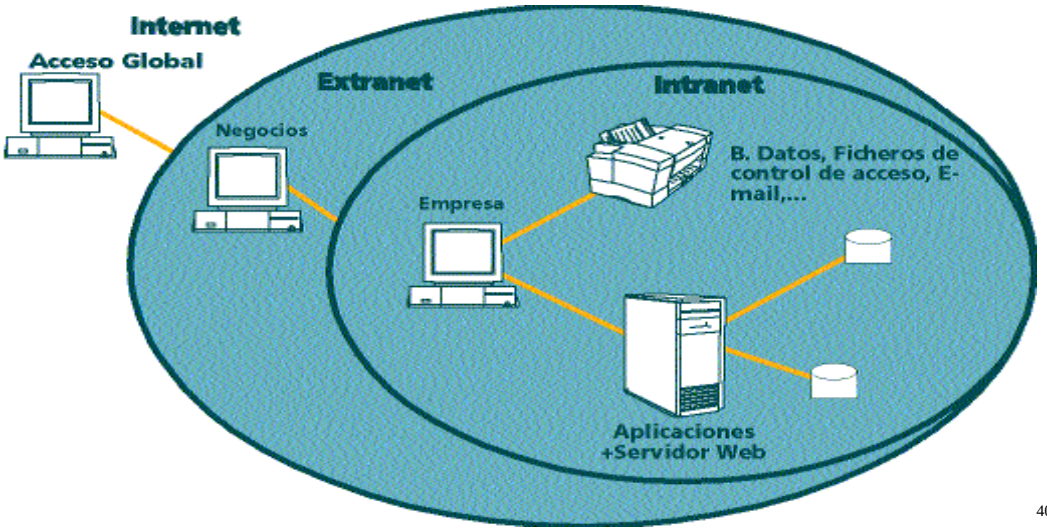
f) Intranet y Extranet, Internet.

La Intranet es una asociación de pequeñas redes dentro de una empresa u organización sin acceso público, funciona de manera similar a la web con el uso de browsers (por ejemplo Chrome, Explorer) , servidores de Web y páginas web, pero de uso interno.

Por su parte, La Extranet está conformada por varias Intranet unidas que comparten información, esto permite un trabajo colaborativo, el enlace es permitido por redes privadas, dedicadas o el uso de la Internet pública.

La Internet, es la asociación global de computadoras que llevan datos y hacen posible el intercambio de información, La World Wide Web es un subconjunto de Internet, una colección de documentos relacionados que trabajan usando un protocolo de Internet llamado http (hiper text transfer protocol: protocolo de transferencia de hipertextos)

[39] http://recursostic.educacion.es/observatorio/web/eu/component/content/article/453-diseno-de-la-red-del-centro?start=2

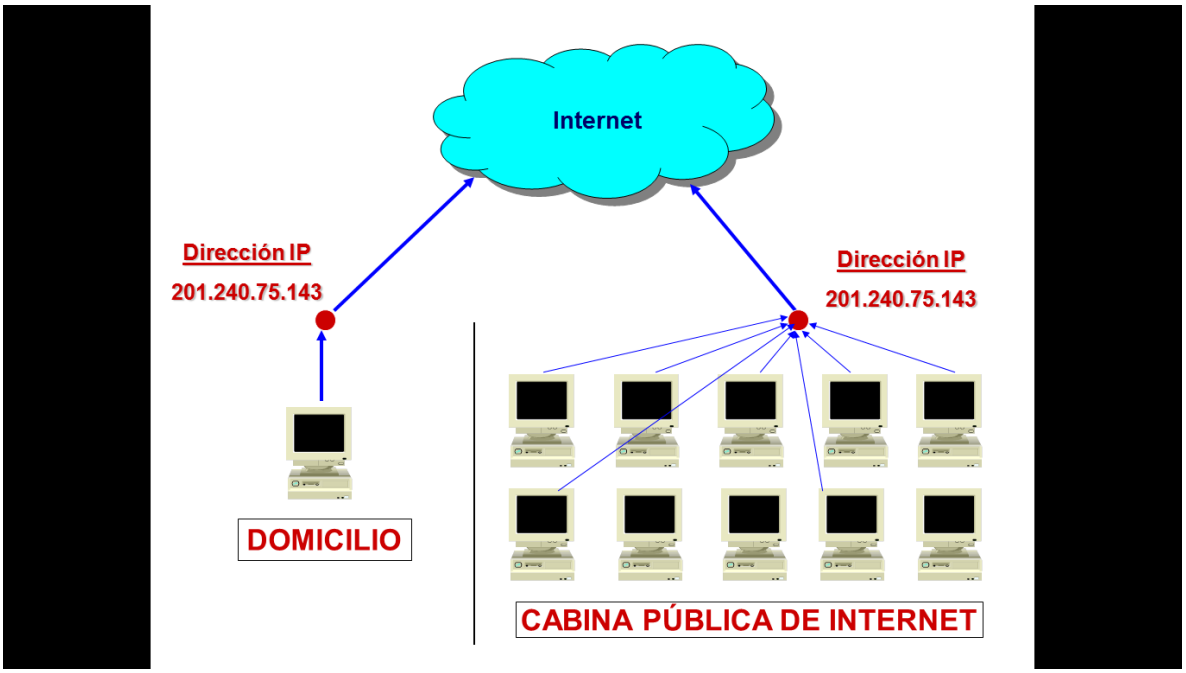


[40]

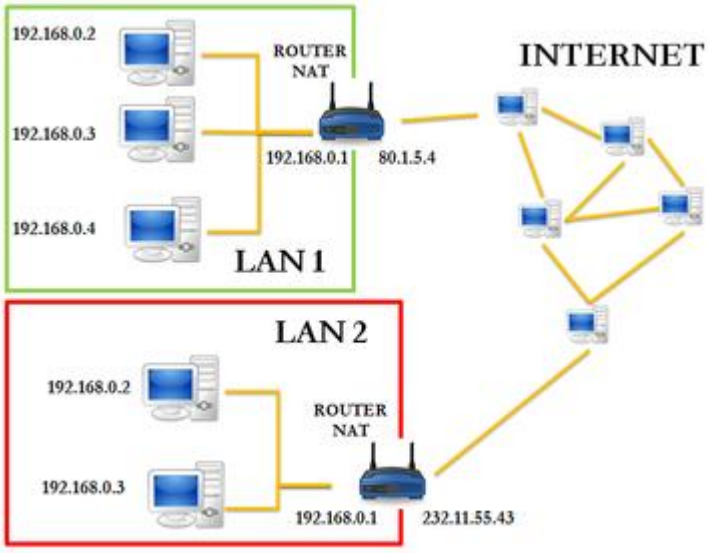
g) Dirección IP:

Es un número de cuatro a doce dígitos que identifica a una computadora específica conectada a internet. Los dígitos se organizan en cuatro grupos de números (que pueden ir de 0 a 255) separados por períodos (por ejemplo 1.160.10.230) dependiendo de cómo un ISP (Internet Service Provider: Proveedor de Servicios de Internet) asigna su dirección IP, usted puede tener una misma dirección todo el tiempo o una diferente cada vez que se conecta. Los servidores de Internet tienen el mismo tipo de direcciones, por ejemplo, si colocamos http://216.58.219.110 en nuestro buscador podemos acceder a www.google.com

[40] http://informaticafrida.blogspot.pe/2013/06/internet-intranet-extranet.html



Interesante gráfico que detalla cómo es que se determina las direcciones IP en caso de un equipo en una red domiciliaria y el compartido en las Cabinas públicas de Internet.



[41]

Procedimiento: Dato interesante, como conocer la dirección IP de una website:

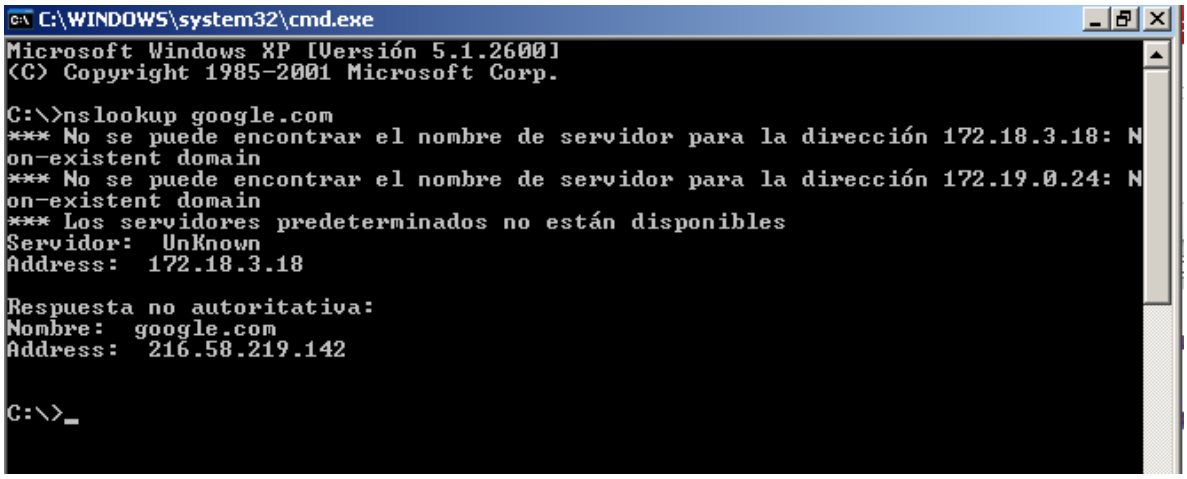
[41] https://aula-informatica-4a.wikispaces.com/T1-12.+Direcciones+reservadas

1.- En Windows busca el **botón INICIO**, escribe “**cmd**” y pulsa **ENTER**. Se

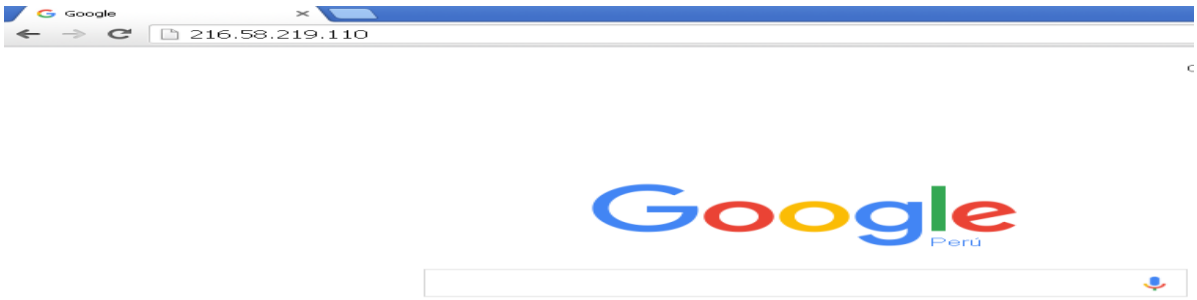
abrirá la consola MS-DOS de Windows.

2.-Ingresa el siguiente texto para ejecutar una acción de búsqueda:

Nslookup (página web *.com) o ejemplo Nslookup google.com



En este caso confirmamos que la Dirección IP es 216.58.219.142, siendo esto así remplazando en el Browser ingresan a www.google.com



42

[42] https://norfipc.com/redes/cambiar-direccion-ip-dinamica-estatica.html

TERCER CAPITULO: MODALIDADES DELICTIVAS Y TECNOLOGÍAS EMPLEADAS EN LOS DELITOS INFORMÁTICOS.

Para tener un conocimiento cabal de los delitos informáticos es necesario conocer los procedimientos, métodos, técnicas, tecnología que se emplea para acciones como sabotaje, alteración de datos, acceso no autorizado entre otros citados en las normas especiales.

Asimismo es preciso mencionar que los reportes al año 2015 de cibercriminalidad, detectada en primera línea por empresas especializadas en el rubro de seguridad de la información presentan un crecimiento en la creación de malwares y variantes, se han contabilizado en el año 2015 aproximadamente 84 millones de nuevas muestras de las 304 millones de muestras ya existentes y se neutralizan sólo por un proveedor de seguridad aproximadamente 230,000 ataques por día, dichas cifras se obtienen por mecanismos denominados “ Inteligencia colectiva” , siendo esta la información que se reporta minuto a minuto a nivel mundial desde los software especializados disponibles en todo terminal conectado a Internet.

Se informa de gran cantidad de ciberataques a empresas y websites, donde el atractivo principal para los ciberdelincuentes no es sino el robo de datos personales, que incluye los registros de usuarios que enlazan información como números de tarjetas de crédito o la posibilidad de habilitar pagos con los mismos, las víctimas a nivel mundial se cuentan en millones, pero algo peculiar sucede en este ámbito, la cantidad de incidencias no es concordante con el número de denuncias, investigaciones o procesos penales.

Una modalidad delictiva en crecimiento es el denominado Cryptolocker[43], que es el secuestro de información corporativa, en la que tu información contenida en diversos servidores pagos o simplemente en la

[43] http://www.pandasecurity.com/spain/mediacenter/malware/cryptolocker/

nube es íntegramente robada y solo accesible posteriormente con el pago de un rescate.

El hacking como modalidad delictiva está encontrando nuevas fronteras de acción como lo es ahora el hackeo de vehículos para poder controlarlos de manera remota o para acceder a la computadora de a bordo que permite en vehículos con seguridad por chip de encendido en la llave o los que tienen encendido por botón el poder encenderlos para robarlos, esta modalidad está en crecimiento y dichos software y hardware que permite el acceso al mismo está disponible en mercados negros presenciales y los virtuales en la Deep Web[44] (o la Web profunda) accesible mediante navegadores especiales y con contenido que va más allá de los límites de la imaginación.

En el transcurso de este artículo hemos comentado ya de términos nuevos que son modalidades como es que se cometen los cyberataques, muchos de ellos como tales no se encuentran detallados en las normas de delitos informáticos, puesto que la norma detalla únicamente la acción que genera una vulneración de algún bien jurídico y porque su creación es permanente y variable, lo que dejaría a la norma desfasada.

Empezamos por elaborar un glosario de términos:

a) **MALWARE**.- es un tipo de programa malicioso que puede ser capaz de propagarse por ejemplo: a través del adjunto de un correo electrónico y también como archivos a través de redes P2P (Peer to Peer redes que comparten datos a través de un software enlace por ejemplo Ares).

El programa puede tener la capacidad de cosechar direcciones de correo electrónico desde un terminal infectado, sin el consentimiento del usuario.

[44] https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

Una clase de Malware son los worms, o gusanos como el gusano de correo electrónico, un gusano P2P o un buscador de correo troyano.

a.1 El Caballo de Troya o “Trojan Horse”:

Método consistente en la inclusión de instrucciones dentro del programa de uso habitual de una rutina para que realice un conjunto de funciones, desde luego no autorizadas, para que dicho programa ejecute en ciertos casos de una forma distinta a como estaba previsto. Puede tratarse en determinados casos de la ejecución de cálculos erróneos, por ejemplo: aumentando el importe de la lista de un empleado, desviando ingresos hacia cuentas ficticias, etc. También puede presentarse cuando se imprimen documentos no autorizados o inclusive no imprimir documentos reales, emitir cheques a proveedores reales cuando previamente se les ha cancelado su deuda, ya que se ha alterado la forma de pago transfiriendo los fondos a una cuenta que pertenece al defraudador. Al igual que la conducta anterior, se trata de una manipulación fraudulenta de los sistemas o programas informáticos generalmente practicados con fines económicos.

Los troyanos tienen la capacidad de:

- ✓ Eliminar datos
- ✓ Bloquear datos
- ✓ Modificar datos.
- ✓ Copiar datos.
- ✓ Interrumpir el funcionamiento de computadoras o redes de computadoras.

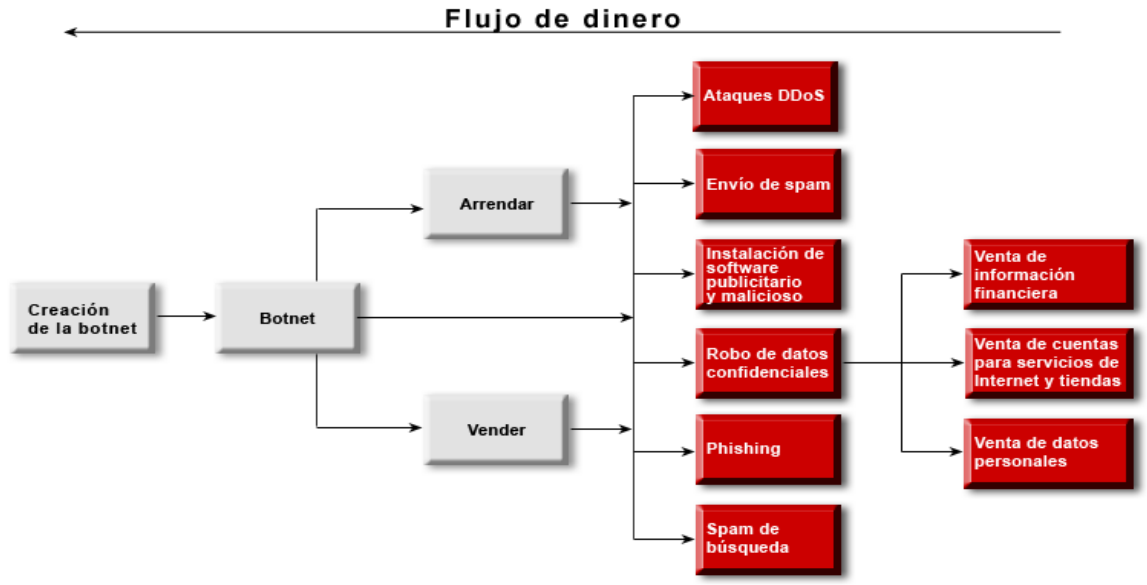
A diferencia de virus y gusanos, los troyanos no son capaces de autorreplicarse.

Los Troyanos se clasifican según el tipo de acciones que pueden realizar en su computadora.

a.2 Backdoor:

Ofrece control a distancia sobre la computadora infectada. Permiten por ejemplo enviar, recibir, ejecutar y borrar archivos, mostrar datos y reiniciar la computadora, a menudo se usan para unir un grupo de computadoras víctimas para formar la denominada red botnet[45] o zombie que son terminales controlados a distancia por el denominado Bot Master.

La siguiente gráfica demuestra cual es el valor que tiene el administrar una botnet, permite arrendar o vender esta red de equipos infectados para cometer ilícitos por ejemplo el ataque DDos que es la denegación de servicio, que incide directamente en impedir el acceso a determinadas website o contenidos sobrecargándolos de accesos falsos, el robo de datos confidenciales, phishing entre otras.



46

El gráfico demuestra como es que fluye el dinero una vez armada una red botnet, en la que la venta de información financiera, cuentas para servicios

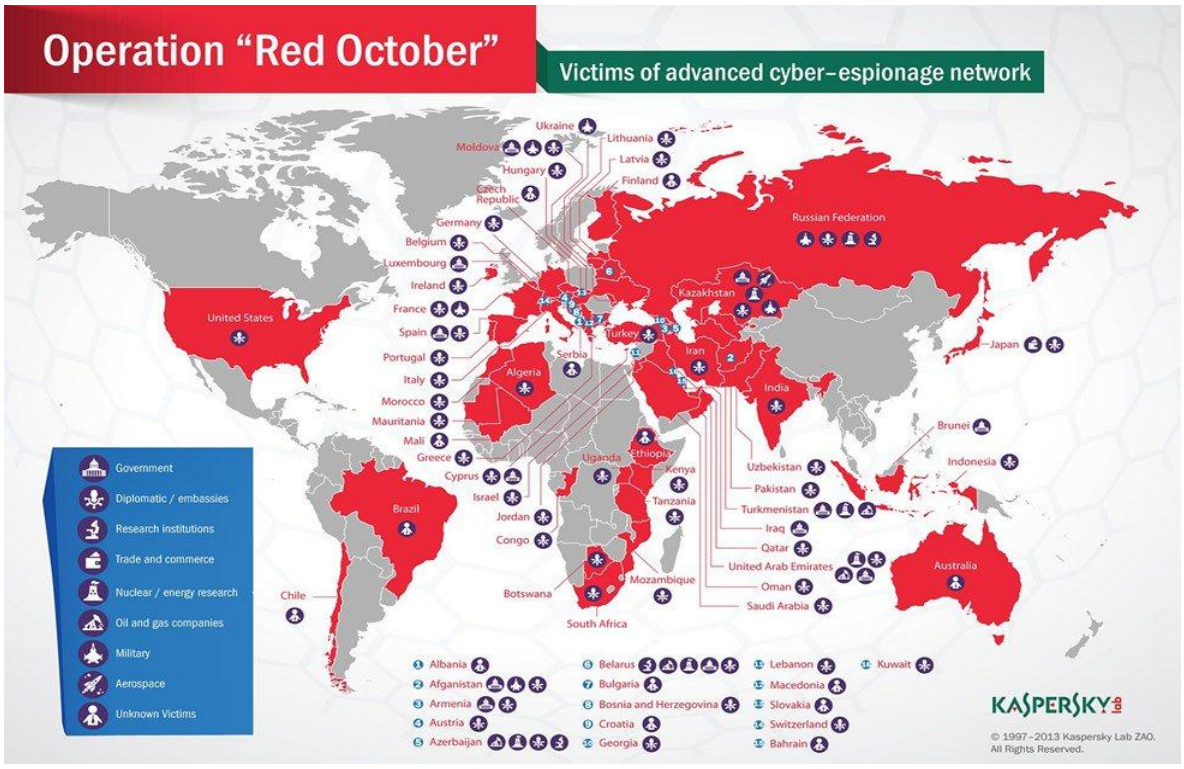
[45] http://www.gitsinformatica.com/botnet.html
[46] http://www.gitsinformatica.com/botnet.html

de internet y tiendas, y la valiosa venta de datos personales, constituyen la motivación de estas redes, es preciso mencionar que la misma no es lineal , sino que es una gran red de delincuentes que trabajan bajo funciones específicas.

a.3 Exploit (Aprovechamiento de vulnerabilidades)

Los Exploits son programas que sus datos o códigos aprovechan una vulnerabilidad dentro del software de aplicaciones que se ejecuta en la computadora que no se encuentren con sus actualizaciones de seguridad respectivas o que no hayan pasado algún control de calidad en seguridad de la información.

La siguiente gráfica demuestra el alcance que puede tener el aprovechamiento de las vulnerabilidades, como la presentada con el software Java, que permitió el ingreso y espionaje a redes informáticas personales, gubernamentales, militares entre otras.



a.4 Rootkit

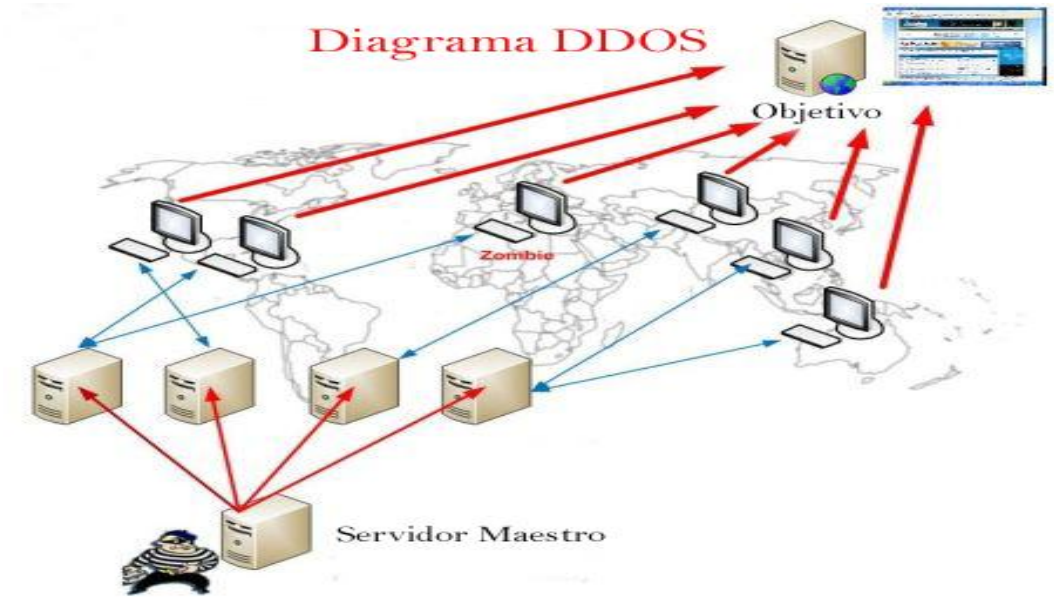
Diseñados con el fin de ocultar ciertos objetos o actividades en su sistema. La finalidad es evitar que programas maliciosos sean detectados, con esto logran permanencia en el terminal infectado.

a.5 Trojan-Banker

Son programas diseñados con el fin de robar los datos de cuentas de sistemas de banca en línea, sistemas de pago electrónico, y tarjetas de crédito y débito.

a.6 Trojan-DDoS

Son programas especializados para ataques DoS (denegación de servicio) contra el servidor(es) que contienen la administración de una dirección web. Generan varias solicitudes de acceso de manera remota incluso utilizando varias terminales controladas, el ataque consume el ancho de banda del servidor llevándolo a su límite, lo cual provoca que si un usuario desea acceder a la página web atacada el servidor emite un mensaje que se encuentra fuera de servicio o que se ha excedido el ancho de banda.



[47]

[47] https://losindestructibles.files.wordpress.com/2012/09/20091122-blog_ddos_attack_diagram-psd.png

a.7 Trojan-Downloader

Tienen la capacidad de descargar y actualizase de manera remota en su computadora, instalando troyanos y adware con publicidad no deseada y dirigida.

a.8Trojan-Dropper

Software letal que permite a los hackers instalar troyanos y virus, o para enmascararlos ante la presencia de programas antivirus o spyware que facilitan la detección de programas maliciosos. No todos los antivirus tienen la capacidad un examen profundo de los componentes de estos programas maliciosos.

a.9Trojan-FakeAV

Los programas Trojan-FakeAV simulan la actividad del software antivirus. Están diseñados para extraerle dinero (a cambio de la detección y eliminación de amenazas, aun cuando las amenazas que informan en realidad no existen).

a.10Trojan-GameThief

Software que roba información de la cuenta de usuario en los juegos en línea.

a.11Trojan-IM

Especializados en robar datos de inicios de sesión y contraseñas para programas de mensajería instantánea y redes sociales, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype y muchos otros.

a.12Trojan-Ransom usado para cometer la modalidad denominada Cryptolocker Este tipo de troyano puede modificar datos en su computadora como registros de acceso al sistema o programas, de manera que su computadora no funcione correctamente o que usted ya no pueda usar archivos específicos. El delincuente que tiene un control remoto del sistema restaurará el desempeño de su computadora o desbloqueará sus archivos después de que usted le haya pagado el dinero exigido.

a.13Trojan-SMS

Programas que envían de manera automática mensajes de texto desde su dispositivo móvil a números de teléfono de tarifa Premium, líneas 0800 o de costo por su uso.

a.14Trojan-Spy

Tienen la capacidad de espiar el uso de su terminal ; tiene la capacidad de seguir los datos que ingresa a través de su teclado, tomando capturas de pantalla , asi como puede saber que aplicaciones tengo en ejecución o uso.

a.15Trojan-Mailfinder

Especializado en recopilar de manera no autorizada y remota direcciones de correo electrónico desde su computadora.

b) **VIRUS O GUSANOS:**

Un virus de computadora o un gusano de computadora es un programa de software malicioso que tiene la capacidad de autorreplicarse en terminales o redes, sin que se tenga alguna advertencia de que su equipo se ha infectado.

Cada copia posterior del virus o el gusano de computadora se pueden autorreplicar, las infecciones se pueden expandir rápidamente por las redes.

La propagación del virus puede darse:

a) Con archivos enviados como adjuntos de correo electrónico

b) A través de un enlace a un recurso web o FTP[48].

c) A través de un enlace enviado en un mensaje ICQ[49] o IRC[50]

[48] **FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos')** en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

d) A través de redes de uso compartido de archivos P2P (entre pares)

e) Algunos gusanos se extienden como paquetes de red. Estos penetran directamente la memoria de la computadora y entonces el código del gusano se activa.

Los gusanos de computadora tienen la capacidad de al detectar errores de configuración de las redes (por ejemplo, para copiarse en un disco totalmente accesible, dispositivos como USBs) o explotar sistema operativos sin actualizaciones de seguridad, así como software diverso como las aplicaciones móviles sin un control de calidad que certifique su uso seguro.

Muchos gusanos usarán más de un método para difundir copias a través de las redes.

C) ESTADÍSTICAS MUNDIALES DE CYBERATAQUES.

c.1 Países con mayor índice de infecciones por año.

Podemos citar el Panda Security / Informe anual Panda Labs 2015[51], que precisa que a nivel mundial el país que cuenta con mayor número de infecciones por virus informáticos se encuentra China, con un 57,24% de las infecciones seguido por Taiwán, con un índice de infección de 49.15 % y Turquía con un 42,52 %

Países con Mayor índice de infecciones el 2015

China : 57.24%

[49] **ICQ** (*"I seek you"*, en castellano *te busco*) es un cliente de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet, mediante el cual es posible chatear y enviar mensajes instantáneos a otros usuarios conectados a la red de ICQ. También permite el envío de archivos, videoconferencias y charlas de voz.

[50] **IRC (**Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí,

[51] http://www.pandasecurity.com/spain/mediacenter/informes/

Taiwan: 49.15%

Turquia: 42.52%

Guatemala: 39.09%

Rusia: 36.01%

Ecuador: 35.51%

México: 34.52%

Perú: 34.23%

Polonia: 34.13%

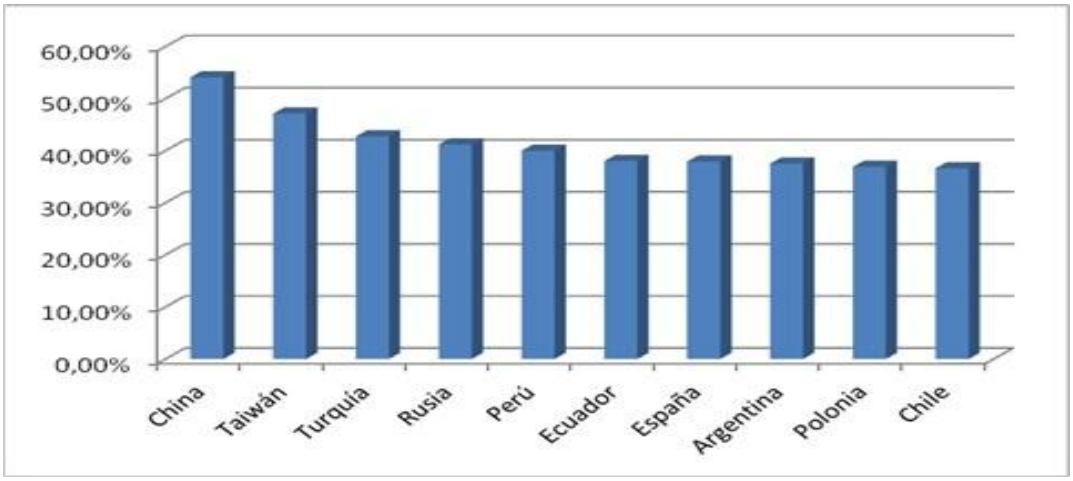
Brasil: 33.34%

Las regiones con mayor cantidad de infecciones se centran en Asia y Latinoamérica.

Países con menor índice de infección el 2015.

Países bajos : 26.51%

Japón: 25.34%



[52]

**Países con mayor índice de infección por virus.

[52] http://www.pandasecurity.com/spain/mediacenter/notas-de-prensa/4-de-cada-5-nuevas-muestras-de-malware-son-troyanos-informa-pandalabs/

RESUMEN DE LA UNIDAD I

1.-Es necesario con el fin de llevar adelante un análisis de los casos de delitos informáticos conocer conceptos técnicos fundamentales que nos permita determinar el grado de autoría o participación de los ciberdelincuentes.

2.-Cobra relevancia la participación de los Proveedores de Servicios de Internet o Internet Service Providers (ISP) , empresas que proveen el acceso a las grandes redes de comunicación, y centralizan mucha información que tiene que ver con el intercambio de data, lo que permite de un análisis la ubicación del ciberdelincuente y su red delictiva.

3.- Asimismo el conocimiento de la topología de las redes permite establecer dentro de una red, la correcta ubicación de un presunto autor y las conexiones que este tenga.

AUTOEVALUACIÓN

1. ¿Qué relevancia cumple los Proveedores de Servicios de Internet en la investigación de los delitos informáticos?

_____
_____

2.- ¿Cuál de las técnicas de hacking mostradas en este módulo consideras que pueden ser utilizadas para la comisión de delitos informáticos?

_____
_____

3. ¿Que entendemos por protección de datos de tráfico?

_____
_____

LECTURAS

Lecturas Obligatorias:

1. EL SECRETO DE LAS COMUNICACIONES CON ELABOGADO DEFENSOR EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN- INMACULADA LÓPEZ-BARAJAS PEREA.

(Disponible en el anexo de lecturas).

LECTURAS

Lecturas Sugeridas:

a) Topología e Infraestructura de Redes.
b) Guía de Nombres de Dominio.
c) Caso Esher vs Brasil.
d) Informe Pandalabs 2015.

(Disponible en el anexo de lecturas).

UNIDAD II

CONOCIMIENTOS LEGALES.

PRESENTACIÓN

Luego de desarrollado en el módulo anterior lo referente a técnicas informáticas destinadas a facilitar la comisión de ilícitos, es preciso mencionar que las mismas no sólo tienen ese fin, en algunos casos, como en las normas que desarrollaremos en este módulo tipifican, son de uso permitido siempre y cuando sean para fines de poner a prueba la protección de la seguridad de la información de sus sistemas, como es el caso del hacking ético.

Asimismo hemos considerado en este módulo de manera introductoria un análisis desde la visión de la seguridad de la información de la protección de los datos personales, para luego desarrollar uno de los mas importantes convenios existentes sobre la materia de ciberdelincuencia, nos referimos al Convenio de Cibercriminalidad de Budapest, origen de la normativa existente a nivel internacional y motor de una visión global en la lucha contra la criminalidad en la red.

Finalmente describimos los tipos penales pertinentes de la Ley de Delitos informáticos peruana, así como análisis del tipo penal, lo que facilitará el análisis de los mismos en cualquier escenario.

PREGUN TAS GUÍA

1. ¿Qué importancia reviste la seguridad de la información en el acceso y tratamiento de los datos personales, dichos sistemas estarían también expuestos a la delincuencia informática?

2. ¿Cuál es la exclusión que tipifica la norma en cuanto al uso de uso de dispositivos informáticos destinados al hacking?

PRIMER CAPITULO: ANÁLISIS RESPECTO A TEMAS DE SEGURIDAD DE LA INFORMACIÓN EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES 29733[53] Y SU REGLAMENTO.

Iniciamos esta unidad con el fin de detallar conceptos fundamentales en el tratamiento de datos personales que inciden en temas de seguridad de la Información, de interés en la investigación de delitos informáticos, antes de ello enunciaremos los principios rectores bajo los cuales se encuentran regulados el titular del banco de datos personales o quien resulte responsable de su tratamiento.

a) Principios.

1. **Principio de Consentimiento**.- requiere para su licitud que el titular del dato personal haya prestado su consentimiento libre, directo, previo y expreso, informado e inequívoco no existe presunción.

2. **Principio de finalidad**.- la misma que debe ser expresada con claridad el objeto que tendrá el tratamiento de datos personales, existe un deber de quien realice el tratamiento de datos personales de guardar secreto profesional.

3. **Principio de calidad.-** Los datos contenidos en un banco de datos personales, deben ajustarse con precisión a la realidad, se presume que los datos facilitados por el titular de los mismos son exactos.

4. **Principio de Seguridad.**- tomarse las medias de seguridad necesarias para evitar cualquier tratamiento contrario a la ley o al reglamento, evitando la adulteración, la pérdida, las desviaciones de información intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

[53] http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

b) **Definiciones:**

Datos Personales:

A tenor del reglamento de la Ley 29733, es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

Datos sensibles:

Aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

Titular de datos personales:

Es quien es responsable de sus propia información personal y por ende atendiendo a la publicidad de la norma es deber del mismo conocer los alcances de la misma, es necesario que su consentimiento, para el tratamiento de los datos personales sea ejercido dentro de cánones de libertad, así como contar con información adecuada en lo que respecta a sus derechos y obligaciones de quien administre sus datos, asimismo que tenga la posibilidad de que su consentimiento quede plasmado de la manera y términos en los que ha consensuado .

Titular del banco de datos personales.

Tiene la responsabilidad respecto a los datos personales bajo su titularidad de otorgar seguridad, protección y adecuado tratamiento, lograr la determinación y cumplimiento de la finalidad y del contenido del banco de datos y garantizar el cumplimiento de derechos del titular los datos personales establecidos en la ley especial.

Autoridad Nacional de Protección de Datos Personales.

La Dirección General de Protección de Datos Personales es un órgano que depende jerárquicamente del Despacho Viceministerial de Derechos Humanos y Acceso a la Justicia. Le corresponde realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley de Protección de Datos Personales – Ley Nº 29733 y su Reglamento.

Esto implica funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras, así como realizar dentro de este marco un seguimiento y evaluación de su aplicación.

Asimismo administra el Registro Nacional de Protección de Datos Personales.

Directiva de Seguridad de la Información

Pretende establecer medidas de seguridad de la información y procedimientos exigibles a los titulares de los bancos de datos personales, realiza una clasificación de categorías de tratamiento de los datos personales desde el nivel básico a crítico considerando factores como:

a) Cantidad de registros.

b) Detalle de los datos personales.

c) Periodo de tiempo de almacenamiento de los datos.

d) Clase de titularidad (persona natural o entidad pública)

e) Finalidad del tratamiento de datos personales con respaldo normativo.

f) Transferencia de datos.

g) Tratamiento de datos determinados como sensibles.

Política de Protección de Datos Personales

Constituye una declaración formal de compromiso entre el personal involucrado en el tratamiento de los datos personales, como para el/los titular/es que haya consentido el tratamiento de los mismos.

Incluyen lineamientos organizacionales, objetivos, cumplimiento de requisitos de seguridad, mejora continua, y comunicación interna adecuada.

Aplicación supletoria de la NTP-ISO/IEC 27001 EDI

Para el tratamiento de los datos complejos o críticos es necesaria la implementar los requisitos y controles que establece la NORMA TÉCNICA PERUANA ISO NTP/IEC 27001:2014[54] TECNOLOGÍA DE LA INFORMACIÓN, TÉCNICAS DE SEGURIDAD DE A INFORMACIÓN, REQUISITOS, 2DA EDICIÓN[55], de manera símil a la citada norma es necesario designar un responsable de seguridad de la información quien coordinará y controlará la implementación de las medidas de seguridad para la protección del banco de datos personales.

Acceso y tratamiento de los datos personales en los sistemas.

Los denominados "Usuarios del sistema de información" son las personas naturales que tienen acceso al sistema de información que realiza el tratamiento de los datos personales, pudiendo ser el administrador del sistema, administrador de banco de datos, operadores, personal de soporte o el titular de los datos personales.

[54] http://www.ongei.gob.pe/docs/isoiec27001.pdf
[55] http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

SEGUNDO CAPITULO: EL CONVENIO DE BUDAPEST- CONVENIO DE CIBERCRIMINALIDAD.

a) DEFINICIONES.

El Convenio sobre la ciberdelincuencia[56] fue firmado en Budapest el 23 de noviembre del 2001 que fue concebido con la atendiendo a la necesidad de aplicar una política común con el objeto de proteger a la sociedad ante la amenaza de la ciberdelincuencia, con un enfoque de cooperación internacional con celeridad y eficacia en materia penal.

¿Pero qué es lo que busca prevenir el convenio?

Los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delitos de dichos actos, así como la asunción de poderes suficientes para luchar contra dichos delitos.

¿Qué busca facilitar?

La detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable.

¿Qué libertades protege el convenio?

Los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos[57] y de las Libertades fundamentales (1959), el Pacto Internacional de los Derechos Derechos Civiles y Políticos de las Naciones Unidas[58] (1966) y otros tratados internacionales aplicables en materia de Derechos Humanos, que

[56] https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF
[57] http://www.echr.coe.int/Documents/Convention_SPA.pdf
[58] http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar obtener y comunicar información e ideas de toda índole[59], sin consideración de fronteras así como el respeto a la vida privada, la protección a los datos personales basado en el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales[60].

Asimismo incluye la protección a los derechos contenidos en la Convención sobre los Derechos del Niño de las naciones Unidas [61](1989) y el Convenio sobre las peores firmas de trabajo infantil de la Organización Internacional del Trabajo[62] (1999)

¿Qué es sistema informático?

El Artículo 1 del Convenio define al mismo como todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

63

[59] Caja de Herramientas para la libertad de expresión, UNESCO, 2013.
[60] https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447
[61] http://www.un.org/es/events/childrenday/pdf/derechos.pdf
[62] http://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182
[63] http://edutecnomatica.pbworks.com/w/page/51294631/el%20sistema%20informatico%20y%20sus%20elementos

¿Qué es dato informático?

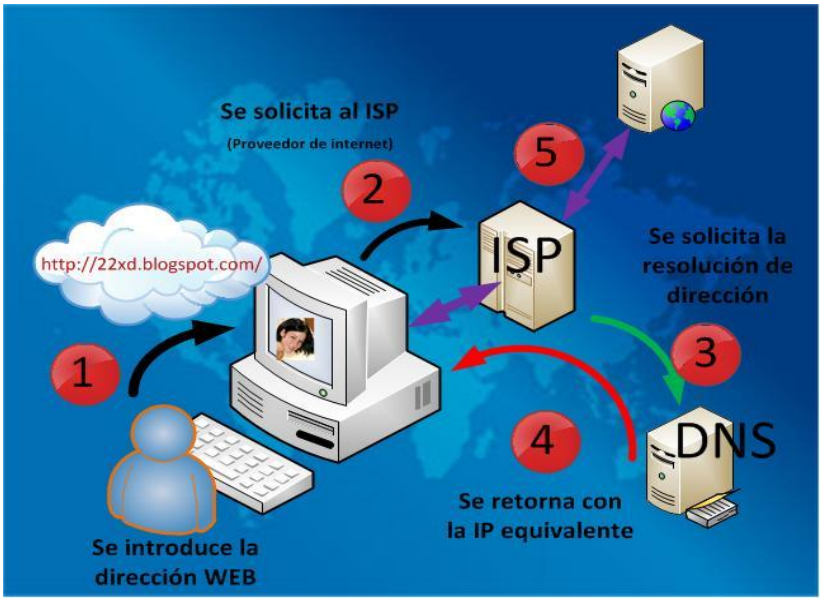
El mismo artículo define la misma como toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

[64]

¿Qué es un Proveedor de Servicios o ISP?

Toda entidad pública o privada que ofrezca a los usuarios de los servicios, la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

[64] http://www.ecured.cu/Sistema_inform%C3%A1tico



¿Qué son Datos relativos al tráfico?

Todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

b) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y Sistemas informáticos.

Considerados en los artículos 2do al 6to del Convenio tenemos:

b.1 Acceso Ilícito.- el tipo requiere a las partes que adopten medidas normativas para tipificar el acceso deliberado e ilegítimo a todo o parte de un sistema informático, infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención con contenido delictivo, o en relación con un sistema informático conectado a otro sistema informático.

b.2 Interceptación Ilícita.- la acción típica en este caso es la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en ellas o efectuadas dentro del mismo, incluyen además emisiones electromagnéticas provenientes de un sistema informático que transporte dicha información, la intención es exigible o en relación con un sistema informático conectado a otro sistema informático.

Otros delitos considerados dentro de este Título tenemos

Ataque a la integridad de los datos cuya acción típica es la de daño, borrado, deterioro , alteración o supresión de datos informáticos y en el caso de ataque a la integridad de los sistemas es la obstaculización del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de los datos informáticos.

Respecto al abuso de dispositivos.- va dirigido como en nuestra legislación a tipificar la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de dispositivos, programas concebidos para la comisión de los delitos precitados, así como contraseñas, códigos de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, esto en clara referencia a información obtenida mediante virus informáticos, incluye la salvedad de que los mismos sean usados para la protección de dichos sistemas, es decir el denominado Hacking ético.

c) Delitos Informáticos.-

Incluidos en el Título 2, artículo 7 y 8 , Falsificación informática, y fraude informático.

En el caso de la **Falsificación Informática** las acciones típicas es la introducción, alteración, borrado o supresión deliberados e ilegítimo de

datos informáticos que generen datos no auténticos con la intención que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.

El **Fraude Informático** la acción necesaria de manera similar a la falsificación que requiere introducción, alteración, borrado , supresión de datos informáticos o cualquier interferencia de un sistema informático, haciendo la salvedad que **causen daño patrimonial a otra persona**.

Es importante mencionar que la técnica informática utilizada para cometer las acciones típicas es **el hacking**, que por medio del ingreso del software con **código malicioso** al sistema informático permite un control remoto de los equipos con la posibilidad de cometer conjuntamente falsificación y fraude informático, cometida mediante el pharming[65] y phishing de usuarios.

d) Delitos Relacionados con el contenido.

Incluye los relacionados con la **pornografía infantil**, tipo legal que va contra la Producción y difusión por sistema informático, oferta o puesta a disposición de dicho contenido, difusión o la transmisión, la adquisición y la posesión de los mismos en un sistema o dispositivo de almacenamiento.

En estos casos la edad del menor es considerada menos de 18 años de edad, teniendo las partes la posibilidad de disminuirla a 16 años.

TERCER CAPITULO: LEY DE DELITOS INFORMÁTICA PERUANA ANÁLISIS TÉCNICO LEGAL. LEY 30096, MODIFICADA POR LEY 30171.

[65] http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=194

A) Delitos contra datos y sistemas informáticos.

a.1 Acceso ilícito.

Tipificada en el **artículo 2** de la Ley 30171 publicada el 10 de marzo del 2014, que modifica la Ley 30096, ley de delitos informáticos establece:

"..El que deliberadamente accede todo o en parte a un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecida para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con 30 a 90 días multa

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado…"

Tenemos en este artículo que la **acción típica** la constituye el **acceso a todo o en parte de un sistema informático** con **vulneración** de medidas de **seguridad** establecidas para impedirlos, el acceso a un sistema informático por medidas de seguridad informática en la práctica está regulado en muchas instituciones o empresas por directivas de uso de claves secretas, las mismas que son de creación y responsabilidad de usuarios de los mismos, asimismo tenemos detrás de este acceso a personal que administra dicha información, como lo pueden ser personal administrador de las bases de datos, quienes tienen accesos con privilegios que los administradores de bases de datos permiten o autorizan, supervisados por un oficial de seguridad de la información.

Al llevar adelante la investigación de este delito es necesario establecer cuál es la medida de seguridad de la información que ha sido violentada para el acceso, la misma que puede ser por la exposición del uso de las claves secretas, han sido compartidas o robadas (mediante hardware de captura de teclado) o ha sido expuesto al no contar el terminal con software que permita la captura remota de los mismos, así también tenemos que el acceso puede darse a nivel de personal técnico

administrador de las bases de datos , bajo supervisión de los administradores de bases de datos, quienes establecen los límites para el acceso a información dependiendo de la función que el personal cumpla, y tenemos detrás de ellos supervisando todo el proceso a un oficial de la información que tiene la capacidad de auditar el cumplimiento de la norma técnica 27001 de seguridad de la información.

El Acceso ilícito se da mediante **el uso de las redes o con el acceso directo a una terminal,** el sujeto activo puede ser cualquier persona y/o con conocimientos técnicos suficientes para vulnerar las medidas de seguridad, en la práctica toda persona tiene el potencial para cometer este delito, con la facilidad con la que en el mercado se encuentran software especializado, tenemos que el sujeto pasivo vendría a ser la persona que ejerce titularidad sobre la información contenida en el dato informático, como en el caso anterior hemos manifestado que existe personas naturales, jurídicas e incluso instituciones públicas que ejercen administración o responsabilidad sobre un sistema informático que contiene el dato informático.

a.2 Atentado contra la integridad de datos informáticos.

Artículo 3.- El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime, o hace inaccesible datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

El bien jurídico tutelado será entonces la **disponibilidad** del dato informático, así como **si integridad** por ende existe estrecho nexo con el **sistema informático.**

66

Analizando los elementos objetivos de este tipo penal encontramos las acciones de dañar, introducir, borrar, deteriorar, alterar o suprimir o hacer inaccesible datos informáticos, como en el caso anterior y en el análisis de los medios tecnológicos con los que se cuenta este se realiza mediante el uso de software o hardware especializado en hacking.

El tipo penal establece que requiere una **acción dolosa**, al detallar una acción deliberada e ilegítima en el accionar del sujeto activo, que en la práctica puede ser cualquier persona, atendiendo a la facilidad de acceso de software con dichos fines e incluso tutoriales al detalle en foros especializados en Internet.

a.3 Atentado contra la integridad de Sistemas Informáticos.

El artículo 4 establece:

" El que deliberada e ilegítimamente inutiliza , total o parcialmente un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa."

En este caso es importante destacar que es una acción dolosa, como en casos anteriores tenemos que cualquier persona puede ser sujeto activo y

[66] http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

el sujeto pasivo es variado dependiendo de quien ejerza titularidad del sistema informático, la comisión de este delito puede realizarse mediante el uso de los virus informáticos, por ejemplo puede ejercerse el entorpecimiento o el impedir el acceso mediante un ataque de denegación de servicio, o con el secuestro de información, que como hemos comentado limita el acceso al propietario del mismo a cambio de una rescate.

En ambos casos es necesario actuar con rapidez para la obtención de pruebas necesarias para acreditar la comisión del delito, como captura de pantalla, registro de incidentes por parte del área técnica encargada del monitoreo de los sistemas informáticos, seguimiento de direcciones IP, así como evitar la manipulación de la evidencia, siendo obtenida de manera exclusiva por la policía y la fiscalía especializada mediante protocolos que aseguren la integridad de la evidencia y en el caso que impliquen el acceso a información de terceros involucrados en el hecho, puede darse el caso de levantamiento de secreto de las comunicaciones.

B.- Delitos informáticos contra la indemnidad y libertades sexuales.

b.1 Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

El tipo penal se encuentra establecido en el artículo 5, que a la letra regula:

"….el que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1,2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tienen entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años, e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal"

El tipo penal requiere acción dolosa y pena el contacto con menores de 14 años para solicitar u obtener material pornográfico, nos detenemos en este punto y podemos referir que:

"**…** El 25 de octubre de 2014 se promulgó la Ley No. 30254[67], Ley de promoción para el uso seguro y responsable de las tecnologías de la información por niños, niñas y adolescentes. Un trabajo desarrollado desde la ONGEI…"

Siendo esta iniciativa, importante para generar una barrera ante la facilidad con la que los menores pueden ser contactados por redes sociales, asimismo con la proliferación de cabinas públicas, acceso a foros que captan menores, ofreciendo sumas de dinero.

El tipo legal se consuma cuando se produce el resultado típico del **contactar o establecer comunicación con un menor de 14 años** para los fines protegidos por la norma, sin importar si este lo haya obtenido o no.

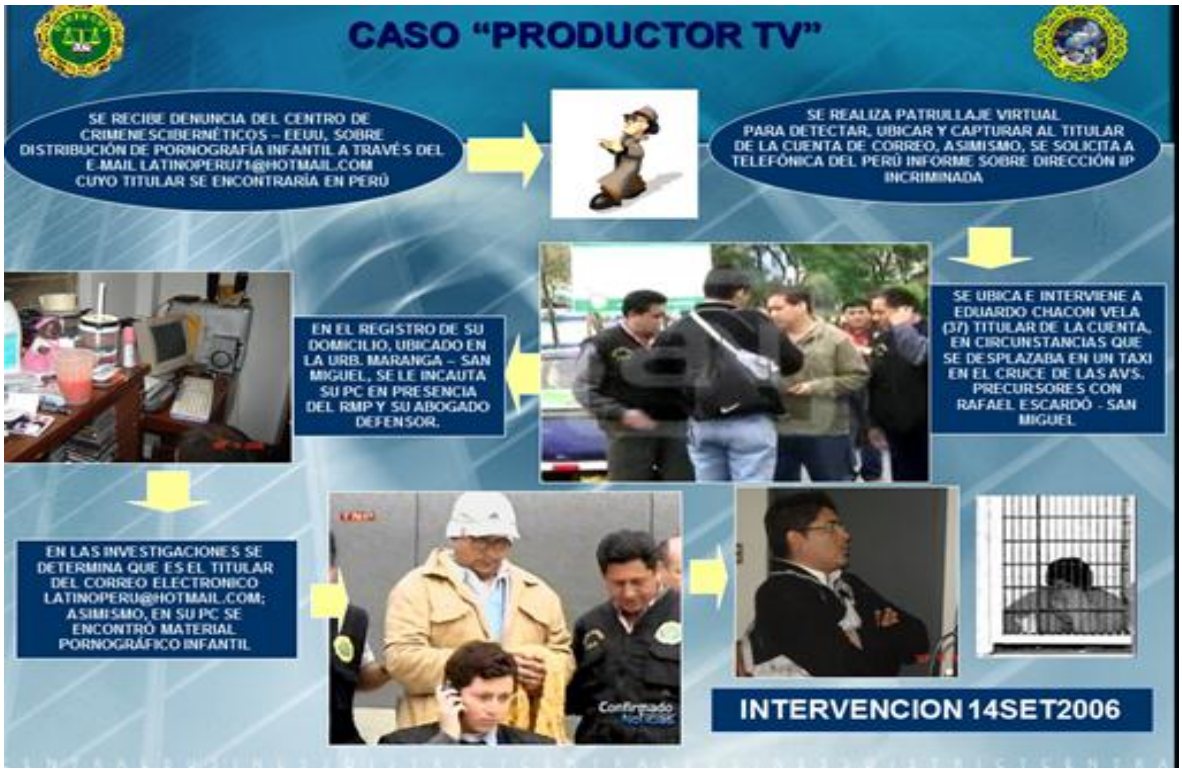
Asimismo el tipo establece que el uso de internet u otro medio análogo para llevar "actividades sexuales" con el menor, esto refiere por ejemplo del uso de sistemas de videoconferencia, ahora accesibles en todas las redes sociales, que obtiene de manera remota imágenes de menores sometidas a acto sexual.

Aquí la consumación se da con la proposición hecha a una menor de edad, con fines sexuales, lo que va contra derechos fundamentales protegidos en el menor como son la indemnidad, la libertad sexual.

[67] http://www.leyes.congreso.gob.pe/Documentos/Leyes/30254.pdf

La investigación en esta modalidad delictiva requiere de un seguimiento de las comunicaciones electrónicas y un manejo adecuado de los datos de comunicación entre la víctima y el presunto autor, es importante también el manejo adecuado de evidencia que impida daño a su integridad.

A continuación publicamos dos infogramas en los que se detalla paso a paso como es que se procedió en dos casos de investigación de este delito.



68

c) Delitos contra la intimidad y el secreto de las comunicaciones.

c.1 Delito de Interceptación de Datos Informáticos.-

Tipificado en el artículo 7 establece:

"Artículo 7.- El que deliberadamente e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta dichos datos informáticos, será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la información Pública.

[68] Fuente: DIVINDAT.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores…"

Al ser un delito de peligro abstracto la consumación del delito se da con la interceptación de datos informáticos, con tres agravantes a) en el caso de información clasificada como secreta, reservada o confidencial; b) Información que compromete a la defensa, seguridad o soberanía nacional; y c) la calidad del agente- integrante de una organización criminal.

D.- Delitos Informáticos Contra el patrimonio.

d.1 Fraude Informático.-

"Artículo 8.-

El que deliberadamente e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión; clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social…"

En este caso las acciones típicas buscan conseguir un beneficio para sí o para otro en perjuicio de tercero, se clasifican como un delito de resultado, requiere el cumplir con el tipo penal y seguida de un resultado

que consiste en causar un perjuicio a un tercero, sino el delito quedará en grado de tentativa.

E.- Delitos Informáticos contra la fé pública.

e.1 Suplantación de Identidad.

"…Artículo 9.- El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Es común con el uso de las redes sociales la posibilidad de la suplantación de identidad al no contar en muchos casos con procedimientos de contraste con documentos oficiales de identidad, en este caso es necesario la suplantación seguida de un perjuicio, sino quedaría en grado de tentativa…"

F.- Abuso de mecanismos y dispositivos informáticos.

Artículo 10.- El que deliberadamente e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa…"

Consiste en un delito de mera actividad[69], se consuma con la actividad típica descrita sin considerar el resultado posterior del ingreso de los mismos al mercado o su uso.

[69] http://www.unav.es/penal/crimina/topicos/delitosderesultadoydemeraactividad.html

Art. 11º.- "El juez aumenta la pena privativa de libertad hasta un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley, cuando: 1. El agente activo integra una organización criminal. 2. El agente tiene posición especial de acceso a la data o información reservada. 3. El delito se comete para obtener un fin económico. 4. El delito compromete fines asistenciales, la defensa, la seguridad y soberanía nacional."

Se detallan los agravantes, habilitando al juez la posibilidad de aumentar la pena hasta en un tercio por encima del máximo legal establecido.

Art. 12º.- "Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.

Dicha excepción se encuentra sustentada si la misma está destinada a realizar pruebas u otro procedimiento con el objetivo de lograr la protección de los sistemas y datos informáticos, siendo estas las denominadas prácticas de Hacking ético, es decir pruebas en sentido inverso en la que simulan ataques a la seguridad de la información y en la que se ponen a prueba medios de protección.

Las empresas privadas incluso ponen a prueba mediante concursos internos y de convocatoria pública mediante premios a quien logre determinar las vulnerabilidades de los sistemas[70], lo que permite mejores mecanismos de protección.

[70] http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11061&lang=es

G.- Sanciones a personas Jurídicas impuestas por organismos reguladores-

Décima.- La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y

circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por Decreto Legislativo 957.
Esta norma remite a una norma especial que establece sanciones a las empresas que omiten una orden judicial.

UNDÉCIMA.- "El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230° del Código Procesal Penal, aprobado por Decreto Legislativo 957[71]. El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente."
Atendiendo a la urgencia requerida para el acceso a información para el procesamiento de los delitos informáticos, se sanciona administrativamente ante el incumplimiento a las empresas prestadoras de servicios de comunicaciones y telecomunicaciones.

71

http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=defaultnuevocodprocpenal.htm&vid=Ciclope:CLPdemo

H) Estadística de Delitos Informáticos en las Cortes Superiores del Perú.

CORTE	DELITO \ ARTICULO		
Etiquetas de fila	DELITOS CONTRA EL PATRIMONIO	LEY N° 30096 y N° 300171 DELITOS INFORMATICOS	Total general
HUAURA	4		4
EN CALIFICACION	1		1
EN TRAMITE(Pendiente)	1		1
TRAMITE	2		2
LIMA - PENAL	67	534	601
APELACION		6	6
ARCHIVO DEFINITIVO		2	2
ARCHIVO PROVISIONAL		6	6
CALIFICADO		7	7
EN CALIFICACION	27	277	304
EN TRAMITE(Pendiente)	23	64	87
IMPUGNATORIA		8	8
INSTRUCCION		8	8
JUZGAMIENTO		1	1
SENTENCIA		1	1
SENTENCIADO/ RESUELTO		1	1
TRAMITE	17	153	170
LIMA ESTE		22	22
APELADO		1	1
APERTURA DE INSTRUCCION		3	3
EN CALIFICACION		5	5
EN TRAMITE(Pendiente)		2	2
TRAMITE		11	11
LIMA NORTE	5	12	17
APERTURA DE INSTRUCCION		1	1
DICTAMEN FISCAL	1		1
EN CALIFICACION	2	5	7
EN TRAMITE(Pendiente)		2	2
TRAMITE	2	4	6
Total general	76	568	644

(Elaboración propia)

El presente cuadro demuestra la incidencia de casos en Delitos informáticos en cuatro cortes superiores de justicia del Perú, refleja que en la Corte de Lima a la fecha existen 601 casos en total, con una menor incidencia en las Cortes Superiores de Lima Este, Norte y Huaura.

Incidencia de Delitos Informáticos.

Delito Informático	Total Casos
Abuso de mecanismos y dispostivos informáticos Art. 10	11
Trafico Ilegal de datos	18
Suplantación de Identidad	33
Fraude informático que afecte el patrimonio del Estado	605
Sabotaje informático	12
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos Art. 5	13
Intrusismo y Fraude Informático	88
Atentado a la integridad de los sistemas informáticos	5
Atentado a la integridad de los datos informáticos	19
Acceso ilícito	14
agravantes artículo 11	18
Total	825

(Elaboración propia)

Analizando ahora la incidencia de casos por delito, encontramos que existen en las cortes analizadas un total de 825 incidencias, en las cortes de Lima, Lima Norte, Lima Este y Huaura, siendo el delito más recurrente el Fraude informático que afecte el patrimonio del Estado.

RESUMEN DE LA UNIDAD II

El presente módulo complementa lo desarrollado en la etapa introductoria del presente material respecto a la comisión de los delitos informáticos, hemos desarrollado de manera integral tres normas que sirven para poder ver la importancia de la protección tanto de datos personales, que son administrados en el marco de la norma especial, como en el caso ya de la protección mas amplia recomendada por el Convenio de Budapest sobre la cibercriminalidad que en muchos aspectos sirve de base a legislaciones nacionales como la ley de delitos informáticos peruana.

Resaltamos la necesidad de un trabajo conjunto y coordinado tanto de los operadores de justicia con el sector privado, tanto en los casos de la investigación de los delitos, como en etapas anteriores preventivas, con mayor comunicación a la ciudadanía respecto a lo que se entiende por seguridad de la información, y los derechos que vienen ya siendo protegidos por la legislación nacional.

La investigación y el procesamiento de los delitos informáticos no tienen fronteras, es por ello que resulta necesario armonizar la legislación, siendo el camino más adecuado la suscripción de Convenios que genere una tipificación homogénea, permitiendo de manera célere algunos casos de extradición.

AUTOEVALUACIÓN

1. ¿Qué diferencia encuentra entre los conceptos de sistema y dato informático?

_____
_____

2. ¿En el caso del delito tipificado en el artículo 5 de la Ley de Delitos informáticos peruana respecto a la proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, en que momento se consuma?

_____
_____

3. ¿Cuáles son los agravantes en el caso del delito de interceptación de datos informáticos?

_____
_____

LECTURAS

Lecturas Obligatorias:

1.- Convenio sobre la Cibercriminalidad de Budapest.

2.- Ley 30071 y 30096 de Delitos Informáticos.

3.- Retención de datos y secreto profesional- Comisión de Derechos Humanos de Barcelona FBE 30 de enero 2015.

(Disponible en el anexo de lecturas).

LECTURAS

Lecturas Sugeridas:

a) Norma Técnica Peruana ISO - IEC .- 27001-2014
b) Ley 29733 - Protección de Datos Personales y su reglamento.

(Disponible en el anexo de lecturas).

MÓDULO III

INFORMÁTICA FORENSE

PRESENTACIÓN:

Luego de haber desarrollado los módulos previos respecto a conocimientos técnicos base para el análisis de casos de delitos informáticos, posteriormente haber complementado y relacionado los mismos con la posibilidad que dan estos en la comisión de delitos informáticos, en los que hemos establecido que con el uso de los mismos, o bajo sus técnicas es como finalmente tendremos claro un esquema de acción y participación de los ciberdelincuentes.

La complejidad que puede mostrar del análisis de los mismos reviste la necesidad de contar con un especialista en el tema, en este caso de un perito informático quien desarrollará técnicas de análisis de evidencia digital mediante procedimientos que aseguren el adecuado manejo de pruebas, aplicando estándares de seguridad de la información y procedimientos que aseguren la integridad de la prueba puesta a evaluación.

La pericia técnica informática será determinante para tener mayores luces en la determinación de responsabilidades, así también es probable que de la misma tengamos un esquema detallado que pueda demostrar un accionar delictivo que va más allá de nuestras fronteras.

PRIMER CAPITULO: ANÁLISIS DE LA EVIDENCIA DIGITAL DEFINICIÓN DE INFORMÁTICA FORENSE.-

Es cada vez más común atendiendo a la necesidad de claridad de cuestiones sensibles que se originan en distintos procesos penales, la necesidad de contratar personas expertas, especializadas que generen dictámenes que puedan generar certeza sobre los hechos materia de prueba en un litigio o proceso penal, siendo el peritaje un medio de prueba por el que se le confiere a un especialista debidamente acreditado la facultad de proveer un concepto en el tema materia a consulta, con el fin de colaborar con la labor del juez en formarse convicción o criterio sobre los hechos puestos en su decisión y dilucidar la controversia.

En el peritaje informático el dictamen versa sobre temas relacionados con la informática, lo realiza un experto en el materia de tecnologías de la información atendiendo al tema requerido a análisis de la prueba electrónica.

A) Evidencia Digital.-

Constituyendo la misma una vez recopilada y procesada por un perito especialista evidencia física, puede ser esta contener:

a) Registros diversos (Log files[72]) generados por el mismo sistema de manera automatizada, en el origen (en la Pc por el mismo software) o remota con datos enviados por medio de la red al terminal conectado a la red.

[72] http://web.mit.edu/rhel-doc/3/rhel-sag-es-3/ch-logfiles.html Los *Archivos de registro* (o archivos de log) son archivos que contienen mensajes sobre el sistema, incluyendo el kernel, los servicios y las aplicaciones que se ejecutan en dicho sistema. Existen diferentes tipos de archivos de log dependiendo de la información. Por ejemplo, existe un archivo de log del sistema, un archivo de log para los mensajes de seguridad y un archivo de log para las tareas cron.

b) Archivos diversos almacenados en equipos informáticos, creados por el propietario del hardware.

c) Registros generados en el computador y externos, por ejemplo datos de tráfico generados en servidores de manera automatizada.

La importancia de la participación de un perito informático en etapas tempranas de la investigación de un delito que contenga **evidencia digital** versa en que la misma:

a) Puede alterarse fácilmente e impugnar su autenticidad.

b) Se puede reproducir y con ello perjudicar su integridad.

c) Puede duplicarse generando falsas pruebas.

d) Nace "anónima" lo que se clarifica con el acceso a la fuente de manera rápida.

e) Es importante obtener rápidamente los medios por los que se crearon, modificaron, alteraron, suprimieron, entre otras actividades punibles.

f) La evidencia requiere ser en algunos casos decodificada y certificar dicha conversión.

g) El almacenamiento de la evidencia digital requiere condiciones especiales de almacenamiento y custodia.

h) Requiere la protección del original de la muestra y trabajar con copias espejo, idénticas al original, certificada mediante software especializado.

i) La información disponible en la red respecto a los datos de tráfico cuentan con regulación para su conservación, pero algunos de ellos por razones técnicas son temporales.

Los archivos de registro pueden ser muy útiles cuando se trate de resolver un problema con el sistema tal como cuando se trata de cargar un controlador del kernel o **cuando se esté buscando por intentos no autorizados de conexión al sistema**.

j) Requiere una coordinación especializada en caso de recibir evidencia procedente de cooperación internacional.

Es necesario llevar adelante la labor mediante procedimientos estandarizados siendo los recomendados:

1) **Recolección de información.-** de la fuente que origino, en tiempo real, o requiriendo información a empresas que almacenen por ejemplo datos de tráfico.

2) **Examinar y clasificar la evidencia.-** origen, procedencia, conexiones, redes, todo ello documentado mediante actas y dependiendo de la legislación, presencia de autoridades o veedores calificados.

3) **Análisis.-** consistente en una valoración de la evidencia obtenida atendiendo a los fines del proceso y los límites determinado por el juzgador.

4) **Dictamen.-** Conclusiones del análisis a consideración del juzgador o tribunal.

2.1 Criterios a considerar en la Evidencia Digital.-

Existen 4 criterios que se toman en consideración para determinar la admisibilidad de la evidencia digital como son:

a) **Autenticidad:** considerando situaciones como que la misma se haya generado y registrado en un lugar determinado y/o determinable que tenga relación con los hechos materia de investigación, asimismo que pueda probarse que no se ha alterado los medios originales, esto último puede acreditarse mediante software especializado, asimismo se puede llevar adelante un "lacrado digital" que permita la contrastación de copias de trabajo utilizadas en el proceso penal.

b) **Confiabilidad.-** atendiendo a la fuente de origen, que la misma en la creación de esta evidencia digital existan medios que permitan acreditar un funcionamiento adecuado, sin alteración en el sistema de origen.

Los sistemas informáticos estos reportan por medio de los denominados Log files, las acciones y comandos ejecutados en un sistema en tiempo real, y es almacenado de manera temporal.

c) **Suficiencia**.- será suficiente la prueba si es completa, necesitamos mecanismos que nos permita deteminar la integridad, sincronización de reportes y centralización de información, como reportes que emitan sistemas operativos o sistemas informáticos.

d) **Legalidad.-** basados en la normativa especial y vigente respecto al tratamiento de evidencia digital de manera concordada con normas procesales y respeto a los derechos constitucionales desde su recopilación.

B) Cadena de Custodia.-

Al llevar adelante un procedimiento de toma de muestras de evidencia digital bajo los alcances de la normatividad vigente, es necesario cumplir con los procedimientos establecidos o buenas prácticas documentadas para recoger y conservar la evidencia digital y la conservación de los medios físicos en los que estuvo esta contenida.

El objetivo es lograr garantizar los principios antes precitados como son los de autenticidad, identidad, estado original para ello es necesario cumplir el procedimiento y documentar información como:

a) Identificación de las personas que intervienen tanto en calidad de peritos, partes, veedores, Fiscales, entre otros.
b) Personal responsable del lacrado y envío de las evidencias, así como determinar el lugar de almacenamiento en condiciones de seguridad y buscando la conservación de los elementos físicos.

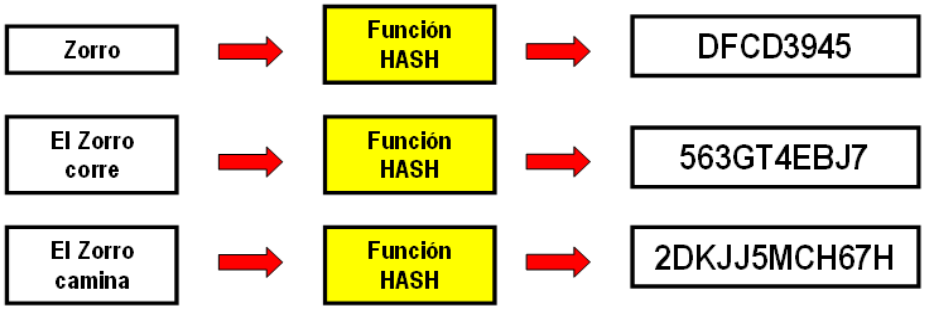
c) Cambios en la custodia de los bienes.

El proceso inicia desde el lugar donde se obtuvo, encuentre o recaude el medio físico que servirá como prueba y culmina con pronunciamiento de la autoridad judicial o administrativa competente.

C Definiciones Técnicas en el análisis de evidencia digital.

c.1 Código Hash.-

Se refiere a una función o método para generar claves o llaves que representen de manera **casi unívoca** a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo. El siguiente ejemplo, la función **HASH** aplica un algoritmo y genera un código diferente en caso los datos cambien.



c.2 COLISION HASH: Es una situación que se produce cuando dos entradas distintas a una función de hash producen la misma salida.

Es matemáticamente imposible que una función de hash carezca de colisiones, ya que **el número potencial de posibles entradas es mayor que el número de salidas que puede producir un hash**. Sin embargo, las colisiones se producen más frecuentemente en los malos algoritmos. En ciertas aplicaciones especializadas con un relativamente pequeño número de entradas que son conocidas de antemano es posible construir una función de hash perfecta, que se asegura que todas las entradas

tengan una salida diferente. Pero en una función en la cual se puede introducir datos de longitud arbitraria y que devuelve un hash de tamaño fijo (como MD5), siempre habrá colisiones, dado que un hash dado puede pertenecer a un infinito número de entradas.

Una de las propiedades deseables de las funciones de hash criptográficas es que sea computacionalmente imposible que se produzca una colisión. El valor de una función hash puede ser usado para certificar que un texto dado (o cualquier otro dato) no ha sido modificado, publicando el valor firmado de la función de hash si no es factible que ocurra una colisión. En este contexto, factible se refiere a cualquier método capaz de producirla más rápido que el tiempo que demora un ataque de virus informático.

c.3 COMPROBACION DE REDUNDANCIA CICLICA (CRC): Es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida.

El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento.

Este método de comprobación complementa la generación de códigos Hash.

c.4 COPIA ESPEJO: Es la copia bit a bit de un archivo, carpeta ó volumen que contiene información grabada digitalmente, incluye los archivos y carpetas que pudieran encontrase ocultos ó marcados como borrados, así como cualquier otra información que forme parte del mismo.

c.5 CRIPTOGRAFIADO: Remplazo de las referencias originales de una cadena de caracteres, archivo ó lenguaje por un método de conversión

gobernado por un algoritmo que permita el proceso inverso o descifrado de la información.

c.6 “DESLACRADO” de los dispositivos: Es el proceso de abrir los sobres ó cajas cerradas y aseguradas (“Lacrados”) y confrontar los dispositivos contenidos en ellos con las listas resultantes del “lacrado, en presencia de las partes interesadas.

c.7 DISPOSITIVO BLUETOOTH: Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretenden lograr con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras y relojes digitales. Los dispositivos que lo utilizan pueden comunicarse entre ellos cuando se encuentran dentro de su alcance (de uno a 100 metros) y no tienen que estar alineados, pueden incluso estar en habitaciones separadas si la potencia de transmisión lo permite.

c.8 DISPOSITIVO MEMORIA USB: (de *Universal Serial Bus*; en inglés *pendrive ó USB flash drive*): Es un dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías (pilas).

c.9 Identificación de los dispositivos de memoria USB:

Las memorias USB cuentan con un número de serie o ID, además el fabricante graba la marca, el modelo, sus características técnicas, etc., que para que pueda identificarse ante el sistema operativo del computador al que se conecta y pueda este cargar los programas que permiten al dispositivo de memoria USB operar adecuadamente. Pero, también es cierto que algunos fabricantes producen memorias USB sin este número de serie (ID), ni registran la marca, ni el modelo, porque el comprador así lo quiere, ya que así lo va ha comercializar. Por ejemplo: si el Congreso de la Republica adquiere 1,000 memorias USB, puede solicitar que el proveedor las entregue sin marca con la finalidad de grabar en el exterior del dispositivo el texto: “Congreso de la Republica”. En este caso, el dispositivo de memoria USB será analizado por el sistema operativo del usuario del computador al que se conecte por primera vez, para que este le asigne un número de serie (ID) y así poder diferenciarlo e identificarlo cada vez que el usuario lo utilice. Este número de serie **podría repetirse** en el caso de que otro dispositivo de memoria USB (distinto al anterior, pero igualmente sin número de serie) sea conectado por primera vez a otra computadora (distinta a la mencionada anteriormente) así esta cuente con el mismo sistema operativo utilizado por la computadora mencionada anteriormente.

Además, si el sistema operativo puede asignar un numero de serie (ID) a un dispositivo de memoria USB, entonces se puede desarrollar un mecanismo (programa) para grabar ó modificar el número de serie de un dispositivo de memoria USB.

Por lo tanto, no se puede afirmar que un dispositivo de memoria USB puede ser identificado plenamente, ya que otro puede tener el mismo número de serie (ID).

RESUMEN DE LA UNIDAD III

1.-El presente módulo tiene por finalidad servir como base para la interpretación y mejor entendimiento de la terminología utilizada en el desarrollo del análisis de evidencia digital, en la que el rol del perito informático reviste importancia para asegurar la calidad de la información que servirá de sustento ante cualquier proceso penal en la materia.

2.- Recapitulemos que los criterios a considerar en la evidencia digital son fundamentalmente cuatro, la autenticidad, la confiabilidad, la suficiencia, la legalidad, asimismo es importante tener en consideración los procedimientos de cadena de custodia de la prueba digital.

AUTOEVALUACIÓN

1. ¿Cuál es el objetivo de la cadena de custodia y que importancia tiene para el análisis de evidencia digital?

_____

_____

2.- ¿En qué consiste el código hash y que es colisión hash?

_____

_____

3. ¿Qué entendemos por cadena de custodia?

_____

_____

LECTURAS

Lecturas Obligatorias:

1. La Cadena de Custodia Informático Forense.
2. Análisis Forense Digital - Miguel López Delgado.

(Disponible en el anexo de lecturas).

LECTURAS

Lecturas Sugeridas:

a) Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 Dr. Santiago Acurio Del PinoDirector Nacional de Tecnología de la Información.

b) Sentencia por Delito de Fraude Informático.

(Disponible en el anexo de lecturas).