Historia de la Informática Forense

Historia de la Informática Forense

En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas "Norton Utilities", entre las que destacan UnErase, una aplicación que permite recuperar archivos borrados accidentalmente. Otras aplicaciones también serán útiles desde la perspectiva forense, como FileFix o TimeMark. Con el éxito de la suite de aplicaciones Peter publica varios libros técnicos, como Inside the I. B. M. Personal Computer: Access to Advanced Features and Programming, del que su octava edición se publicó en 1999, 11 años después de la primera edición.. La compañía será vendida a Symantec en 1990.

Introduccion a la Informática Forense

Ciencias forenses.

- Las ciencias forenses son la utilización de procedimientos y conocimientos para **encontrar, adquirir, preservar y analizar** las evidencias de un delito y presentarlas apropiadamente ante una corte de justicia o tribunal.
- Tienen que ver principalmente con la recuperación y análisis de la llamada “EVIDENCIA LATENTE”.
- Combinan el conocimiento científico y las diferentes técnicas que este proporciona con los presupuestos legales a fin de demostrar con la evidencia recuperada la existencia de la comisión de un acto delictivo y sus posibles responsables ante un tribunal de justicia.
- Están en constante cambio, siempre buscando nuevos métodos para encontrar y fijar las evidencias de cualquier tipo. Creando nuevos estándares y políticas.

Informática Forense - Definición.

- Es una ciencia forense que se ocupa de utilizar métodos científico aplicables a la investigación de delitos, no solo informáticos y donde se usa el análisis forense de evidencias digitales, o sea toda información o dato que se guarde en una computadora o sistema informático, en conclusión diremos que la Informática Forense es **"la ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego, esta, ser presentada en una Corte de Justicia".**

(Dr. Santiago Acurio Del Pino: "Introducción a la Informática Forense").

Informática Forense – Otra Definición.

- La **informática forense** es un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias del equipamiento de computación de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo en un juzgado.

(fuente: https://www.unir.net/ingenieria/revista/informatica-forense)

Informática Forense – Marco teorico.

- La informática forense es el vehículo idóneo para localizar de forma adecuada los hechos jurídicos informáticos relevantes dentro de una investigación, ya sea civil o penal.
- La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas y luego analizarlas.
- En el caso de la identificación, recolección y análisis forense de sistemas informáticos tienen un papel de suma importancia en recaudar información y los elementos de convicción necesarios.
- La escena del crimen son las PCs, los smartphones, Tablets, redes de comunicación informática, en definitiva, las TICs.
- La ciencia forense se basa en estándares de practica y entrenamiento con el fin de lograr la probidad profesional y solvencia de conocimientos para el área de trabajo que se elija, lo mismo ocurre para la Informática Forense.
- Es necesario que las personas encargadas en esta ciencia tengan parámetros básicos de actuación y también de procesamiento cumpliendo los principios básicos del debido proceso.

Informática Forense – Marco teorico.

- La informática forense es el vehículo idóneo para localizar de forma adecuada los hechos jurídicos informáticos relevantes dentro de una investigación, ya sea civil o penal.
- La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas y luego analizarlas.
- En el caso de la identificación, recolección y análisis forense de sistemas informáticos tienen un papel de suma importancia en recaudar información y los elementos de convicción necesarios.
- La escena del crimen son las PCs, los smartphones, Tablets, redes de comunicación informática, en definitiva, las TICs.
- La ciencia forense se basa en estándares de practica y entrenamiento con el fin de lograr la probidad profesional y solvencia de conocimientos para el área de trabajo que se elija, lo mismo ocurre para la Informática Forense.
- Es necesario que las personas encargadas en esta ciencia tengan parámetros básicos de actuación y también de procesamiento cumpliendo los principios básicos del debido proceso.

Introducción a la Informática Forense | Relación con otras disciplinas

Informática Forense – Criminalística.

La informática forense, es una disciplina que combina elementos del derecho y la informática para recopilar y analizar datos digitales par investigar y perseguir delitos informáticos.

Esta disciplina se relaciona estrechamente con la criminalística ya que utiliza técnicas científicas la recolección de los contenedores de la potencial evidencia digital, mas debemos aclarar que es una ciencia completamente diferente a la criminalística per-se.

Informática Forense – Criminalística.

Los profesionales en informática forense, conocidos como criminalistas digitales, deben identificar los diferentes elementos probatorios informáticos vinculados al caso, determinando la relación entre los elementos y los hechos para descubrir el autor del delito.

Estos expertos buscan en dispositivos digitales potenciales evidencias digitales, que los abogados pueden utilizar en investigaciones penales, casos civiles, investigaciones de delitos Informáticos y otros asuntos de seguridad informática.

Informática Forense – Seguridad Informática.

La Informática Forense y la Seguridad Informática están estrechamente relacionadas, ya que la informática forense se encarga de la investigación, preservación y análisis de evidencias digitales (ya sea de un delito informático, o de un incidente informático) en el ámbito de la seguridad informática y la ciberseguridad.

Su objetivo principal es determinar la existencia de delitos informáticos, identificar a los posibles autores y recopilar pruebas digitales para su uso en investigaciones y procesos judiciales, como así también las evidencias de las vulnerabilidades en sistemas informáticos (este ultimo en el ámbito empresarial).

Informática Forense – Seguridad Informática.

La informática forense juega un papel crucial en la prevención y respuesta a incidentes de seguridad, identificando y mitigando vulnerabilidades, así como respondiendo de manera efectiva a incidentes para minimizar el impacto.

Los especialistas en informática forense recopilan y preservan evidencia digital mediante el uso de técnicas especializadas, que incluyen la extracción de datos desde discos duros, dispositivos de almacenamiento, redes y otros medios digitales/electrónicos.

Informática Forense – Seguridad Informática.

El análisis forense informático también ayuda a identificar patrones (conducta digital), establecer la secuencia de eventos y determinar la naturaleza y el alcance de la actividad delictiva.

Además, la informática forense puede aportar evidencia crucial en procesos judiciales cuando se producen vulneraciones de la seguridad en sistemas informáticos, redes, dispositivos móviles, correos electrónicos, discos duros, etc.

Informática Forense – Seguridad Informática.

En resumen, la informática forense es una disciplina esencial dentro de la seguridad informática, ya que proporciona herramientas y técnicas para investigar y prevenir delitos informaticos, así como para responder a incidentes de seguridad de manera efectiva.

Informática Forense – Antiforense.

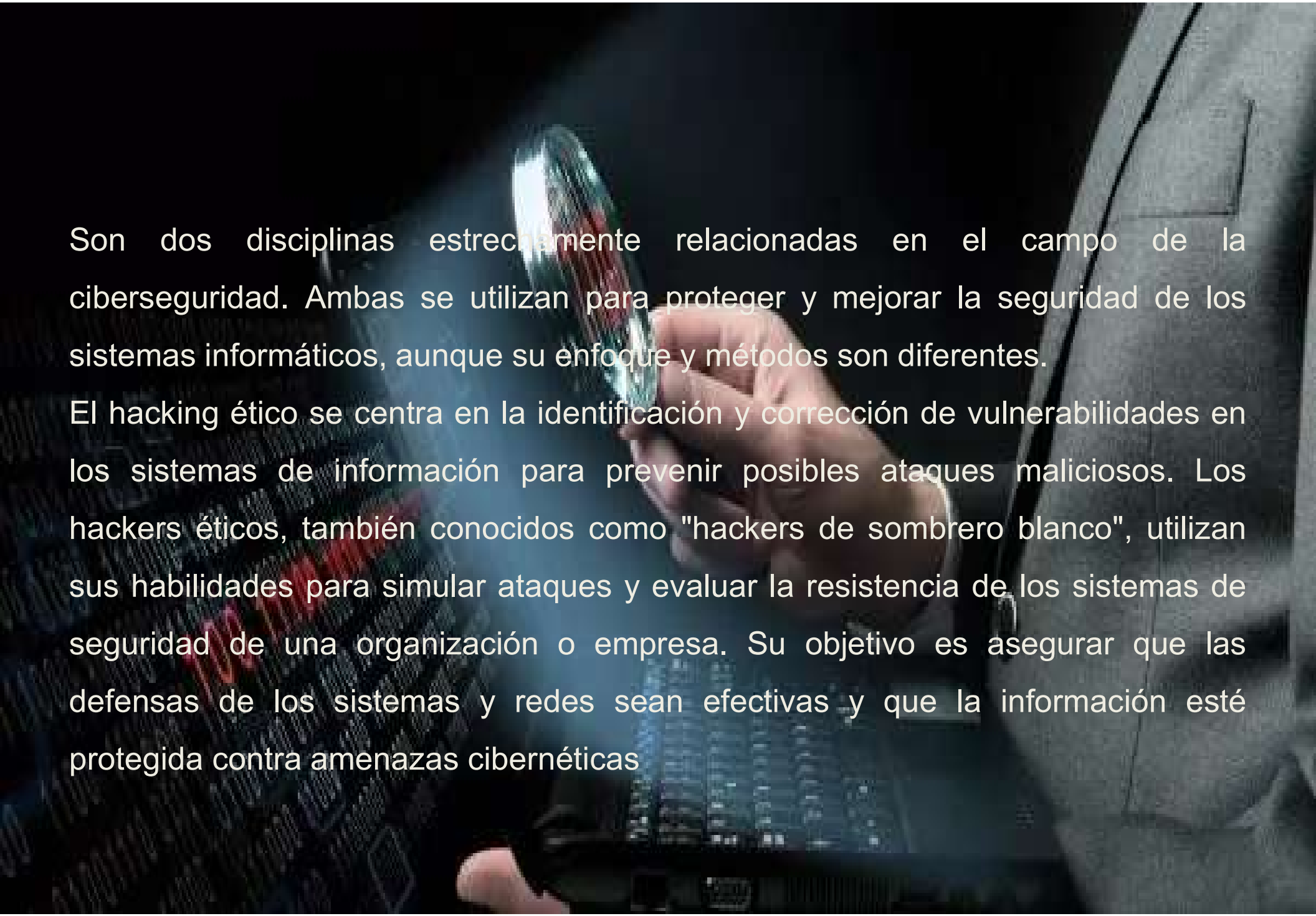
La informática antiforense esta estrechamente relacionada, ya que las técnicas anti forenses buscan frustrar a los peritos, pericias y herramientas forenses. Mientras que la informática forense se encarga de realizar un análisis profundo de los sistemas para evaluar los puntos débiles y recolectar evidencias, la informática antiforense utiliza técnicas para ocultar, destruir o distorsionar la evidencia digital. Esto incluye el ocultamiento de datos, la eliminación de datos, la anticoncepción de datos y la ofuscación, que pretende distorsionar la investigación forense

Informática Forense – Antiforense.

Además, se ha identificado una tendencia más reciente en la informática antiforense que ataca al software y procedimientos forenses cuestionando las herramientas o metodologías empleadas.

Esta relación entre técnicas antiforense, hacking y delitos informáticos ha llevado a un análisis del contexto legal a nivel mundial.

Por otro lado, el concepto de hacker ético también se ha discutido en relación con estas técnicas, ya que pueden ser utilizadas para mejorar el software y los procedimientos forenses



Son dos disciplinas estrechamente relacionadas en el campo de la ciberseguridad. Ambas se utilizan para proteger y mejorar la seguridad de los sistemas informáticos, aunque su enfoque y métodos son diferentes.

El hacking ético se centra en la identificación y corrección de vulnerabilidades en los sistemas de información para prevenir posibles ataques maliciosos. Los hackers éticos, también conocidos como "hackers de sombrero blanco", utilizan sus habilidades para simular ataques y evaluar la resistencia de los sistemas de seguridad de una organización o empresa. Su objetivo es asegurar que las defensas de los sistemas y redes sean efectivas y que la información esté protegida contra amenazas cibernéticas

Informática Forense – hacking ético.

En conjunto, estas dos disciplinas trabajan para mejorar la seguridad de los sistemas informáticos y proteger los activos digitales de una organización. El hacking ético encuentra las vulnerabilidades y propone soluciones, mientras que la informática forense investiga los incidentes y proporciona evidencia para tomar decisiones informadas sobre cómo prevenir futuros ataques

Informática Forense – Convenio de Budapest.

El Convenio sobre delitos cibernéticos, Convenio de Budapest sobre delitos cibernéticos o Convenio de Budapest es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes.1 Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de Canadá, Japón y China como estados observadores.

Informática Forense – Convenio de Budapest.

El Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de la seguridad en redes.5 También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la intercepción de comunicaciones privadas.

Informática Forense – Convenio de Budapest.

Los principales objetivos de este tratado son los siguientes:

1- La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.

2- La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.

3- Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Informática Forense – Convenio de Budapest.

El 1 de marzo de 2006 entró en vigor el Protocolo Adicional a la Convención sobre el delito cibernético. Los estados que lo han ratificado deben penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como amenazas racistas y xenófobas e insultos.

Informática Forense – Convenio de Budapest.

Por su parte, el segundo protocolo adicional de la convención de Budapest que habría a su firma el 12 de mayo de 2022, busca dar respuesta al desafío de obtener evidencia electrónica, que puede estar almacenada en jurisdicciones extranjeras, mientras se llevan adelante investigaciones criminales, y tiene como objetivo proporcionar herramientas para mejorar la cooperación y la divulgación de evidencia electrónica.

Informática Forense – Ley 27.411.

ARTÍCULO 1°.- Apruébase el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, que consta de CUARENTA Y OCHO (48) artículos cuya copia auténtica de su traducción al español así como de su versión en idioma inglés, como ANEXO I, forma parte de la presente.

Informática Forense – Ley 27.411.

a) La REPÚBLICA ARGENTINA hace reserva del artículo 6.1.b. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal.

b) La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388.

Informática Forense – Ley 27.411.

c) La REPÚBLICA ARGENTINA hace reserva parcial del artículo 9.1.e. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL).

d) La REPÚBLICA ARGENTINA hace reserva del artículo 22.1.d. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional.

Informática Forense – Ley 27.411.

e) La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL N° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados.

Informática Forense – Ley 26.388.

ARTICULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente.

Informática Forense – Ley 26.388.

ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Informática Forense – Ley 26.388.

ARTICULO 4º — Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Informática Forense – Ley 26.388.

ARTICULO 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente:

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).