FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

FACTORES QUE AFECTAN LA ADECUADA APLICACIÓN DE LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE ACTOS DELICTIVOS

SUSTENTADO POR:

BRENDA ISABEL RIVERA LANZA

FÁTIMA JESSILLE ARITA PAZ

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, F. M. HONDURAS, C.A.

ENERO, 2017

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON BREVÉ REYES

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANO DE LA FACULTAD DE POSTGRADO

JOSE ARNOLDO SERMEÑO LIMA

FACTORES QUE AFECTAN LA ADECUADA APLICACIÓN DE LA INFORMÁTICA FORENSE EN LA INVESTIGACIÓN DE ACTOS DELICTIVOS

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR

CARLOS ROBERTO ARIAS

MIEMBROS DE LA TERNA (O COMISIÓN EVALUADORA):

RODOLFO VELÁSQUEZ

JUAN MARTÍN HERNÁNDEZ

GEOVANNY FORTÍN

DEDICATORIA

Agradecida con Dios, por darme la sabiduría necesaria para lograr uno de mis sueños propuestos, porque me ha guiado a lo largo de toda mi vida y me ha brindado bendiciones, aprendizajes y experiencias que día con día cultivan mi ser. A mi madre, por su apoyo invaluable, por incentivarme a seguir adelante en mis metas profesionales y educativas.

Fátima Arita

AMDG, a Dios por permitirme alcanzar esta meta, por darme sabiduría y fortaleza en cada una de las etapas de mi vida. A mi madre y en memoria de mis abuelos Jesús e Isabel.

Brenda Rivera

AGRADECIMIENTOS

Queremos agradecer en primer lugar a nuestros padres, hermanos y demás familia, así como a nuestros amigos, compañeros de generación y compañeros de trabajo por todo su apoyo en este proceso.

Al Abogado Ernesto Urbina Soto, por su apoyo y asesoramiento en temas legales relacionados con el tema investigado.

A Mario Salgado un agradecimiento especial por todo su apoyo.

Agradecer a nuestro asesor de tesis Doctor Carlos Roberto Arias, por su orientación en la elaboración de nuestro proyecto.

Agradecemos a UNITEC, por la oportunidad de formar parte de su alumnado y presentar nuestro proyecto de tesis.

A todos, Gracias.

Fátima Arita y Brenda Rivera

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE APÉNDICE

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

En el primer capítulo se expondrá la naturaleza del estudio realizado, partiendo de una introducción que pone en contexto el tema y plantea de forma general en qué consiste la investigación realizada, se realiza la definición del problema, así como el planteamiento del objetivo general y los objetivos específicos y la justificación de la importancia de dicho estudio, validando así el mismo y la investigación realizada.

1.1 INTRODUCCIÓN

Los avances en las tecnologías de la información y comunicación generan cambios en nuestra sociedad y en los usos que le damos tanto a nivel personal como empresarial, estos cambios a su vez ocasionan que otros sectores deban actualizarse para estar a la par de las exigencias que dichos avances plantean.

Uno de los sectores afectados es el judicial y los entes encargados de impartir justicia, así como aquellos profesionales que realizan investigaciones de delitos donde existen componentes informáticos. Este impacto se debe al surgimiento de la informática forense, como ciencia encargada de apoyar las investigaciones de hechos delictivos donde se da participación de la informática, esto debido a que a través de los años han surgido una serie de delitos relacionados con esta rama.

La investigación de delitos puede resultar una tarea compleja, adicional a las facilidades que las tecnologías de la información y comunicación provee los delincuentes provoca un incremento a esta complejidad, por lo que resulta imperativo contar con personal capacitado (auditores y peritos forenses tecnológicos) en el desarrollo de investigaciones de índole forense orientados al campo informático, profesionales tanto del sector público como privado, que realicen trabajos orientados a establecer la comisión de un delito mediante el uso de equipo o software informático o cuyo fin del delito sea un equipo o programa informático.

De igual forma es necesario contar con un aparato judicial, que parta desde leyes que tipifiquen los delitos informáticos y dé validez a las pruebas obtenidas en el desarrollo del proceso investigativo hasta jueces que conozcan sobre este tipo de análisis.

Partiendo de lo expuesto anteriormente, se considera conveniente realizar un estudio que permita identificar la situación actual de la investigación forense en el campo informático específicamente en Tegucigalpa, y que como resultado permitirá conocer sobre algunos de los factores que afectan su correcta aplicación.

En el primer capítulo se plasma a nivel general cuál es el problema que se ha encontrado y las preguntas y objetivos a los que se busca dar respuesta mediante la investigación, así como la debida justificación que da lugar a la misma.

En el capítulo segundo se encuentra el análisis de la situación actual, partiendo de la situación a nivel mundial hasta concluir con la situación nacional, de igual manera se presentan aquellas teorías relacionadas con la informática forense, los objetivos que persigue y los pasos y procedimientos que se deben seguir al momento de su aplicación.

De igual manera se desarrollan una serie de conceptos que son de conocimiento indispensable para una mejor comprensión del tema.

En el tercer capítulo se plasma la metodología utilizada para el desarrollo de la investigación, también se presentan las variables consideradas para apoyo de la misma y la forma en la que se relacionan entre sí y con los objetivos planteados en el capítulo primero.

El capítulo cuarto se ha reservado para los resultados arrojados al finalizar la investigación efectuada y que se realizó considerando varios aspectos. El análisis de las entrevistas y encuestas realizadas se ve reflejado en este mismo capítulo.

Las conclusiones y recomendaciones planteadas en el quinto capítulo están basadas en el análisis y resultados expuestos en el capítulo anterior, y su propósito es brindar recomendaciones que permitan mejoras en el campo estudiado.

1.2 ANTECEDENTES DEL PROBLEMA

El uso de herramientas o dispositivos tecnológicos en las actividades diarias tanto personales, empresariales y comerciales y los avances que la tecnología ha experimentado a través de los años, ocasiona que exista un alto riesgo de verse involucrado en delitos donde uno o más de sus componentes sean relacionados a tecnologías de información y comunicación, por lo que resulta importante contar con profesionales capacitados y herramientas adecuadas que permitan llevar a cabo investigaciones correctas y oportunas.

Es por ello que ante esta necesidad surge una rama dentro de la informática que se conoce como Informática Forense, encargada de realizar estudios y análisis a los equipos o componentes tecnológicos que se ven involucrados en delitos.

El uso de la Informática Forense en los Estados Unidos surge en la década de los ochenta, siendo pionero en la materia, posteriormente se inició en países europeos. En Honduras, el uso de esta rama de la computación actualmente se encuentra en su etapa inicial, ya que hasta hace unos años era un tema desconocido aún entre los profesionales del medio informático.

En el medio hondureño es un campo no muy estudiado y utilizado, por lo que nos encontramos con inconvenientes como vacíos jurídicos y legales que no permiten un adecuado accionar de los entes encargados de impartir justicia, de igual manera los investigadores se ven limitados debido a la poca preparación de personal involucrado, falta de equipo y herramientas especializadas, dando como resultados que las investigaciones no siempre se lleven a cabo de manera correcta.

Sumado a esto en el país no se cuenta con instituciones educativas que preparen personal en las áreas involucradas, como por ejemplo técnicos especialistas en informática forense que conozcan las mejores prácticas, normas que regulan las investigaciones, la importancia de preservar la evidencia digital y de cuidar la cadena de custodia, o profesionales del derecho con orientación a derecho informático, hasta el momento no es parte del pensum de la licenciatura en leyes dentro del país. Los pocos que conocen de la materia en el espacio territorial han obtenido la información mediante una combinación de estudios, abogados que han hecho estudios en el

área de tecnología a nivel de licenciaturas y/o Maestrías; abogados que por su relación laboral o afinidad personal se han interesado en los temas jurídicos en los que interviene la tecnología; dicha especialidad es un tanto compleja para el jurista por el dominio de la "jerga" tecnológica que debe conocer para: Redactar normas adecuadas; interpretar las normas ya existentes a fin de regular correctamente el sector tecnológico en el país, evitando de esta forma los abusos en que pueden ser sometidas las personas por el uso de las tecnologías que están a disposición de ciertos usuarios.

1.3 DEFINICIÓN DEL PROBLEMA

1.3.1 ENUNCIADO DEL PROBLEMA

La evolución tecnológica, así como el surgimiento de nuevos delitos y los cambios en la forma de operar de la delincuencia han provocado cambios en la forma de realizar investigaciones, sobre todo en aquellos casos que hacen referencia a delitos con elementos tecnológicos sea como fin o medio, por lo que los entes y/o personas encargadas de realizar estas investigaciones han debido realizar cambios en su preparación y proceder.

En Honduras, la investigación forense sea pública o privada, a través de los años ha mostrado ciertas debilidades, ya sea en la investigación propiamente dicha -que incluye conocer sobre el delito, la obtención de evidencia, el proceso de custodia, entre otros- o en el proceso de legalización del delito y su judicialización, corriendo la investigación de delitos tecnológicos con esta misma suerte.

Es por esta razón que resulta necesario realizar un estudio que permita identificar qué factores intervienen en la investigación forense orientada a hechos delictivos informáticos y cuales afectan su adecuada aplicación.

1.3.2 FORMULACIÓN DEL PROBLEMA

Al momento de aplicar la informática forense se involucran una serie de factores que pueden afectar la investigación delictiva que se lleva a cabo, por ejemplo, el especialista responsable de la resolución del caso en controversia, los instrumentos y metodologías que

utiliza, conocimiento del personal, entre otros factores que pueden alterar los resultados de la misma. Razón por la cual es necesario realizar una investigación que permita dar respuesta a la siguiente interrogante:

¿Qué factores perjudican la correcta aplicación de la informática forense en la investigación de hechos delictivos que involucran componentes tecnológicos en la ciudad de Tegucigalpa?

1.3.3 PREGUNTAS DE INVESTIGACIÓN

- ¿Qué recursos deben utilizarse en la realización de una auditoría forense?
- ¿Qué otros conocimientos tienen relación con la informática forense?
- ¿Cuáles son las normas que regulan la aplicación y ejecución de la informática forense?
- ¿Cuál es la instrucción requerida para formarse como auditor de informática forense?

1.4 OBJETIVOS DEL PROYECTO

Las investigaciones de hechos delictivos que involucran componentes tecnológicos en Tegucigalpa, no se desarrollan con todas las herramientas y personal necesario y/o adecuado, evitando con ello que las mismas arrojen resultados que permitan concretar satisfactoriamente los casos investigados, una de las materias que se ve afectada es la informática forense, es por esta razón que surge la necesidad de indagar sobre los factores y elementos más relevantes que no permiten realizar investigaciones exitosas.

1.4.1 OBJETIVO GENERAL

Determinar qué factores perjudican la correcta aplicación de la informática forense en la investigación de hechos delictivos que involucran componentes tecnológicos en la ciudad de Tegucigalpa.

1.4.2 OBJETIVOS ESPECÍFICOS

- Determinar los recursos que deben utilizarse para realizar una auditoría forense informática.

- Investigar las ramas y/o conocimientos que están relacionadas al momento de aplicar informática forense en casos delictivos.

- Describir las normas, estándares, mejores prácticas y guías relacionadas a la aplicación y ejecución de casos delictivos que involucran evidencia digital.

- Dar a conocer los atributos, capacidades, habilidades y/o conocimientos que se requiere para convertirse en un auditor de la informática forense.

1.5 JUSTIFICACIÓN

Las actividades cotidianas en los últimos años han sufrido cambios, en gran medida gracias a la incursión de la tecnología en el día a día y las facilidades que brindan los avances que la misma proporciona, hace que la vida sin herramientas tecnológicas sea casi inconcebible. Pero a la par de todas las ventajas que nos proveen dichas herramientas esta la contraparte, que es relacionada con el mal uso que se hace de las mismas y los hábitos poco adecuados que se tienen, lo que ocasiona se genere una exposición por parte de la ciudadanía, como de las empresas a los delitos relacionados con factores tecnológicos.

Honduras, no es ajena a dicha situación, pues se conoce que existe la comisión de delitos tecnológicos, que pasan desde ataques de denegación de servicio, fraudes electrónicos o delitos considerados más graves como lo es la extorsión o la pornografía. En el Artículo "Ciberdelito en América Latina y el Caribe, Una visión desde la Sociedad Civil" para el año 2013 coloca a Honduras como un país altamente vulnerable a los ciberdelitos (Prandini & Maggiore, 2013). Por otra parte el Artículo "La geografía del ciberdelito: América Latina" del años 2012, muestra que la cantidad de usuarios atacados vía web es de 37%, no muy lejano al primer lugar que en ese momento pertenecía a Chile con un 39% (Kaspersky, 2012).

El Observatorio de Delitos Informáticos de Latinoamérica (ODILA), que permite realizar denuncias en línea y tiene como fin servir de guía al denunciante sobre el actuar al ser víctima de un delito cibernético, en su 2do. Informe del Observatorio de Delitos Informáticos de

Latinoamérica (2016), el cual es generado a partir de 1260 denuncias recibidas entre el 16 de junio 2015 y el 16 de junio 2016 indica que en Latinoamérica la mayoría de este tipo de delitos no es denunciado, en gran medida a que las personas son saben dónde denunciar. En dicho informe se observa como el delito más común es el Hacking seguido del fraude informático. Cabe mencionar que a Honduras corresponde para el período presentado el 7.94% de las denuncias, siendo el 3er país con más denuncias en el Observatorio, en comparación con un 2.33 del periodo 2014-2015.

Por otra parte, en el documento "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte de Ignacio (2013), muestra la estadística sobre el nivel de sanción penal de los delitos analizados en el mismo o la protección jurídica penal, donde Honduras tiene un 50%. En dicho estudio se presenta también el resultado de la investigación por delitos sancionados, siendo a nivel general el abuso de los dispositivos el más sancionado y el acceso ilícito, la pornografía infantil y el atentado contra la seguridad de los datos, los menos sancionados.

La Organización de Estados Americanos en el Informe Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, del año 2016 el cual fue realizado en colaboración entre el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA), y que muestra un reporte por países sobre el estado actual de la seguridad cibernética, indica que en el país existen una población de 7.961.680 personas, 7.725.092 abonados de teléfonos celular y las personas con acceso a internet son 1.512.719 lo que representa una penetración del 19%. Igualmente en dicho informe se hace mención sobre los esfuerzos que se realizan por mejorar la seguridad de los activos sin embargo estos no han dado los resultados esperados (Banco Interamericano de Desarrollo, 2016).

La presente investigación se realizó con el propósito de indagar en el campo de la Informática Forense aquellos factores que se ven involucrados en la aplicabilidad de metodologías y el uso de hardware y software forense, durante la investigación de actos delictivos donde se ven involucrados componentes tecnológicos y que pueden ser considerados medios probatorios.

Este campo de estudio es objeto de inquisición debido a que en la actualidad existe debilidad en la resolución de casos delictivos en instituciones judiciales, financieras, comerciales y demás.

La información recabada durante la investigación servirá para dar a conocer los principales factores que retrasan, interrumpen o afectan la resolución de actos delictivos donde dispositivos tecnológicos estén involucrados, permitiendo con ello se orienten esfuerzos tanto académicos, profesionales y judiciales para mejorar los aspectos señalados buscando así mejorar la aplicación y resultados de los análisis informáticos forenses.

CAPÍTULO II. MARCO TEÓRICO

En el marco teórico se presentan varias secciones para un mejor enfoque en cuanto al tema estudiado, los apartados serán: Un primer apartado sobre la situación actual, en el segundo se plantean las generalidades de la Informática Forense (definición, objetivos, pasos, procedimientos, usos, principios, ciencias relacionadas, elementos a analizar, y el especialista forense), así como las técnicas aplicadas, herramientas utilizadas, metodologías, y los delitos investigados por medio de la Informática Forense, de igual forma las evidencias y pruebas periciales y un tercer apartado donde se detallan las normas o guías internacionales y las legislaciones nacionales.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

2.1.1 INFORMÁTICA FORENSE EN EL MUNDO

Como se mencionó anteriormente, Estados Unidos es pionero en la materia, sin embargo, existen otros países que al ver la necesidad de atacar los peligros a los que las tecnologías de la información los expone por el mal uso que pueda hacerse de las mismas, consideraron necesario tomar medidas que permitan poder judicializar los delitos que son informáticos, entre las medidas legales que fueron tomadas podemos mencionar las que se detallan en la Tabla 1:

Tabla 1. Legislaciones de delitos de delitos informáticos en Estados Unidos y Europa

PAÍS	LEGISLACIÓN
Alemania	En el año 1986 en Alemania se adoptó la Segunda "Ley contra la Criminalidad Económica", que permite judicializar varios delitos informáticos y cuenta con el Centro Nacional de Ciberdefensa (Balanta, 2009).
Austria	Durante el año de 1987 reformaron el "Código Penal", con la finalidad de incluir los delitos relacionados con tecnología (Balanta, 2009).
Francia	Para el año de 1988 crearon la "ley número 88-19" que contempla los delitos informáticos (Acurio Del Pino)

Continuación de la Tabla 1.

PAÍS	LEGISLACIÓN
Estados Unidos	En el año 1994 modificaron el Acta de Fraude y Abuso Computacional correspondiente al año 1986, mediante el Acta Federal de Abuso Computacional (Balanta, 2009)
Inglaterra	Para el año 1990 mediante el Computer Misuse Act introduce el delito de acceso no autorizado, mediante la Ley de Abusos Informáticos, misma que fue modificada en 1994 (Viega Rodríguez, 2011).
España	Las actividades relacionadas con crimen tecnológico en el año 1995 con reformas a la "Ley orgánica" (Acurio Del Pino).

Fuente: (Viega Rodríguez, 2011)

2.1.2 INFORMÁTICA FORENSE EN AMÉRICA LATINA

En Latinoamérica aún y cuando se debe reconocer que la toma de conciencia en cuanto a la importancia de este tipo de delitos fue de forma tardía en comparación a los países europeos y Estados Unidos se están realizando esfuerzos por contrarrestar la criminalidad mediante delitos informáticos. Países como Bolivia, Chile, Argentina, Perú y Colombia son pioneros en la aplicación de forense informática, contando con leyes que hacen una referencia más específica a este tipo de delitos, también son países que cuentan con capacitaciones especializadas en Informática Forense.

Por otra parte, un grupo de estudiantes de la Universidad Nacional Autónoma de México (UNAM), con especial interés en la Informática Forense, desarrollaron el primer sistema operativo de Latinoamérica, sistema basado en el kernel de linux, en español y combina una serie de herramientas que permiten un análisis efectivo de los dispositivos electrónicos (Valencia Juliao, 2015).

A continuación, en la Tabla 2, se exponen las leyes que son utilizadas en algunos países latinoamericanos:

Tabla 2. Legislación en algunos países latinoamericanos

PAÍS	LEGISLACIÓN
Perú	La legislación peruana tipifica una serie de delitos informáticos en su "Ley 27,309" con fecha 26 de junio de 2000 (Balanta, 2009). informáticos
Uruguay	Las leyes de Uruguay tipifican delitos considerados informáticos en el "Acuerdo de la Ronda Uruguay de Aranceles Aduaneros y Comercio" (Viega Rodríguez, 2011).
Chile	Fue el primer país latinoamericano que aprobó una ley que contempla los delitos informáticos en 1993, al aprobar la "Ley 19,223" (Balanta, 2009).
Argentina	Con la "Ley 26388" del año 2008 realizaron modificaciones al Código Penal e incluyeron delitos informáticos (Balanta, 2009).
Colombia	"Ley 1273" de 2009 se crean nuevos tipos penales relacionados con delitos informáticos (Canedo Estrada, 2010).
Costa Rica	"Ley 8148 mediante Gaceta oficial 9.11.2001". Sanciona aquellos delitos que ya se encuentran en Ley pero que se cometen utilizando medios informáticos (Balanta, 2009).
Guatemala	En su legislación "Código Penal" tipifican los delitos informáticos (Balanta, 2009).
México	En el año 1999 se modificó la legislación para incluir los delitos informáticos. Creando el "Código Penal Federal" (Jiménez Rojas, 2016)
Puerto Rico	Tipifica los delitos informáticos en su "Código Penal" (Balanta, 2009).
El Salvador	En el año 2016 se aprobó la "Ley Contra Delitos Informáticos"
República Dominicana	Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología del 23 de abril de 2007 (Ley No. 53-07, 2007)
Panamá	En su Código Penal se contemplan los delitos informáticos (Balanta, 2009), se han realizado modificaciones en su legislación de derecho sustantivo y procesal para incluir en los delitos informáticos (Departamento de Cooperación Jurídica, 2011).

Fuente: (Balanta, 2009), (Canedo Estrada, 2010), (Jiménez Rojas, 2016) y (Departamento de Cooperación Jurídica, 2011).

Adicional a la legislación de cada país, existe el convenio sobre ciberseguridad, conocido también como Convenio de Budapest sobre ciberdelincuencia, que representa el primer tratado con carácter internacional y cuya intención es crear legislación penal común que permita hacer frente a los delitos informáticos. La apertura del tratado fue el veintitrés de noviembre de dos mil uno en la ciudad de Budapest y entró en vigor el día uno de julio de dos mil cuatro (Council of Europe, 2016).

Este convenio ha sido firmado y ratificado tanto por miembros del Consejo de Europa como por países que han sido invitados. En el apéndice D se presenta un listado con los países que han ratificado el Convenio, cabe mencionar que Honduras no forma parte de esta lista.

2.1.3 INFORMÁTICA FORENSE EN HONDURAS

En Honduras la aplicación de la investigación informática es relativamente nueva, por lo que se puede considerar como una ciencia que se encuentra en desarrollo, sumado a las deficiencias históricas de la investigación en Honduras, podemos indicar que existen muchas oportunidades de desarrollo en esta materia.

En la actualidad se cuenta con pocos profesionales capacitados en la materia, tanto a nivel informático como en las materias relacionadas, razón por la cual se dificulta la aplicación de auditorías forense, adicional a la falta de equipos y herramientas (Hardware y Software) adecuadas por lo que los resultados de las investigaciones son fácilmente objetables como medios probatorios.

A nivel de órganos de seguridad nacional, en los últimos años se han realizado esfuerzos por disminuir esa brecha de no aplicabilidad de una adecuada investigación delictiva, en todos los ámbitos, incluidos aquellos delitos de orden tecnológico, creando agencias de investigación, realizando modificaciones legales, incrementos al presupuesto de seguridad entre otros, sin embargo estos esfuerzos aún no son suficientes para mejorar sustancialmente las investigaciones, ya que en el país no se cuenta con un laboratorio certificado y especializado en informática forense ni con equipo suficiente para realizar el análisis de la evidencia, sumado al hecho que el personal que realiza el peritaje no está correctamente capacitado y en ocasiones desconoce de temas informáticos, por lo que las investigaciones no siempre se realizan en el marco de las buenas prácticas.

Adicionalmente se encuentra el hecho que los entes encargados de impartir justicia muchas veces desconocen este tipo de trabajo o el peso que la evidencia informática tiene en un caso judicial.

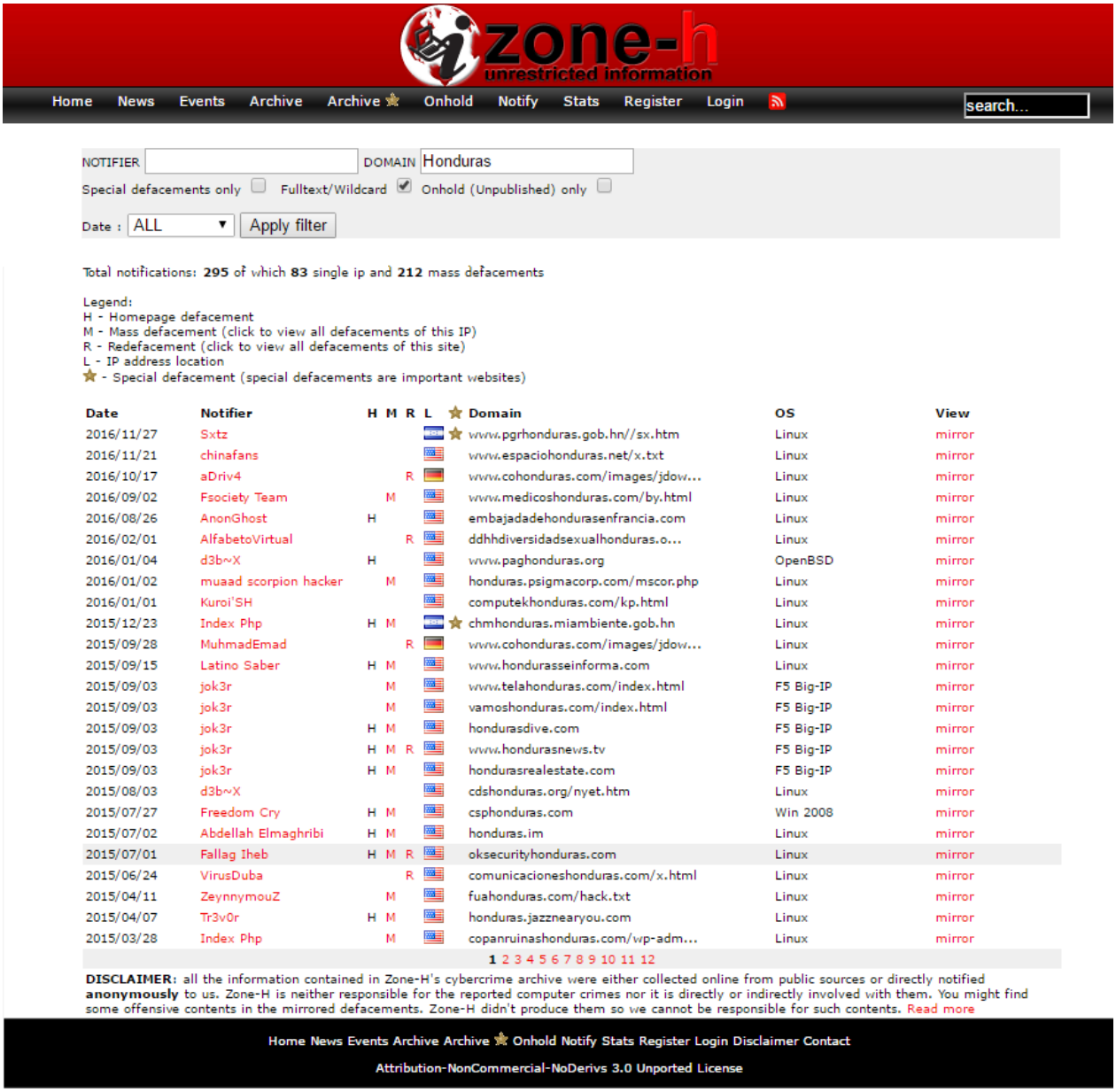


Figura 1. Dominios de sitios web hondureños que han sido hackeados.

Fuente: (i zone-h unrestricted information)

En el estudio desarrollado por el Observatorio de la Ciberseguridad en América Latina perteneciente a la Organización de los Estados Americanos (OEA), el cual mide la madurez y situación actual que en temas de seguridad cibernética tienen los países de América Latina, hace referencia a la falta de carencia de una política de seguridad cibernética y de un marco legal para

seguridad de las Tecnologías de la Información, de igual manera hace alusión a las medidas que se están tomando para contrarrestar la capacidad limitada que se tiene actualmente.

En dicho estudio se puede encontrar un detalle de la situación actual, evaluada desde diferentes aspectos como ser legislación, conciencia sobre seguridad cibernética, gestión de crisis, entre otros. De igual manera se puede realizar un comparativo con otros países latinoamericanos que permite visualizar las diferencias existentes entre cada punto evaluado. En el apéndice E podrá encontrar un cuadro comparativo de los cinco países de Centroamérica (Observatorio de la Ciberseguridad en América Latina y el Caribe, 2016).

Igualmente, en el sitio web Zone-H.org que es un sitio donde entre otras cosas se registran los sitios web que han sufrido algún tipo de ataque cibernético, se muestra como Honduras ha sido víctima de este tipo de delitos. En la imagen Figura 1 se muestra un resultado sobre los sitios relacionados con Honduras.

2.1.3.1 INSTITUCIONES IMPLICADAS EN LA APLICACIÓN DE LA INFORMÁTICA FORENSE

Con la finalidad de esclarecer casos delictivos ya sea meramente informáticos o que involucren componentes tecnológicos y evitar que estos queden impunes, existen instituciones en el país, encargadas de proteger los derechos de los ciudadanos nacionales o residentes, así como los de las empresas públicas o privadas, para investigar, resolver y hacer cumplir la justicia amparados en legislación nacional en aquellas situaciones en las que se pueda aplicar.

En la resolución de un caso delictivo, el Ministerio Público es el encargado de la parte acusatoria y de la búsqueda de pruebas incriminatorias, también forma parte en estos procesos judiciales como el ente encargado de guardar la cadena de custodia, una vez concluida la investigación por parte del Ministerio Público a través de sus diferentes fiscalías, remite los resultados a los Juzgados pertinentes, ya que estos se encargan de verificar el cumplimiento de las leyes y dar el veredicto final el cual es comunicado por los medios con lo que cuente la institución, que en la mayoría de casos es un juez.

También se cuenta con el apoyo de Agencias que han sido especializadas y son encargadas de realizar investigaciones estratégicas y de inteligencia.

1. Ministerio Público (MP)

El Ministerio Público es la institución encargada de llevar a cabo las investigaciones judiciales en el país y es uno para toda la República. Sus funciones son ejecutadas según los principios de actuación y con dependencia en la materia a la cual han sido asignados y sus funcionarios están bajo la dependencia del Fiscal General de la República y en el ejercicio de sus funciones goza de independencia completa.

Los funcionarios del Ministerio Público para realizar intervenciones legales les basta presentarse y comparecer ante los tribunales de justicia y podrán a su vez ordenar que cualquier persona comparezca ante la justicia.

El Ministerio Público tiene a su cargo las diferentes fiscalías especiales de la República (ver inciso 5), incluidas las Fiscalía de Protección Intelectual y Delitos Informáticos, razón por la cual se contempla como parte de la investigación (Ministerio Público, 2014).

Fue establecido mediante decreto N° 228-93, el cual promulga la Ley del Ministerio Público, con fecha veinte de diciembre de mil novecientos noventa y tres (Diario La Gaceta Núm. 27241 del seis de enero de 1994).

2. Dirección Nacional de Investigación e Inteligencia (DNII)

La DNII fue creada mediante la Ley de Inteligencia Nacional, decreto N° 211-2012 que fue aprobada por el Congreso Nacional el dieciocho de enero del dos mil trece, como parte de la Ley de Visión de País y el Plan de Nación (Diario La Gaceta Núm. 33,099 del 15 de abril del 2013).

La Dirección Nacional de Investigación e Inteligencia tendrá como objeto desarrollar actividades de investigación e inteligencia para proteger los derechos y libertades de los ciudadanos y residentes en el país, prevenir y contrarrestar amenazas internas o externas contra el

orden constitucional y ejecutar las políticas públicas que en materia de defensa y seguridad establezca el Consejo Nacional de Defensa y Seguridad (DNII).

Las instituciones del Estado especializadas en Inteligencia son: La DNII, las Fuerzas Armadas de Honduras, La Policía Nacional, Secretaria de Estado en el Despacho de Relaciones Exteriores y la Unidad de Información Financiera (UIF) (Art. 6 Ley de Inteligencia Nacional).

3. Agencia Técnica de Investigación Criminal (ATIC)

La Agencia Técnica de Investigación Criminal, integrante del Ministerio Público y ente investigativo y especializado en la resolución de delitos judiciales graves y de fuerte impacto social y que ayuden a sustentar con pruebas que puedan ser evidencia en los tribunales de justicia.

Esta Agencia Especial fue creada bajo el Decreto 379-2013, del veinte de febrero de dos mil catorce (Diario La Gaceta Núm. 33,382 del diez y ocho de marzo del año dos mil catorce).

4. Dirección Policial de Investigación (DPI)

Fue creada bajo las reformas realizadas al Sistema de Investigación Criminal de la Policía Nacional, anteriormente era conocida como Dirección Nacional de Investigación Criminal (DNIC). La DPI trabaja bajo la orientación judicial del Ministerio Público y su finalidad es proveer de elementos probatorios para el ejercicio penal en delitos de acción pública. Fue creada mediante Decreto Ejecutivo N° PCM-063-2015 a los catorce días del mes de septiembre del dos mil quince (Diario la Gaceta Núm. 33979 del ocho de marzo del dos mil diez y seis).

5. Fiscalías Especiales

En Honduras contamos con una serie de Fiscalías especializadas en materias distintas, en la Tabla 3 se encuentran cada una de ellas:

Tabla 3. Fiscalías Especiales

SIGLAS	FISCALÍA
FEDCV	Fiscalía Especial de Delitos Contra la Vida
FEDH	Fiscalía Especial de Derechos Humanos
FEN	Fiscalía Especial de la Niñez
FEM	Fiscalía Especial de la Mujer
FETCCOP	Fiscalía Especial para la Transparencia y Combate a la Corrupción Pública
FESCCO	Fiscalía Especial Contra el Crimen Organizado
FEDC	Fiscalía Especial de Delitos Comunes
FEMC	Fiscalía Especial en Materia Civil
FEPROSI	Fiscalía Especial de Propiedad Intelectual y Seguridad Informática.

Fuente: (Ministerio Público, 2016)

La Fiscalía Especial de Propiedad Intelectual y Seguridad Informática forma parte de un convenio con los Estados Unidos para luchar por la protección a la propiedad intelectual, y surge mediante la firma con la oficina Comercial de los Estados Unidos (USTR), del Plan de Acción para la protección a la Propiedad Intelectual en noviembre del dos mil quince, y son los encargados de llevar los casos relacionados con delitos que atentan contra los derechos de autor como ser piratería y falsificación.

6. Corte Suprema de Justicia (CSJ)

La Corte Suprema de Justicia es el poder Judicial, y cuenta con jurisdicción territorial en todo el país, está organizada en cuatro Salas (Constitucional, Civil, Penal y Laboral-Contencioso Administrativo), quince Cortes de apelación y los diez y seis Tribunales de sentencia, los diferentes Juzgados igualmente forman parte de la Corte Suprema.

Es el ente encargado de impartir justicia a través de jueves independientes que se rigen bajo la legislación nacional y los tratados internacionales, garantizando la seguridad jurídica del país (Poder Judicial, 2016).

En el anexo 6.1 se presenta la información de una investigación realizada en una empresa privada hondureña, por personal que labora en la misma, haciendo uso de Informática Forense. Dicha investigación concluyó con la identificación del causante del delito, sin embargo, aun y cuando se contaba con los medios de prueba, el mismo no pudo ser judicializado por los vacíos legales existentes.

2.2 TEORÍAS

Acurio Del Pino (2009) menciona: "El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales."

La Informática Forense, también conocida como computación forense o análisis forense consiste en aplicar técnicas científicas y de análisis a equipo tecnológico que permita presentar información válida dentro de un proceso judicial.

Según McKennish (1998), el análisis forense "es la técnica de capturar, procesar e investigar información procedente de sistemas informáticos utilizando una metodología con el fin de que pueda ser utilizada en la justicia".

Es utilizada en la investigación de delitos donde existan componentes tecnológicos, ya que consiste en investigar los equipos y/o sistemas de información de las empresas o personas con la finalidad de detectar cualquier evidencia o rastro que contribuya al esclarecimiento de un crimen.

El origen de la informática forense se remonta a la década de los ochenta, cuando las computadoras personales tuvieron mayor apertura en el mercado y su acceso fue posible para un mayor número de personas. Para el año 1984 es creado el Equipo de Análisis de Computación (CART por sus siglas en inglés), un proyecto que surge de la Oficina Federal de Investigación (FBI por sus siglas en inglés), posteriormente un agente especial de la División de Investigación Criminal del Servicio de Impuestos Internos de los Estados Unidos de nombre Michael

Anderson, inició su trabajo en este campo, por lo que es conocido como el padre de la informática forense.

En el año 1988 se creó la Asociación Internacional de Especialista en Investigación Informática (IACIS por sus siglas en inglés), como ente encargado de certificar a los profesionales en el ámbito forense mediante el Examinador Certificado de Computación Forense (CFCE por sus siglas en inglés), y en el año 1995 se fundó la Organización Internacional de Evidencia Digital (IOCE por sus siglas en inglés).

2.2.1 OBJETIVOS DE LA INFORMÁTICA FORENSE

La informática forense plantea varios beneficios y objetivos, entre los cuales se pueden mencionar los siguientes:

- La informática forense permite garantizar que las políticas de seguridad de una organización son efectivas, esto debido a que pueden realizarse auditorías preventivas que dan la oportunidad de crear y aplicar medidas preventivas para disminuir el riesgo de ser víctima de un delito informático.

- Si el delito se dio, la computación forense provee apoyo para la persecución y procesamiento judicial de criminales, gracias a la obtención de rastros, huellas digitales, que permitan dar indicios racionales del origen del delito, probar el origen y el responsable del mismo.

- Compensación de daños causados por los criminales. Esto se logra gracias a la reconstrucción del hecho y la identificación de los daños causados.

Estos objetivos se logran mediante la recolección de los medios de prueba de los hechos (López, Amaya, & León, 2001).

Para realizar una auditoría informática forense que permita dar cumplimiento a los objetivos se requiere que sea realizada por personal experimentado y que conozca la información general sobre el delito a perseguir.

De igual forma considerando lo recomendado por la empresa de Auditores de Seguridad de Internet (ISA por sus siglas en inglés), para un procedimiento exitoso es necesario conocer "las normas bajo las cuales se realiza la recolección de medios de prueba y las condiciones en las que el medio de prueba será admisible, autentica, completa, confiable y creíble. De igual manera se deberá conocer el procedimiento para ejecutar la investigación, cuando se llevará a cabo y los factores legales a considerar" (Internet Security Auditors, 2016).

Como menciona Arias Chaves (2007), en su artículo Panorama general de la Informática Forense y de los delitos informáticos en Costa Rica, "básicamente la importancia de la informática forense radica en identificar y determinar los perjuicios generados por el ataque(s) al que ha sido víctima una organización en particular".

2.2.2 CARACTERÍSTICAS DE LA INFORMÁTICA FORENSE

a) La informática forense debe contar con varias características, que permite el cumplimiento de los objetivos que al aplicarla se buscan.
b) La informática forense se aplica con un propósito, el cual es obtener suficiente y adecuada evidencia, como medio de prueba de un delito.
c) Busca una verdad histórica de los hechos y se basa en evidencia, por lo que es objetiva.
d) Sigue una metodología ya que sigue un orden establecido, en el cual se aplican técnicas que permiten la recolección de pruebas.
e) Se encuentra sujeta a una Normativa y Legislación vigente en el país.
f) La informática forense es importante ya que apoya la investigación de un ilícito.
g) El periodo de investigación es desde el inicio del hecho hasta su fin.

2.2.3 PASOS DE LA INFORMÁTICA FORENSE

La informática forense combina una serie de áreas que van desde la investigación, el análisis de información, la recopilación de pruebas y evidencias legales, la declaración y presentación ante una corte en los casos que así lo requiera, es por esta razón que para un mejor desarrollo se realiza en pasos, los cuales se detallan a continuación:

a. Identificación

Consiste en identificar el bien informático y todas aquellas posibles fuentes disponibles, para recolectar todo medio de prueba posible y su respectivo análisis, de igual manera se debe considerar el tema legal y todas las acciones que pongan en peligro la integridad de la información.

Al momento de realizar la identificación de los posibles medios de prueba, el investigador debe conocer los antecedentes y la situación actual de los sistemas y/o equipos, lo que le permitirá definir de mejor manera el proceso a seguir con relación a las búsquedas y la investigación, en esta etapa inicia además la cadena de custodia.

b. Validación y preservación

Incluye la revisión y generación de los medios de prueba por medio de copias exactas que permiten realizar un análisis sin exponer los datos, esto se realiza mediante el uso de procedimientos forenses certificados por medio de la verdad legal, un código de validación y tecnología, también se utiliza equipo que evita la contaminación de la data permitiendo con ello que la integridad de los medios de prueba obtenida se conserve, de igual manera se debe asegurar que la cadena de custodia se realice de manera tal que asegure la integridad del medio de prueba.

c. Análisis

Se realiza aplicando técnicas analíticas y científicas, así como herramientas que permiten encontrar pruebas sobre los hechos investigados, se realiza mediante la aplicación, a la copia del medio probatorio de una serie de pruebas. Permite buscar y analizar información en diferentes niveles, como ser archivos borrados o modificados previamente, archivos renombrados, búsquedas mediante palabras claves, entre otras.

El análisis desarrollado permite determinar el patrón de comportamiento del usuario investigado.

d. Presentación

Consiste en recopilar la información obtenida en el análisis para elaborar el informe que será escrito y presentado utilizando lenguaje claro, acompañándolo de los medios de prueba recuperados. El éxito del informe depende en gran medida del buen trabajo que se realice en los pasos anteriores.

2.2.4 PROCEDIMIENTOS DE LA APLICACIÓN DE LA INFORMÁTICA FORENSE

a) Realizar esterilización de los medios de trabajo informáticos.
b) Verificar en los medios informáticos las copias, utilizando métodos certificados por la autoridad.
c) Documentar los procedimientos, herramientas y resultados de los medios informáticos que fueron analizados.
d) Realizar el mantenimiento de la cadena de custodia de los medios de prueba recolectados.
e) Elaborar el informe y presentar los resultados de los análisis realizados a los medios informáticos de prueba.
f) Administrar adecuadamente el caso realizado.
g) Efectuar una auditoría a los procedimientos realizados durante la investigación (Jeimy J. Cano, Introducción a la Informática Forense - Una disciplina técnico-legal).

En el artículo “Criminalística para informáticos forenses y peritos” de Antonio Salmerón menciona que en la investigación de delitos a través de la historia, uno de los factores que más influye en los errores de juicio con relación a los elementos de prueba que se aportan en un proceso judicial, es la no aplicación del método científico y del uso de las tecnologías que se encuentran disponibles y que permiten recolectar, comprender, realizar un análisis y la evaluación de aspectos técnicos que se presentan en los hechos criminales (Salmerón, 2015).

De igual forma se conoce que “los investigadores no han observado procedimiento específico alguno que regule la obtención, conservación y presentación de la prueba electrónica ante los Tribunales de Justicia.

En general, los países aplican por analogía la regulación del procedimiento general de la prueba tradicional" (Insa Mérida, Lázaro Herrero, & García González, 2008).

2.2.5 USOS DE LA INFORMÁTICA FORENSE

A la informática forense se le puede utilizar en diversas situaciones, y brinda apoyo en el esclarecimiento de diversos delitos, entre sus usos encontramos los siguientes:

a. Prosecución Criminal: Los medios probatorios recolectados pueden ser utilizados para procesar crímenes, como ser fraude, tráfico de drogas, pornografía, entre otros.

b. Litigación Penal: La informática forense apoya casos de delitos penales, como ser acoso o fraude.

c. Investigación de Seguros: Las compañías de seguro la utilizan para encontrar los medios de prueba que les permita disminuir los costos de reclamos relacionados con accidentes y compensaciones.

d. Temas corporativos: Puede ser utilizada para recabar información que sea medio probatorio en casos relacionados con acoso, robo, divulgación de información confidencial, espionaje industrial.

e. Mantenimiento de la ley: La ley debe actualizarse a medida cambian las formas de cometer delitos, por lo que la informática forense permite aportar información acerca de las formas de operar de los criminales (López, Amaya, & León, 2001).

"Todo hecho en el que un sistema informático esté involucrado, tanto si es el fin o un medio, puede ser objeto de estudio y análisis, y por ello, puede llevarse a juicio como medio probatorio" (Pagès López, 2013).

2.2.6 PRINCIPIOS RELACIONADOS

- Principio de Locard

El principio Locard, conocido como de Intercambio –Edmond Locard (Francia, 1877-1966)- pionero de la criminalística indica que "Cada contacto deja un rastro" lo que significa que cuando dos objetos realizan contacto siempre se transfiere material de uno hacia el otro, por lo que en una escena de crimen siempre queda algo del criminal a cambio de lo que se lleva con él.

En la computación forense este principio cobra validez con las evidencias electrónicas y el establecimiento del ¿Cómo? y el ¿Dónde? se pueden localizar las evidencias.

- El criterio de Daubert Daubert Criteria o Daubert Standard (1993)

En los Estados Unidos este criterio es utilizado ya que permite admitir una evidencia que es pertinente y fiable, se utiliza en conjunto con la regla 702 de Evidencias Federales, "si los conocimientos científicos, técnicos, u otro especializado ayudará al juzgador de hecho, para entender la evidencia o para determinar un hecho en cuestión, una testigo calificado como un experto en el conocimiento, la destreza, la experiencia, la formación, o educación, puede declarar a la misma en la forma de una opinión o de lo contrario, si:

a. el testimonio se basa en hechos o datos suficientes,

b. el testimonio es el producto de los principios y métodos fiables, y

c. el testigo tiene aplicados los principios y métodos de forma fiable a los hechos del caso" (Pagès López, 2013)

- Principios Internacionales de la IOCE

La IOCE describe principios para recuperar de manera estandarizada las pruebas, los mismos fueron presentados y aceptados en la International Hi-Tech Crime and Forensics Conference en 1999, los principios aprobados son los siguientes:

a. La toma de evidencia no debe modificar las pruebas.
b. El acceso a evidencia digital original debe ser por parte de un forense profesional.
c. Toda actividad realizada con la evidencia como ser acceso, almacenamiento, entre otras, debe documentarse plenamente y estar disponible para su revisión.
d. La responsabilidad de las acciones con respecto a las pruebas digitales es del individuo que la tenga en su posesión.
e. Las agencias o personas responsables de realizar las incautaciones, los accesos, el almacenamiento o transferencia de la evidencia, debe cumplir estos principios.

Estos principios se rigen por los atributos siguientes:

a. Consistencia con los sistemas legales
b. Uso de un lenguaje común
c. Durabilidad
d. Capacidad de traspasar fronteras
e. Generar confianza en lo referente a la integridad de las pruebas
f. Aplicación a todas las pruebas forenses
g. Aplicación a todo nivel

Adicional a los principios mencionados anteriormente encontramos principios aplicables independientes del análisis forense que se realiza, a continuación, dichos principios:

a. Evitar la contaminación: esto debido a que una prueba contaminada puede causar errores en el análisis.
b. Actuar metódicamente: se debe documentar todos los pasos realizados, la información sobre el equipo utilizado y los resultados obtenidos.
c. Controlar la cadena de valor (Federal Bureau of Investigation, 2000).

2.2.7 CIENCIAS RELACIONADAS

Al realizar un análisis forense es importante considerar el acompañamiento de profesionales de otras áreas, según el delito investigado, de manera tal que todos los rastros

dejados puedan ser considerados y dar un mayor soporte a las evidencias encontradas. Entre las ciencias/profesiones que se relacionan con la informática forense se encuentran las siguientes:

a. Derecho: es importante considerar la legislación al momento de realizar la investigación, para actuar conforme a ley, de igual forma es necesario presentar los resultados de forma tal que sea admitida las pruebas.
b. Criminalista: Permite guiar la investigación en base a los principios y mejores prácticas aplicadas en investigaciones de tipo criminal.
c. Contabilidad y Finanzas: En caso de delitos financieros relacionados con elementos tecnológicos se requiere un especialista que acompañe el proceso de recolección y análisis de evidencia, adicional al momento de elaborar el informe final es preferible contar con el especialista de la materia para plasmar los resultados de manera correcta.

Es necesario también contar con una participación interdisciplinaria de especialistas de otras ramas de la informática, como ser seguridad, base de datos, redes, entre otras, ya que esto permite que según el tipo de delito y el medio utilizado se pueda realizar el rastreo y obtención de evidencia de la mejor manera.

Contar con especialista permite presentar resultados mejor justificados y con una explicación más detallada sobre la forma en que se llevó a cabo el delito y serán de apoyo para el juzgador para aclarar cualquier duda que surja.

2.2.8 ELEMENTOS A ANALIZAR

Los elementos que se analizan, son aquellos donde se puede encontrar información que sirva como pista de auditoría y/o evidencia, entre los cuales se puede mencionar:

a. Disco duro de un servidor o computadora: Se realizan imágenes de los discos y las particiones, para poder revisar la data que en ellos se encuentra sin comprometer la información.
b. Bitácoras de seguridad: la revisión de las bitácoras es importante para identificar las operaciones realizadas con la información.

c. Credenciales de autenticación: Al verificar las autenticaciones se podrá comprobar que usuarios accedieron y si todos lo hicieron en base a los permisos otorgados, buscando con ello detectar cualquier intento de ingreso no autorizado.
d. Trazo de los paquetes de red: Al estudiar la red se podrá identificar si hubo algún tipo de intromisión a la red.
e. Teléfono Móvil o Celular: En la revisión de dispositivos de comunicación se puede conocer información relacionada con llamadas, envío de mensajes, chat, que puede ser considerada como prueba en un juicio.
f. Impresoras: Las impresoras que cuentan con memoria de impresión pueden brindar pistas sobre qué información fue impresa, que usuario la realizó y tipo de datos, que puede ser útil en caso de acusaciones por sustracción de información.
g. Memorias USB: Las memorias USB se deben estudiar para identificar si fueron utilizadas para sustracción de información o para implantar archivos maliciosos, de igual forma en algunos casos puede ser el medio de prueba al contener información relacionada con los delitos.
h. Documentación referida del caso: La documentación del caso, aun cuando sea física es necesario conocerla, ya que esta puede contener pistas de auditoría, de igual manera es necesario realizar una comparación entre los medios de prueba digital y la documentación física que permita comprobar que se conserva la integridad de la prueba (Juristas Forenses y Asociados, 2012).

2.2.9 ESPECIALISTA

Características

El especialista de la informática forense debe estar certificado y acreditado en ciencias que le permitan realizar sus funciones de la mejor manera, además debe contar con habilidades y características que le permitan realizar su labor de la mejor manera, entre estas se puede mencionar las siguientes:

- Debe ser apasionado de la tecnología y respetuoso de ella.
- Ser una persona paciente y persistente.

- Gusto por la investigación.
- Analítico
- Facilidad de comunicación, pero discreto.
- Persuasivo
- Capacidad de negociación
- Curioso y creativo

Labor del especialista en cómputo forense

El especialista forense apoya la investigación aportando sus conocimientos en la materia informática, haciendo uso de tecnología más avanzada que le permite acceder al equipo tecnológico utilizado en la comisión de un delito, en busca de huellas o rastros que permitan identificar al responsable del mismo, debe comprender lo que sucede tanto en el hardware como el software, por lo que en su trabajo debe realizar análisis de todas los elementos involucrados ya que la inobservancia puede generar resultados erróneos (Gómez, 2012).

El forense debe determinar los componentes relacionados al delito investigado, como ser naturaleza, hechos y autores.

2.2.10 TÉCNICAS

Las técnicas de auditoría informática forense son aquellos métodos que permiten reconstruir un bien informático, lo que facilita la obtención de datos para su análisis, examen y autenticación.

Existe un sin número de técnicas que permiten la verificación ocular, verificación oral o escrita, las que permiten la verificación documental y analítica. La finalidad de las técnicas informáticas es la búsqueda, preservación y análisis de la información en los equipos tecnológicos en búsqueda de evidencia de la comisión de un delito, es por ello que a la par de una metodología se deben utilizar técnicas que permitan el cumplimiento de estos fines y la correcta

interpretación de la información obtenida y una adecuada presentación de informes con pruebas que sean fiables, objetivas y transparentes.

El uso de las técnicas debe permitir la recolección de pruebas físicas y digitales, así como de las evidentes, las que han sufrido daño o se encuentren escondidas en la escena, de igual forma deben junto a la experiencia y capacidades del investigador poder construir el perfil y modus operandi del hechor.

2.2.11 HERRAMIENTAS DE SOFTWARE

En el mercado se pueden encontrar una amplia gama de herramientas de software que apoyan la realización de la informática forense, las mismas varían según el fin para el cual serán utilizadas, y las hay de diferentes precios, complejidad y requerimientos de hardware y software. En el apéndice 1 se presenta una lista de algunas de estas herramientas.

2.2.12 HARDWARE

Adicional al apoyo de herramientas de software, es necesario al momento de realizar una investigación, hacer uso de hardware especializado que permita obtener mejores resultados en la auditoria forense informática, de igual manera el hardware especializado se encuentra en el mercado con variedad de precio, capacidad, funcionalidad, soporte y rendimiento. En el apéndice 2 se detallan algunos de los equipos de hardware disponibles.

2.2.13 METODOLOGÍAS

Al igual que se cuenta con una serie de herramientas para realizar una auditoría forense informática, existen también una serie de metodologías para desarrollar dicha investigación. Las metodologías permiten una obtención segura de información sin modificación y daños desde diferentes fuentes sin alterar los datos originales ya que guían la investigación y la búsqueda de evidencia y pruebas, esta información considerada evidencia permite presentar un informe debidamente fundamentado y justificado.

La adecuada selección de la metodología a utilizar permitirá realizar una investigación más completa, con un correcto manejo de las pruebas, lo que reduce el riesgo de incurrir en errores.

Las diferentes metodologías existentes cuentan con ventajas y desventajas, y con diferentes enfoques de aplicación como ser la escena del delito o la información. En el apéndice 3 se detallan algunas de las metodologías existentes.

2.2.14 DELITOS INVESTIGADOS

El Consejo Europeo en su tratado sobre crimen cibernético se refiere por crimen cibernético como "delitos que abarcan desde actividades criminales contra datos hasta las infracciones de contenidos y de copyright" (Krone, 2005).

Para Zeviar-Geese (1997-98), esta definición es más amplia e incluye actividades como el fraude, acceso no autorizado, pornografía infantil y el acoso en internet (cyberstalking).

Para Téllez Valdes (2004), un delito informático es "en forma típica y atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Como es señalado anteriormente, el delito informático se da cuando utiliza una computadora ya sea directa o indirectamente para cometer una acción malintencionada, generando daños, hurto y/o problemas a sus víctimas, y para que se configure la acción penal debe probarse que se dio la acción típica, antijurídica, culpable y punible.

Al analizar la cantidad y de crímenes informáticos que se dan y las diferentes formas de operar, es conveniente separarlos para un mejor análisis.

Julio Téllez Valdés presenta dos clasificaciones:

a. Informática como objeto del delito.

En esta categoría se incluyen todos aquellos delitos que van dirigidos contra el equipo informático (Hardware y/o Software).

b. Informática considerada como medio del delito.

Dentro de esta clasificación se encuentran aquellos delitos donde se utiliza equipo tecnológico como medio para cometer un ilícito.

Sin embargo, María de la Luz Lima (1984), sugiere que los delitos informáticos deben clasificarse en tres categorías:

a. Los delitos donde la tecnología es utilizada como método

En esta clasificación se engloban las conductas criminales donde se utilizan métodos electrónicos para llegar al resultado ilícito.

b. Delitos donde la tecnología es un medio

Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo, y

c. Cuando la tecnología es utilizada como fin

Dentro de esta sección se encuentran aquellas acciones dirigidas contra el bien físico o su contenido con la intensión de ocasionar daño (Lima de la Luz, 1984).

Listado de algunos delitos tipificados como delitos informáticos

1. Falsificación de documentos.
2. Modificación/alteración de los registros contables.
3. Planear y/o simular delitos comunes como ser homicidio, fraude o robo, entre otros.

4. Leer, sustraer o copiar información confidencial.
5. Modificar datos entrada y/o salida.
6. Aprovechar indebidamente o violentar un código para acceder a un sistema con la finalidad de ingresar instrucciones inadecuadas.
7. Acceso no autorizado.
8. Apropiación indebida de dinero de cuentas bancarias mediante la desviación de dinero.
9. Uso de programas de computación sin la debida autorización.
10. Ingreso de líneas de código que provocan "interrupciones" en la operación lógica interna de los programas o su bloqueo total.
11. Introducción de virus informáticos que alteren el funcionamiento de los sistemas de información.
12. Obtener información impresa en papel después de ejecutados los trabajos.
13. Acceso no autorizado a áreas restringidas que pertenezcan a sistemas.
14. Intervenir sin autorización las líneas de comunicación de datos.
15. Destruir programas utilizando cualquier medio o método.
16. Dañar intencionalmente los dispositivos de almacenamiento.
17. Atentar físicamente contra una o más computadoras o sus accesorios.
18. Realizar sabotaje político o terrorismo.
19. Secuestro de información con fines de chantaje.

Por su parte la Organización de las Naciones Unidas (ONU) ha realizado su propia clasificación de los diferentes tipos de delitos informáticos reconocidos, los cuales son:

a. Manipulación de computadoras con la finalidad de cometer fraudes

Dentro de esta categoría encontramos los siguientes delitos:

1. Manipulación de los datos de entrada: Consiste en la sustracción de datos.
2. Manipulación de programas: En este caso se modifica la información y/o programas existentes, un delito difícil de descubrir.
3. Manipulación de datos de salida: En este caso se afecta el correcto funcionamiento del sistema de información.
4. Fraude por manipulación informática: Hace uso de las rutinas de repeticiones automáticas.

b. Falsificaciones informáticas.

Se clasifican en: Como objeto que se da cuando se alteran los datos de los documentos almacenados y como instrumentos, cuando se utilizan las computadoras para falsificar los documentos.

c. Daño o modificaciones a los programas o los datos computarizados.

1. Sabotaje informático: se da cuando se borra, suprime o modifica sin autorización datos o el funcionamiento de los sistemas.
2. Acceso a los sistemas informáticos sin autorización: Intrusión, sabotaje, espionaje.
3. Reproducir programas sin la debida autorización (Estrada Garavilla).

2.2.15 MEDIOS DE PRUEBA

Las pruebas digitales cada vez son más habituales en el análisis de incidentes que conlleven un litigio para hacer frente a un delito ya que son demostración legal de la verdad de un hecho. La evidencia será tan amplia como la investigación así lo requiera y el auditor la recabe. La evidencia para que sea legal y se convierta en prueba debe ser ordenada por un juez, debe obtenerse bajo un sistema de investigación y debe ser recopilada sin errores o malas prácticas, sin malicias o intención de incriminar a una persona, así mismo deberá ser documentada paso a paso los procedimientos que se llevaron a cabo para su recolección.

Dentro de la evidencia se puede encontrar:

- Documentos digitales
- Fotografías e imágenes
- Audios, videos
- Información relacionada al hardware y software.

El primer paso para obtener la evidencia consiste en recolectar los elementos físicos y la información, este paso se considera un proceso legal ya que se realiza la recolección de pruebas, mismas que manejadas de forma inadecuada pueden ser alteradas al punto que no puedan ser utilizadas.

El desafío más grande al momento de utilizar en la corte los medios de prueba digital es la detección de la manipulación de la misma cuando ésta es realizada sin dejar rastro. Algunas técnicas para realizar dicha manipulación son las siguientes:

- Ocultamiento de datos: Práctica que consiste en almacenar la data en un lugar donde no pueda ser encontrada, dentro de este grupo se encuentra la estenografía, que consiste en esconder la información dentro de otra. Para contrarrestar esto se puede hacer uso de herramientas de código abierto.

- Cifrado: Se protege la data mediante un algoritmo que mezcla la información para que no pueda ser detectada sin utilizar la llave que permite el descifrado.

- Esconder información en áreas del sistema: Existen métodos que permiten ocultar información en espacios del sistema que son áreas reservadas, estos programas permiten que los atacantes tengan acceso a una computadora y escondan la información.

- Destrucción de Data: Es el método más utilizado por parte de los cibercriminales ya que es sencillo remover o eliminar cualquier rastro que se les vincule.

- Ofuscación de trayecto (rastro): El cual consiste en realizar cambios en la información que no la destruyan pero que dificultan su entendimiento o lectura. Existen tres métodos básicos, el primero tiene como objetivo oscurecer información requerida para la investigación, el segundo consiste en alterar la data relacionada con los equipos forenses alterando la meta data, y el tercer método es la eliminación o modificación de bitácoras con el propósito de desviar atención de las acciones.

- Data Anticoncepción (Contracepción): Permite evitar el origen de la evidencia buscada, consiste en utilizar software que no dejan pistas de trazabilidad en el sistema operativo.

- Fabricación de Data: Modificar data o la creación de data excesiva de un tipo específico, para desviar la atención de la investigación tanto que se llega a considerar si dar continuidad o no con la misma.

- Ataques al Sistema de Archivos: Se genera un ataque severo al sistema para impedir se realice de forma correcta la investigación forense.

El medio donde se encuentra la evidencia material probatoria no es el elemento al que se le realiza la réplica, sino a los bits que están contenidos en él y son los bits los que forman el elemento material probatorio, dicho concepto es conocido como todo objeto que evidencie conductas punibles, presentado voluntariamente para lograr determinar un juicio racional en un caso de investigación (Ley 906, 2004).

Los pasos que se deben realizar para analizar la información que se encuentra dentro del medio de almacenamiento, es en primer lugar realizar la copia bit a bit para no trabajar sobre la información contenida en el dispositivo de almacenamiento, adicional a la copia, es recomendable, realizar otra copia bit a bit de la copia, de forma tal que hay una imagen de referencia de la original, hay una réplica y una copia de esta última, que servirá para realizar los procedimientos de análisis (Rojas, 2010, p. 10).

2.2.16 DESAFÍOS

En la aplicabilidad de la Informática Forense en Honduras ya sea como empresa, persona o ente investigativo se presentan varios desafíos, entre los que se puede mencionar los siguientes:

- Desconocimiento de la materia: actualmente el conocimiento que se tiene sobre Informática Forense y la forma de aplicarla es limitado. De igual manera no se cuenta con suficiente conocimiento sobre las herramientas y técnicas que pueden ser aplicadas.
- Complicidad: Existe el riesgo de la complicidad entre personas externas ajenas a la organización y personal interno para dificultar la aplicación de un análisis forense.
- Poca credibilidad: La evidencia digital no siempre cuenta con credibilidad al momento de incriminar al delincuente.
- Marco Legal: La legislación nacional no contempla de forma específica los delitos informáticos por lo que pueden existir vacíos jurídicos, adicional no hay tratados legales internacionales.
- La complejidad de los sistemas
- Desconocimiento por parte de los operadores de justicia.

2.2.17 INFORMÁTICA ANTIFORENSE

Uno de los mayores desafíos con los que se enfrenta el forense al momento de realizar la investigación, es el uso de técnicas anti forenses por parte de los criminales, las cuales permiten ocultar información, por lo que resulta importante que se conozca sobre las mismas para una mejor y más completa investigación (Jeimy José, y otros, 2010).

Harris (2006), plantea la siguiente clasificación para las técnicas anti forenses:

- Destrucción de evidencia

Su finalidad es evitar que la evidencia sea encontrada

- Ocultamiento de evidencia

En este caso no se realiza destrucción la información, únicamente se oculta por lo que no es una técnica altamente segura para el atacante.

- Eliminar fuentes de evidencia

Mediante esta técnica el intruso no crea evidencia, se bloquea cualquier posibilidad de rastro.

- Falsificar evidencia

Consiste en crear falsa evidencia, se inculpa a terceros y de oculta la verdadera identidad del criminal, desviando la atención.

2.3 CONCEPTUALIZACIÓN

2.3.1 INFORMÁTICA FORENSE

Existe un sin número de definiciones para esta rama de la informática también llamada computación forense, a continuación, se detallan algunas:

a. La connotación núcleo del equipo forense se pueden describir de manera concisa como el proceso de identificación, preservar, analizar y presentar la evidencia digital en de una manera que es legalmente aceptable (McKemmish, 1999).

b. El cómputo forense, conocido como una disciplina científica y especializada de las ciencias forenses que tiene como objetivo de descubrir e interpretar, la información que reside en los medios informáticos para reconstruir los hechos y formular teorías relacionadas en la investigación de un caso delictivo (Jeimy J. Cano, Introducción a la Informática Forense - Una disciplina técnico-legal).

c. Para el FBI, es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional (Federal Bureau of Investigation, 2000).

d. Pagès López (2013), afirma que la Informática Forense "es una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica o para la simple investigación privada".

2.3.2 DELITO INFORMÁTICO

El delito informático es definido por la Organización para la Cooperación Económica y el Desarrollo (OCED) como "cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos".

2.3.2.1 Delito Informático versus Delito Informatizado

A simple vista se puede pensar que ambos delitos son lo mismo, sin embargo, existen diferencias entre ambos:

El delito informático según la Real Academia Española (RAE) es "el ilícito penal perteneciente o relativo a la informática, cuando el bien jurídico protegido es la información informatizada, el soporte informático". Mientras que el delito informatizado es la acción de utilizar la informática para cometer delitos (Abog. Rodriguez Barreda, 2009).

2.3.3 PERITO INFORMÁTICO

El perito es el profesional que cuenta con conocimientos en el campo de la informática, y cuyos servicios los utiliza la persona o empresa afectada por un delito informático, de igual manera es utilizado por el juez para el apoyo en el esclarecimiento de un hecho que requiera los conocimientos especiales, científicos y técnicos relacionados a la informática.

El perito informático hace un análisis exhaustivo de los equipos informáticos, y sobre todo de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o brinden indicio acerca de cómo se ejecutó el delito informático investigado (Gómez, 2012).

2.3.4 DERECHO INFORMÁTICO

Es una rama del derecho que consiste en un conjunto de normas y principios que regulan los efectos jurídicos del uso de la informática y las tecnologías de información y comunicación (TIC). De esta manera, las Ciencias Jurídicas analizan los impactos de la informática en todos los ámbitos de la sociedad y estudia los cambios y transformaciones que produce para poder regularlas adecuadamente (Informática Legal, 2016).

2.3.5 CADENA DE CUSTODIA

Olga Aceituno de Parhham, del Consultorio Técnico Criminalístico de Tegucigalpa, Honduras, en su artículo Cadena de Custodia en Honduras refiere a la misma como:

"un procedimiento administrativo y legal de aplicación mundial, que garantiza la correcta recolección, descripción, cuantificación, individualización, embalaje y transferencia de custodia de una evidencia. Esta demuestra y afirma que la evidencia no ha sido objeto de alteración, confusión, contaminación o substracción antes y después de ser analizada", en dicho artículo Aceituno refiere la falta de interés de los encargados de impartir justicia hacia la cadena de custodia, lo que afecta la aplicación correcta de la justicia, ya que no es valorada de la manera más acertada.

En la Norma ISO/IEC 27037 que trata sobre la Normalización de la Práctica Forense, en su apartado número siete refiere las Instancias en la Identificación, recolección, adquisición y preservación de Evidencia Digital, en la norma se mencionan los pasos que deben seguirse para llevar a cabo una adecuada recolección de evidencia y una cadena de custodia que permita la conservación correcta de la misma.

En la legislación nacional mediante el Reglamento sobre el manejo de indicios y evidencias físicas o biológicas obtenidas como consecuencia de la comisión de un hecho constitutivo de delito, hace referencia a la cadena de custodia y su relación con el Código Procesal Penal, ya que este hace mención a las garantías de preservación de evidencia, por lo que el término de "Cadena de Custodia" se sustituye por "Garantía de Autenticidad" el cual se define en dicho Reglamento como "Los procedimientos transparentes y debidamente documentados, a los que se sujeta un indicio localizado en un sitio de un suceso criminal o relacionado con éste, mientras transita por diferentes momentos, lugares, y condiciones, hasta ser presentado legítimamente como elemento de prueba en un juicio penal".

2.3.6 MEDIOS DE PRUEBA DIGITAL

La información almacenada de manera digital o que es transferida y se considera con valor probatorio se conoce como evidencia digital. En textos relacionados con el tema se encuentra una definición que es considerada la más acertada y es la de J. Cano, quien se refiere a evidencia digital como un tipo de evidencia física que se forma por campos magnéticos y pulsos electrónicos que pueden ser recolectados, almacenados y analizados con herramientas y técnicas especiales (Jeimy J. Cano, Introducción a la Informática Forense - Una disciplina técnico-legal).

El medio de prueba digital describe cualquier registro que se genere o almacene en un sistema informático y puede ser considerado como prueba en un proceso legal.

El manual HB: 171 2003 Directrices para la gestión de las pruebas de TI define evidencia digital como, "Cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático."

De igual manera el referido manual divide en tres categorías la evidencia digital:

- Registros que han sido almacenados en el equipo informático.
- Registros que fueron generados por los equipos de tecnología informática
- Registros que han sido generados y almacenados parcialmente en los equipos.

La diferencia entre evidencia física y la digital radica en la fragilidad de la digital y en la capacidad de realizar copias idénticas no autorizadas de documentos sin dejar rastros.

Características de la Evidencia Digital

- Volatilidad: La evidencia volátil es aquella que rápidamente desaparece, por lo que al inicio de la investigación se debe asegurar la misma y adquirirla por orden de volatilidad., Ejemplo: Registros de Cache, memoria.

- Anónima: Se dice que es anónima ya que en algunos casos los sitios web no mencionan autores, por lo que es casi imposible a simple vista saber el origen.

- Se puede duplicar de manera exacta: La evidencia se puede reproducir fácilmente de manera exacta, lo cual beneficia la investigación sin poner en riesgo la evidencia original.

- Puede ser alterada y modificada o eliminada: La evidencia digital al no conservarse adecuadamente mediante la cadena de custodia, es fácilmente alterada o modificada, pudiendo ser hasta eliminada, con el fin de ocultar información o de alterar algún resultado que perjudique o beneficie al imputado. También por tener esta característica es

necesario que al momento de realizar el análisis se haga en base a una imagen o copia exacta de los datos, para así evitar posibles daños a la información.

Para que la evidencia digital sea admisible, debe probarse su autenticidad y confiabilidad, además debe ser suficiente para probar el hecho delictivo y deberá estar acorde a las leyes judiciales que rigen en el país.

2.3.7 INFORME PERICIAL

Es la presentación de los resultados de la pericia realizada, los mismos son presentados de forma adecuada para que sean comprendidos e interpretados por personas no especialistas en la materia (Darahuge & Arellano González, 2011).

Debe ser presentado con una estructura criminalista que cubra con todos los requerimientos legales que permita sea aceptado como prueba y presentando los resultados relevantes de la investigación y de forma concluyente.

2.4 MARCO LEGAL

2.4.1 NORMAS INTERNACIONALES O MEJORES PRÁCTICAS PARA LA APLICACIÓN DE LA INFORMÁTICA FORENSE

Luego de años en los que se ha aplicado una serie de metodologías en la Informática Forense, diversas organizaciones a nivel mundial han establecido normas, estándares, guías y mejores prácticas para lograr una estandarización de la aplicación en investigaciones de la Informática Forense, a continuación, se presenta una recapitulación sobre ellas:

a. ISO/IEC 27037:2012 Guía para la Identificación, recolección, adquisición y preservación de evidencia digital.

La finalidad de esta norma es proporcionar directrices para aquellas actividades específicas de manejo de la evidencia digital, las cuales incluye la identificación, recolección, consolidación y preservación de aquella evidencia digital que pueda ser considerada como medio de prueba. Mediante esta norma internacional se orienta a las personas en relación a situaciones comunes

que se encuentran en el proceso del tratamiento de las pruebas digitales y ayuda a las organizaciones en sus procedimientos disciplinarios, de igual manera facilita que la información sea intercambiada como prueba digital.

Principios básicos en los que se basa la norma:

- Aplicación de Métodos
- Proceso Auditable
- Proceso Reproducible
- Proceso Defendible
- La identificación
- La recolección y/o adquisición
- La conservación/preservación (ISO, 2012).

b. ISO/IEC 27042:2015 Guía para el análisis e interpretación de la evidencia digital.

Esta Norma Internacional proporciona orientación sobre el análisis e interpretación de las pruebas digitales de una manera que se ocupa de cuestiones de continuidad, validez, reproducibilidad y repetitividad. Se encapsulan las mejores prácticas para la selección, el diseño y la implementación de los procesos de análisis y registro de la información suficiente para permitir que estos procesos sean sometidos a un control independiente cuando sea necesario. Se proporciona orientación sobre los mecanismos apropiados para demostrar la aptitud y la competencia del equipo de investigación.

Además, proporciona un marco común, para los elementos de análisis y de interpretación de manejo de incidentes de seguridad de sistemas de información, que pueden ser utilizados para ayudar en la aplicación de nuevos métodos y proporcionar un estándar común mínimo para las pruebas digitales producidos a partir de tales actividades (ISO, 2015).

c. RFC 3727 Guía para recolectar y archivar evidencia

Esta guía brinda a los administradores de los sistemas las directrices para recopilar y archivar datos obtenidos de las pruebas correspondientes a un incidente de seguridad o intrusiones que afecten la información de manera financiera, imagen o económica. Detalla claramente cómo se debe determinar la volatilidad de los datos, lo que se debe recolectar, el desarrollo de la recolección, lo que se debe almacenar, cómo documentar los datos y cómo manejar la parte legal (RFC 3727, 2002).

d. Red Europea de Institutos de Ciencias Forenses (ENFSI, por sus siglas en inglés) Manual de mejores prácticas en examen forense de tecnología digital.

Este Manual de Mejores Prácticas está dirigido a expertos en la materia y que tienen un conocimiento previo en la disciplina. No es un procedimiento operativo estándar, sino que aborda los requisitos de los sistemas judiciales en términos generales.

Este documento se centra principalmente en las mejores prácticas en el campo de la Tecnología de la Información de la ciencia forense de computadoras y telefonía.

Este manual contiene recomendaciones generales que están contenidos dentro del documento completo y permite a que los laboratorios ENFSI tengan la flexibilidad para diseñar e implementar sus propios procesos en función de sus necesidades nacionales individuales relativas a los procedimientos de laboratorio, el personal, equipo y servidores (ENFSI, 2015).

e. Grupo de Trabajo Científico en Evidencia Digital (SWGDE, por sus siglas en inglés) - Mejores Prácticas para la Informática Forense

Este documento proporciona información básica sobre la adquisición lógica y física de las computadoras y sus medios de almacenamiento asociados. Está dirigido a los examinadores en un entorno de laboratorio y el personal que recogen la evidencia digital en el campo. Este documento no está destinado a ser utilizado como un paso o una guía detallada para la realización

de una adecuada investigación forense en componentes tecnológicos ni debe interpretarse como asesoramiento legal (SWGDE, 2013).

f. Asociación de Jefes de Policía (ACPO, por sus siglas en inglés) - Guía de buena práctica para la evidencia digital.

Esta guía de buenas prácticas ha sido creada por el Área de Negocios de Delito de la ACPO y fue aprobado originalmente por el Consejo de Ministros de la ACPO en diciembre de 2007. El propósito de este documento es proporcionar una guía no sólo para ayudar a la policía, sino para ayudar a todos aquellos que realizan investigación de los incidentes de seguridad cibernética y crimen. Será actualizado de acuerdo a los cambios legislativos y políticos y re- publicado como sea necesario (ACPO, 2014).

g. Sociedad de Seguridad de la Información y Forense (ISFS, por sus siglas en inglés) - Computación Forense - Parte 2: Mejores Prácticas

En este documento se plasman procedimientos y otros requisitos participantes en todo el proceso forense de la evidencia digital, a partir de las evaluaciones realizadas en la escena del hecho criminal hasta la elaboración del informe que se presentará ante la corte. También proporciona explicaciones de por qué se llevan a cabo ciertos procedimientos y brinda detalles a nivel técnico de la informática forense.

Está escrito de una manera tal que sea lo más neutral tanto de forma tecnológica como jurisdiccionalmente posible, aunque esté escrito pensando en los lectores de Hong Kong. Sin embargo, los lectores deben tener en cuenta que:

- La legislación varía de un país a otro. Por lo tanto, los profesionales de las investigaciones en múltiples jurisdicciones legales tienen que determinar los requisitos legales de las jurisdicciones que están operando (especialmente en las leyes que se refieren a la recolección y protección de pruebas, la cadena de custodia, y suficiencia de las pruebas para el enjuiciamiento) y poner en práctica los procedimientos necesarios para cumplir con los requisitos.

- Los especialistas deben tener en cuenta las variaciones en los sistemas operativos, aplicaciones, etc., así como sistema de configuraciones en la realización de exámenes forenses y que ningún conjunto de directrices puede aplicarse a todas las situaciones posibles y contingencias.

- Este documento no pretende ofrecer asesoramiento legal. Por cuestiones legales, el ISFS recomienda que los lectores busquen un asesor jurídico calificado y adecuado en la jurisdicción correspondiente (ISFS, 2009).

h. Servicio de Referencia Nacional de Justicia Criminal (NCJRS, por sus siglas en inglés) - Investigación en la escena del crimen electrónico: Una guía para el primero en responder.

Esta guía está destinada a ayudar a los Estados, a la aplicación de leyes locales y otros investigadores que pueden ser responsables de la preservación de la escena del crimen electrónico y el reconocimiento, recopilación, y protección de la evidencia digital. No todas las situaciones están incluidas sin embargo aquella evidencia digital que se puede encontrar en la escena del delito será considerada.

Todas las escenas del crimen y el juicio del primer nivel de respuesta son únicas, los protocolos de la agencia, y la tecnología prevaleciente deben ser considerados al aplicar la información de esta guía. Los primeros en responder a la escena de los crímenes electrónicos deben ajustar sus prácticas como las circunstancias, incluyendo el nivel de experiencia, condiciones y disposición de equipo de orden. Las circunstancias de cada escena del crimen y federales, estatales, y las leyes locales pueden dictar actos o un orden determinado de acciones distintas de las descritas en esta guía. Los primeros en responder deben estar familiarizados con toda la información en esta guía y llevar a cabo sus funciones y responsabilidades según dicten las circunstancias (OJP, 2009).

i. Servicio de Referencia Nacional de Justicia Criminal (NCJRS, por sus siglas en inglés) - Examen Forense de la Evidencia Digital: Una guía para la aplicación de la ley.

La guía NCJRS está considerada para su uso de oficiales de la ley y otros miembros de la comunidad de las leyes responsables del examen de la evidencia digital.

NCJRS es una guía que trata de situaciones habituales que pueden surgir durante el examen de la evidencia digital. No es un mandato para que la comunidad aplique la ley; es una base que se puede utilizar para ayudar a desarrollar sus propias políticas y procedimientos. La tecnología avanza a un ritmo tan rápido que las sugerencias de esta guía se examinan mejor en el contexto de la tecnología y las prácticas actuales. Cada caso es único y el juicio del examinador debe dar deferencia en la aplicación de los procedimientos sugeridos en esta guía. Las circunstancias de cada caso y las leyes federales, de Estados Unidos y en cuanto puedan aplicarse localmente en Honduras, también pueden requerir acciones distintas de las descritas en esta guía (NCJRS, 2004).

2.4.2 LEGISLACIÓN NACIONAL

En la actualidad el país no cuenta con legislación que permita investigar y judicializar delitos informáticos como tales. Sin embargo, se están realizando esfuerzos por cubrir este vacío jurídico mediante la aprobación de un nuevo código penal en el cual se contemplan este tipo de delitos, dicho código se encuentra como anteproyecto de ley en el Congreso Nacional.

A continuación, se detallan los artículos de los diferentes códigos vigentes y que pueden ser aplicados en aquellos casos de delitos informáticos:

2.4.2.1 Código Penal

El Artículo 214, en su capítulo VII hace referencia a la VIOLACIÓN Y REVELACIÓN DE SECRETOS y reza lo siguiente: “Quien, sin la debida autorización judicial, con cualquier propósito, se apodere de los papeles o correspondencia de otros, intercepta o hace interceptar sus comunicaciones telefónicas, telegráficas, soportes electrónicos o computadoras, facsimilares o de cualquier otra naturaleza, incluyendo las electrónicas”.

Este artículo se debe considerar por la importancia que tiene conocer que antes de realizar cualquier tipo de recolección de medios de prueba se debe contar con la debida autorización judicial para evitar cometer delito.

Artículo 240 y 242 hacen referencia a quienes cometen los delitos de estafa y otros fraudes, delitos que se pueden ejecutar utilizando sistemas informáticos o sistemas de información, medios o equipos de telecomunicaciones, piratería informática, reventa no autorizada o clonación de números móviles y sus sanciones.

Artículo 241 hace referencia a las sanciones que serán aplicadas en caso de los delitos mencionados en los artículos 240 y 242.

Capítulo 9 Artículo 254 bajo el contexto del artículo 254 se podrá judicializar aquellos casos donde se dañe o destruya información de sistemas informáticos o redes.

En estos artículos se enmarcan delitos considerados delitos informáticos, por lo que al momento de realizar investigaciones relacionadas con éstos, se debe considerar dichos artículos para dar peso a la misma (Decreto 144-83 Código Penal, 2006).

2.4.2.2 Código Procesal Civil

El Artículo 279 hace referencia a la validez legal que un soporte informático tiene en relación a la contabilidad, por lo que puede ser considerado soporte de los libros contables.

En el Artículo 280, numeral 5, se menciona la fuerza probatoria de los documentos electrónico, indica que la forma de proceder cuando se solicite la eficacia o se impugne la autenticidad de un documento electrónico, será en base a lo previsto en esta y otras leyes.

La sección cinco se refiere a temas de Propiedad Intelectual y en Artículo 532, numeral 2, inciso d, se refiere a ordenar el cese de la actividad ilícita que violenta la propiedad intelectual, ordenando la destrucción de elementos que facilitan la reproducción no autorizada de un programa de computadora.

En el Libro Tercero del Código, capítulo II, en el artículo 361 hace referencia a las medidas cautelares y el embargo preventivo, e indica que el embargo puede recaer sobre bienes informáticos, y en caso de un embargo se tendrá derecho a que la información existente en los medios de almacenamiento sea retirada (Decreto No. 211-2006 Código Procesal Civil , 2007).

2.4.2.3 Código Procesal Penal

El artículo 223 refiere a la legalidad de la intervención de las comunicaciones, y la potestad que tiene el Juez de solicitar la grabación de comunicaciones telefónicas, informáticas o de cualquier índole y que esté relacionada con el delito investigado.

En caso de intervención se deberá identificar y registrar su origen, destinatario o ambos, así como el registro de su contenido (Decreto No. 9-99-E Código Procesal Penal, 2002),de igual manera en caso de una intervención deberá tomar en consideración el artículo 100 de la Constitución de la República de Honduras, que refiere el derecho a la inviolabilidad y al secreto de las comunicaciones que toda persona tiene, por lo que su intervención será únicamente por resolución judicial (artículo 100, Constitución de la República de Honduras, Decreto N° 131del 11 de enero 1982).

CAPÍTULO III. METODOLOGÍA

En este capítulo se encuentra la descripción de la metodología que será utilizada durante el proceso de investigación, detallando los métodos e instrumentos utilizados en el caso de la Informática Forense a fin de dar respuesta al problema planteado.

3.1 COHERENCIA METODOLÓGICA

La congruencia metodológica plasmada en la Tabla 4, permite ver la forma en la que interactúan las variables dependientes e independientes con los objetivos que se busca cubrir en la investigación. De igual manera se observa cómo el problema planteado deriva en una serie de preguntas de investigación que contribuyen a guiar a guiar a la misma y que a su vez se relacionan con los objetivos planteados.

Tabla 4 Coherencia Metodológica

TÍTULO	PROBLEMA	PREGUNTAS DE INVESTIGACIÓN	OBJETIVOS		VARIABLES	
			GENERAL	ESPECÍFICO	INDEPENDIENTE	DEPENDIENTE
Factores que afectan la adecuada aplicación de la informática forense en hechos delictivos.	¿Qué factores afectan la adecuada aplicación de la informática forense en hechos delictivos que involucran componentes tecnológicos en la ciudad de Tegucigalpa?	¿Qué recursos son necesarios para realizar una auditoría forense?	Determinar los factores que afectan la adecuada aplicación de la informática forense en hechos delictivos que involucran componentes tecnológicos	Identificar los recursos necesarios para llevar a cabo una auditoría de informática forense.	Herramientas de informática forense Recurso humano	Cantidad de Casos Resueltos
		¿Qué otras materias tienen relación con la informática forense?		Investigar las ramas y/o materias que están relacionadas al momento de aplicar informática forense en casos delictivos.	Derecho, Contabilidad, Finanzas, Especialistas en Computación Seguridad de Información Redes	Aplicación de teorías de ramas relacionadas

Continuación de la Tabla 4						
TÍTULO	PROBLEMA	PREGUNTAS DE INVESTIGACIÓN	OBJETIVOS		VARIABLES	
			GENERAL	ESPECÍFICO	INDEPENDIENTE	DEPENDIENTE
		¿Existen normas que regulen la aplicación y ejecución de la informática forense?		Describir las normas, estándares, mejores prácticas y guías relacionadas a la aplicación y ejecución de casos delictivos que involucran evidencia digital.	Normas Procedimientos para Resolver delitos informáticos	Cumplimiento de Controles de Seguridad
		¿Cuál es el entrenamiento necesario para convertirse en auditor de informática forense?		Dar a conocer los atributos, capacidades, habilidades y/o conocimientos que se requiere para convertirse en un auditor de la informática forense.	Seguridad de Información Conocimiento en Redes Leyes Herramientas de Informática Forense	Capacidad para resolver delitos que involucran dispositivos tecnológicos

3.2 DEFINICIÓN DE VARIABLES

Tabla 5. Definición de Variables

VARIABLE	DEFINICIÓN	INDICADORES
Factores involucrados en la aplicación de la informática forense	Factores que directa o indirectamente influyen en el desarrollo de una auditoría basada en informática forense.	• Tipo de delito • Forma del delito • Capacitación del investigador • Herramientas tecnológicas para realizar la investigación. • Falta de tecnología especializada en la informática forense • Recurso humano no calificado • Falta de conocimiento de las entidades en los procedimientos a seguir para la aplicación de la informática forense. • Alto índice de delitos Informáticos impunes o no reportados

Continuación de la Tabla 5		
VARIABLE	DEFINICIÓN	INDICADORES
Características y habilidades de un auditor forense informático	Conjunto de características y habilidades mínimas que un auditor debe tener para realizar con buen suceso una investigación.	• Características de un auditor • Habilidades propias de un informático forense.
Conocimientos académicos y técnicos que debe tener un auditor forense informático	Currículo adecuado para el personal que lleva a cabo la aplicación de la informática forense	• Estudios académicos • Preparación especializada • Capacitaciones
Ciencias y/o ramas relacionadas con informática forense	Grupo de profesionales que dan apoyo al especialista forense para obtener un mejor resultado de la investigación.	• Especialistas necesarios según el tipo de delito
Recursos necesarios para realizar una investigación forense en delitos informáticos	Unión de recursos necesarios para llevar a cabo una auditoria forense informática.	• Técnicos • Herramientas • Equipo • Financiero • Personal • Información
Entes y/o personas encargadas de realizar investigaciones delictivas.	Entidades o profesionales encargados de realizar las investigaciones y juzgar los casos que se presentan.	• Profesionales independientes • Entes de Investigación • Policía • Ministerio Público, Fiscalías
Normas y legislación nacional e internacional	Normativa legal nacional aplicable en caso de delitos, y guía de buenas prácticas internacionales.	• Leyes nacionales que hagan referencia a delitos informáticos. • Normas o guías internacionales de buenas prácticas

3.3 ENFOQUE Y MÉTODOS

Durante la investigación se utilizará un enfoque mixto, debido al uso de herramientas de recolección de datos cuantitativos y cualitativos como ser las encuestas y entrevistas (no serán tabuladas, ni cuantificadas) respectivamente, que permite conocer las fortalezas y debilidades en la aplicación de la informática forense en Tegucigalpa.

Se utilizará además el método deductivo, debido a que se cuentan con premisas sobre los factores que intervienen y afectan la informática forense, y se busca a través de la investigación dar respuesta a estas premisas y al problema planteado (Roberto Hernández Sampieri, 2014).

3.4 TIPO DE INVESTIGACIÓN

La investigación se enmarca en un alcance exploratorio en Honduras, específicamente en la zona de Tegucigalpa, ya que nos centraremos en investigar un tema del cual no se cuenta con mucha documentación nacional y referencias de anteriores investigaciones.

3.5 DISEÑO DE LA INVESTIGACIÓN

El estudio se realizó bajo el esquema de un diseño No Experimental-Transeccional correlacional, debido a que se realizó una investigación sin manipulación de variables de manera deliberadas y en situaciones ya existentes; transeccional pues la investigación se centró en analizar las diferentes variables y su estado actual, adicionalmente la recolección de datos se realizó una vez. El diseño de la investigación es correlacional ya que se busca describir la relación que existe entre las variables estudiadas (Gomez, 2001).

Sampieri, Roberto & Baptista, describen este diseño como "El que recolecta datos en un solo momento, en un tiempo único y su propósito es describir variables y analizar su incidencia e interrelación en un momento dado".

El diseño de la investigación contempla los siguientes pasos:

a. Definición del problema de investigación: En esta etapa se realiza la definición de objetivos, alcance y se expone el porqué del estudio a realizar.

b. Elaboración del Marco Teórico: Se presenta la información soporte para dar respuesta al problema planteado.

c. Metodología: Se determina la metodología a seguir en la investigación, que incluye definición de enfoque, instrumentos, muestra a la cual se le aplicarán las técnicas de recolección de datos, entre otros.

d. Análisis de Datos: Se realiza el análisis de los datos obtenidos en la recolección de datos.

e. Conclusiones - Recomendaciones: Recomendaciones realizadas en base al análisis realizado.

3.6 POBLACIÓN Y MUESTRA

La población a considerar para el levantamiento de datos son profesionales de Informática y Derecho que laboran en el sector privado y público, entes encargados de investigación y justicia del país, así como la Docencia del área de Informática en la educación superior, en la ciudad de Tegucigalpa.

Para determinar el tamaño de la muestra no se plantea un cálculo, debido a que no se conoce la población total que forman parte de los diferentes universos considerados, adicional en algunos casos el acceso a la población es limitada, por lo que se realizará un muestreo de o por conveniencia, el cual consiste en "un grupo de sujetos seleccionados sobre la base de ser accesibles o adecuados" (McMillan & Schumacher, 2005). La muestra se tomará según el personal al que se tenga acceso o que se nos permita realizar la encuesta que corresponda.

Realizando un muestreo de o por conveniencia existe el riesgo de no obtener una muestra mayor del universo, lo cual no significa que los resultados no puedan ser concluyentes en cuanto los profesionales de tecnología, derecho y docencia, sin embargo, en el caso de los entes encargados pudiere existir el riesgo de no obtener toda la información requerida para el estudio.

3.7 TÉCNICAS E INSTRUMENTOS APLICADOS

3.7.1 TÉCNICAS APLICADAS

Para llevar a cabo el enfoque mixto que fue definido previamente se requirió el uso de técnicas de medición relacionados con las variables para un análisis posterior, orientados a determinar los factores de mayor influencia en la aplicación de la informática forense.

3.7.2 INSTRUMENTOS APLICADOS

En nuestra investigación se emplearon los instrumentos de encuesta y entrevista. Esta elección de instrumentos se debe a que permiten obtener la información requerida para el estudio, de una forma clara y precisa.

Las encuestas permiten la recolección de información de una manera práctica, debido a su forma de aplicación, lo cual facilita la recolección de datos con personas que no cuentan con mucho tiempo disponible o desean mantener su identidad en privado.

Las entrevistas facilitan indagar sobre la materia con personal que tienen un alto conocimiento de la materia o que están relacionadas con la misma.

3.7.3 ENCUESTA

La encuesta se aplicó a los profesionales de informática, con el fin de conocer el grado de conocimiento sobre informática forense, al igual que a los profesionales del derecho, y personal de las agencias de investigación y Ministerio Público.Igualmente se realizó la aplicación de encuestas a personas no relacionadas con el área de sistemas o derecho, con el fin de obtener resultados sobre el nivel de conocimiento que la población en general tiene sobre informática forense y derecho informático, de igual manera si este sector de la población han sido víctimas de algún hecho que requiera el uso de la investigación forense.

3.7.4 ENTREVISTA

Esta está orientada a los entes judiciales y gerentes de TI. Se realizarán encuestas en base a preguntas relacionadas al tema investigado y la información que se busca obtener.

3.8 PROCEDIMIENTOS

3.8.1 ENCUESTAS

Se realizó la aplicación de encuestas con respuestas cerradas, buscando con ello la obtención de datos concretos sobre el tema investigado.

Objetivos de las encuestas:

- Conocer sobre los factores que afectan la aplicación de la informática forense
- Identificar el grado de preparación académica y técnica del personal que realiza las auditorías forenses.
- Determinar la necesidad de capacitación del personal involucrado en las investigaciones.
- Establecer el nivel de conocimiento de informática forense que los profesionales de informática y derecho tienen.

Las encuestas serán entregadas al encuestado quien las completará sin intervención del investigador, una vez obtenida la información se procederá a realizar la tabulación y procesamiento de los datos obtenidos.

3.8.2 ENTREVISTAS

Orientadas a conocer el grado de conocimiento y aplicación de la informática forense, tanto en las empresas privadas, públicas y en los entes de investigación.

3.9 FUENTES

3.9.1 FUENTES PRIMARIAS

Las fuentes de información primaria será la recolección de información por medio de la aplicación de instrumentos de recolección de datos.

3.9.2 FUENTES SECUNDARIAS

Dentro de las fuentes secundarias se dispone de artículos científicos, informes, libros, tesis, documentos, entre otras.

3.10 INSTRUMENTOS PARA LA RECOLECCIÓN DE DATOS

El instrumento que se seleccione para la medición debe ser el adecuado para el registro de los datos, que represente las variables que el investigador definió previamente y genere información válida.

Por esta razón se necesita que el instrumento seleccionado sea confiable y permita medir lo que se desea en la investigación, de igual forma debe conceptualizar las ideas y conceptos debidamente clasificados y representados, buscando con ellos que cualquier persona que tenga acceso a los resultados los entienda.

Partiendo de esto se puede decir que la conceptualización es el proceso por medio del cual se va de la idea a la investigación y la medición es cuando se lleva a la matemática lo planteado en la conceptualización; la representatividad se refiere a la relación entre los resultados generados por la muestra, son atribuidos a la generalidad de la población.

Por las razones expuestas se decide aplicar los siguientes instrumentos:

- Entrevista
- Encuesta

Para seleccionar los instrumentos se tomó en consideración las ventajas y desventajas de ambos.

Ventajas de la encuesta:

- Al utilizar respuestas cerradas se obtiene la información clara y específica de lo que deseamos conocer.
- Mayor cantidad de muestra poblacional abarcada
- Estandarización de datos, que facilita el análisis de la información.
- Genera resultados con mayor precisión
- Obtención de datos secundarios

Desventajas de la encuesta:

- Preguntas cerradas/limitadas que no permite consultar más que lo plasmado en la misma, en caso de presentarse esta situación y que se observe que el encuestado puede brindar más información que contribuya a la investigación el encuestador debe solicitarle una cita para realizar una entrevista.

- Información obtenida que es condicionada a las preguntas y respuesta plasmadas, en ocasiones brindando opciones al entrevistado que no representen su opinión, por lo que es necesario se pueda detectar esta situación y en caso de considerarlo permitirle al encuestado brinde la respuesta que considere correcta.

- Pueden ser poco objetivas, cuando al momento de aplicarlas el encuestado tenga un cambio de humor o se sienta presionado por la presencia del encuestador, razón por la cual el encuestador debe ser sutil al momento de abordar el posible encuestado para detectar si es el momento adecuado para aplicar la encuesta y de igual manera debe respetar el espacio del encuestado siempre pendiente para detectar las situaciones planteadas anteriormente.

Ventajas de entrevista:

- Se realizan preguntas con flexibilidad dependiendo de quién sea el entrevistado.
- El entrevistador puede preguntar sobre temas que vayan surgiendo durante la entrevista.
- Se obtienen datos relevantes y significativos, así como mayor cantidad de información.

Desventajas entrevistas

- Respuestas dadas por el entrevistado no acorde a las preguntas o que no satisfagan el interés del entrevistador, por lo que debe indagarse y profundizar la entrevista y de ser necesario reformular la pregunta de manera que se obtenga la información esperada.

- Análisis de la información con interpretación compleja dado los resultados obtenidos, razón por la cual se debe establecer parámetros para el tipo de información que se busca recabar y guiar la entrevista bajo esos lineamientos

- Información recolectada no necesaria, esto debido a que la entrevista se puede desviar del tema principal o el entrevistado puede buscar evadir la pregunta brindando otro tipo de

respuesta, por lo que se debe mantener la línea de la entrevista y no permitir desvíos o distracciones en la misma.

- Debe existir habilidad de comunicación y conocimiento del tema por parte del entrevistador para obtener la información deseada, por lo que es necesario tener conocimientos fuertes acerca del tema a tratar en la entrevista, mostrar seguridad y mantener una comunicación fluida con la entrevista, permitiendo con esto mejores resultados.

3.11 LIMITANTES

La principal limitante fue la obtención de información de parte de los entes de investigación y judicialización, ya que al ser un tema relacionado con seguridad y la forma de operar de los entes encargados de la justicia se maneja con mucha reserva por parte de los empleados que laboran en la misma.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En el capítulo cuarto se presentan los resultados adquiridos mediante las investigaciones realizadas y la aplicación de instrumentos en los entes de investigación, profesionales del área de sistemas y derecho, en los centros de educación y población en general. El análisis efectuado tiene como finalidad poder presentar posteriormente recomendaciones que contribuyan a una mejor aplicación de la informática forense en la investigación de delitos informáticos.

4.1 RESULTADOS Y ANÁLISIS DE ENTREVISTAS

4.1.1 ENTREVISTAS A ENTES DE INVESTIGACIÓN

Una vez finalizadas las entrevistas en los entes de investigación siguientes:

1. Ministerio Público (MP)
2. Dirección Nacional de Investigación e Inteligencia (DNII)
3. Agencia Técnica de Investigación Criminal (ATIC) y
4. Dirección Policial de Investigación (DPI).

Se obtuvo información sobre la situación actual de los mismos, y los esfuerzos que realizan por contar con las herramientas y personal capacitado necesario para llevar a cabo las investigaciones, igualmente el efecto que tiene al momento de investigar un hecho, el criterio del Fiscal, ya que es quién define si en un hecho será necesario realizar investigación forense informática.

En entrevista realizada a personal con conocimientos avanzados en el tema de las investigaciones sobre casos delictivos que involucran tecnología y que pertenece a la Policía Nacional de Honduras, se obtuvo información sobre el estado actual del proceso de las investigaciones que se realizan a aquellos delitos informáticos o delitos realizados a través del uso de la informática y la aplicación de la Informática Forense en los mismos. Entre los puntos relevantes derivados de la entrevista se encuentran los siguientes:

- Los operadores de Justicia del país son los siguientes:

    - Corte Suprema de Justicia
    - Ministerio Público
    - Órganos Policiales
        - Dirección Nacional de Investigación e Inteligencia
        - Policía Militar de Orden Público
        - Policía Nacional

- La policía cuenta con una unidad especializada en delitos informáticos.
- Las escenas donde se realiza levantamiento de evidencia se llama “Escena del suceso”.
- Se cuenta con información estadística mínima.
- Actualmente se está implementando un laboratorio de rasgos biométricos para realizar peritajes informáticos. El personal que estará laborando en dicho laboratorio, está siendo capacitado en el extranjero con los temas relaciones a rasgos biométricos.
- En las investigaciones se utiliza la herramienta de hardware y software “Cellebrite” para realizar descargas de datos de dispositivos móviles con sistema operativo Android.
- Existe falta de comunicación entre las instituciones de seguridad del gobierno (Policía Nacional y Policía Militar) al momento de realizar el levantamiento del proceso.
- La comunicación del policía es con el Fiscal asignado al caso.
- El Sub Comisionado Aguilar es miembro de la Asociación de Ciber Policías (Iberpol)
- Los delitos informáticos o aquellos delitos que involucran tecnología, son considerados delitos atípicos que es lo equivalente a delitos no convencionales y son investigados bajo una investigación forense no formal, basándose en normas atípicas ya que no existe una ley escrita específica para estos delitos.
- Los delitos que involucran tecnología no son clasificados como tal, sino que se incluyen en las estadísticas de las fiscalías de delitos comunes y en las fiscalías de delitos financieros, de igual manera en la Corte Suprema de Justicia se encuentran los archivos de los delitos informáticos, pero no se encuentran clasificados como tales.

- Durante el proceso de investigación y juzgamiento definido en el artículo 263 del código procesal penal, se realiza la investigación forense, específicamente en la etapa preparatoria.

  ARTÍCULO 263.- Etapas de la Investigación y del Juzgamiento. El proceso de investigación y juzgamiento de los delitos constatará de las fases siguientes: 1) Etapa preparatoria; 2) Etapa intermedia; y, 3) Debate o Juicio Oral y Público.

- El proceso investigativo en etapa preparatoria se inicia con la denuncia del hecho criminal según lo establecido en el artículo 267.

  "ARTÍCULO 267.- Denuncia del Hecho Criminal. La etapa preparatoria del juicio se iniciará con la denuncia del hecho criminal ante la Policía Nacional o el Ministerio Público, o con las informaciones que se hayan recibido del mismo, sin perjuicio de la acción del Acusador Privado, del Estado y sus entes."
- Aclaración términos, el "Delito Informático" es el delito y la "Informática Forense" es la pericia que el investigador debe tener.
- Existe una brecha tecnológica en el personal
- Se ha presentado situaciones en las que la custodia o evidencia no se protege de la manera correcta, ejemplo: manipulación de aparato telefónico.
- A criterio del Sub Comisionado entre los retos que se tienen se puede mencionar los siguientes:
  - Falta de Marco Legal, la legislación actual obliga a encasillar el delito
  - Bajo nivel de conciencia
  - Capacitación
  - Investigación forense no formal
    - Limitantes en metodología
    - Recursos inadecuados o inexistentes
    - No existe laboratorio
    - Falta de conocimientos de las fuentes de indicios
    - Esfuerzos dirigidos para tapar hueco
    - No hay procedimientos dentro de las organizaciones para responsabilizarse de los casos.

También, se estableció comunicación con personal de la Dirección de Policía de Investigación (DPI) vía teléfono e informó que las capacitaciones recibidas han sido en el extranjero (en el país China), en estas capacitaciones se incluyó al personal que realiza las investigaciones de delitos incluyendo los informáticos.

De igual manera, en entrevista realizada a personal de la Dirección Nacional de Investigación e Inteligencia (DNII), se obtuvo información relacionada con las tareas llevadas a cabo en las DNII, los puntos dados son los siguientes:

- En la DNII realizan investigaciones utilizando la informática forense y cuentan con herramientas para realizar dichas investigaciones, sin embargo, las mismas son más orientada a los dispositivos móviles (celulares).
- No se cuenta con suficiente equipo para extracción de información.
- Al perito se le certifica en el uso de la herramienta que utiliza, para que de esta forma sepa que información está obteniendo de los equipos/aparatos investigados.
- En el juzgado al perito lo avala la certificación del uso de la herramienta y la experiencia.
- Laboratorios de forense en la DNII no hay.
- Los peritos no cuentan con estudios en el área de sistemas.
- Software utilizado XRY.
- No siempre la cadena de custodia se realiza de manera correcta.

Además, se realizó entrevista a personal de la DPI-Interpol, quien ha sido capacitado en temas relacionados con la investigación forense del campo informático. El entrevistado brindo algunos detalles acerca de la situación actual en la DPI con respecto a dicha investigación. A continuación, los puntos mencionados:

- En la policía actualmente no hay una oficina específica, se está en proceso de creación de la Unidad de delitos tecnológicos.
- No se cuenta con preparación para los policías asignados.
- Los técnicos la mayoría son policías que actualmente cursan la carrera de sistemas, pero no todos los que realizan investigaciones tienen conocimientos sobre sistemas.

- Se cuenta con herramientas que permiten realizar análisis de dispositivos, verificar el hash de un medio de prueba digital y herramientas para el análisis de casos y capturadores de imágenes.

El contacto del ente de investigación ATIC, comentó algunos puntos relacionados con las investigaciones que realizan:

- Se cuenta con equipo (personal y herramientas) para realizar las investigaciones.
- Investigar un hecho delictivo depende de los requerimientos del Fiscal, en ocasiones se presentan delitos que involucran componentes tecnológicos, sin embargo, los fiscales no siempre consideran necesario realizar las investigaciones forenses informáticas.
- Los delitos informáticos son tratados bajo denominaciones distintas, como consecuencia de no contar con una ley que los estipule.

4.1.2 ENTREVISTA A OPERADORES DE JUSTICIA

El Ministerio Público (a través de las diferentes Fiscalía), es el órgano encargado de ordenar las investigaciones y definir el tipo de delito a investigar. Por lo que se procedió a entrevistar a personal que labora en dicha institución, se logró obtener la siguiente información:

- Las investigaciones de delitos no se hacen uso de todas las herramientas que deberían ser aplicadas para obtener resultados acertados y concretos.
- En las Fiscalías no se tiene amplio conocimiento sobre temas de delitos informáticos y/o informática forense.

4.1.3 ENTREVISTAS A PERSONAL CLAVE EN UNIVERSIDADES

En las visitas realizadas a los departamentos de Sistemas y Derecho de la Universidad Nacional Autónoma de Honduras, Universidad Tecnológica de Honduras y Universidad Católica de Honduras, se pudo constatar que en el pensum académico no se cuenta con asignaturas de derecho informático o informática forense.

- Universidad Autónoma de Honduras (UNAH)

Se llevó a cabo una reunión con la Lic. Sandra Velásquez Jefe del Departamento de la carrera de Informática en la Universidad Autónoma de Honduras (UNAH), quien indicó que en el plan de estudios actual se tiene incluida la clase Auditoría Informática, sin embargo, los temas de Delitos Informáticos e Informática Forense no son contenidos dentro del plan de la clase.

- Universidad Católica de Honduras (UNICAH)

Se realizó una reunión con la Ing. Victoria Alejandra Patiño Decana de la Facultad de Ciencias de la Computación de la Universidad Católica de Honduras (UNICAH), quien explicó que en el plan de estudios actual para la carrera de Ingeniería en Ciencias de la Computación se tiene incluida la clase "Auditoría de Sistemas de la Información", sin embargo los temas de Delitos Informáticos e Informática Forense no son incluidos dentro de la clase.

- Universidad Tecnológica de Honduras (UTH)

En reunión con el Ing. Alberto Martínez en ausencia de la Lic. Marina Castellanos, Directora de Computación y Electrónica de la UTH, el catedrático compartió el plan de estudios de la carrera Ingeniería en Computación e indico que dentro del plan se cursa la clase "Auditoria y Seguridad de Sistemas" pero los temas de Delitos Informáticos e Informática Forense no son estudiados en la clase.

4.1.4 CENTROS DE CAPACITACIÓN

En el centro de capacitación New Horizons, especialistas en capacitaciones informáticas, cuentan con cursos relacionados con forense digital y de red, por lo que se realizó comunicación vía correo electrónico con la Lic. Ibeth Castillo, quien es Gerente de Cuentas, en el centro de capacitación. Se consultó sobre los cursos de capacitación que tiene en su oferta académica, obteniendo respuesta positiva.

A continuación, se detalla los cursos que ofrecen:

- Examinador Forense Certificado Digital (Certified Digital Forensics Examiner)
- Examinador Forense Certificado de Redes (Certified Network Forensics Examiner)
- Investigación Forense de Delitos Cibernéticos y Digitales.

4.2 BUFETES LEGALES

Se realizó una investigación orientada a conocer si los bufetes legales de la ciudad de Tegucigalpa podrían llevar un caso de delito informático, se tomó una muestra de 25 bufetes, ya que fue de los que se pudo obtener información de contacto.

De los veinticinco bufetes consultados se obtuvo un cien por ciento (100%) de respuesta negativa al consultar si tiene en su historial algún caso de este tipo, y al consultar sí podrían llevar en la actualidad un caso, tres mencionaron que no están capacitados en la materia pero que podrían estudiar el caso.

4.3 RESULTADO DE ENCUESTAS APLICADAS

A continuación, se muestra los resultados obtenidos mediante la aplicación de encuestas al personal técnico que realiza investigaciones, a gerentes de TI, Oficiales de Seguridad, Auditores de Sistemas, profesionales de sistemas y derecho, así como población en general no relacionado con los mencionados anteriormente.

La muestra de personas encuestas varía según el tipo de encuesta aplicada, siendo el número de encuestas aplicadas según las personas a las que se tuvo acceso de acuerdo al perfil del encuestado.

Cabe mencionar que en la Dirección Nacional de Investigación Criminal no fue autorizada la aplicación de encuestas, por lo que no fue posible obtener información de este ente de investigación.

De igual manera no fue posible la aplicación de las encuestas de la Corte Suprema de Justicia (Jueces) y del Ministerio Público (Fiscales), ya que al momento de finalizar la investigación no se había obtenido respuesta a la solicitud de permiso para aplicar las mismas.

4.3.1 ENCUESTAS APLICADAS A ENTES DE INVESTIGACIÓN

La encuesta aplicada al personal técnico de investigación de los casos delictivos categorizados como delitos informáticos o que la informática fue utilizada para llevar a cabo la actividad penal, tuvo como objetivo principal conocer cuáles han sido las causas que les han dificultado aplicar adecuadamente la Informática Forense en las investigaciones realizadas.

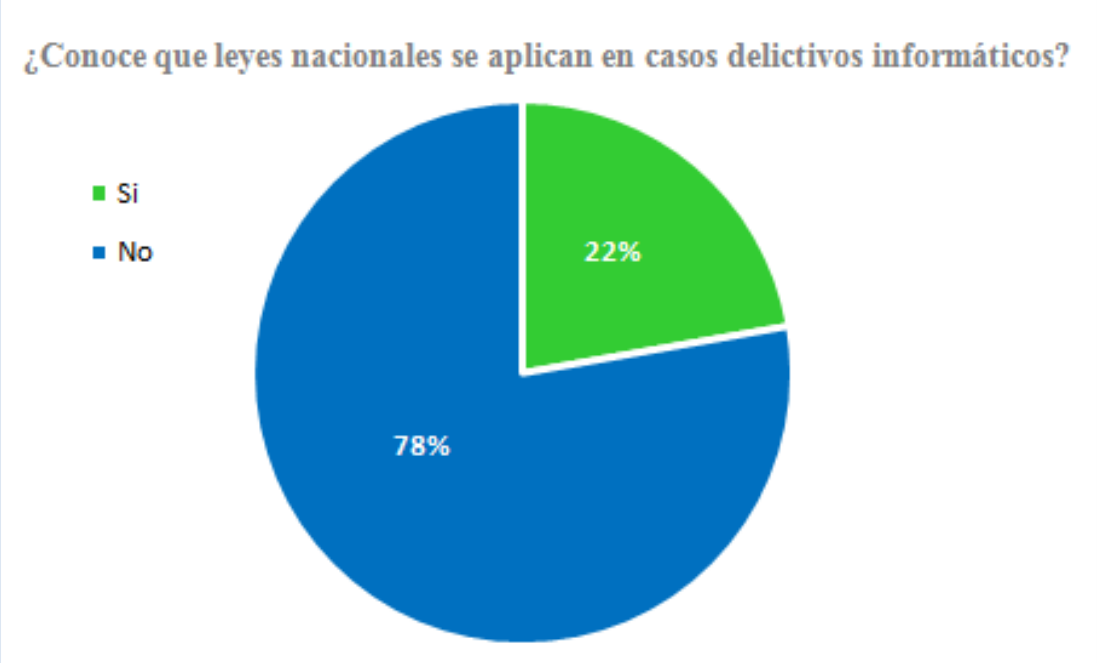


Figura 2. Leyes nacionales

Basándose en el resultado de la pregunta sobre el conocimiento de las leyes nacionales que son aplicadas a los casos delictivos informáticos como se presenta en la Figura 2, se logró determinar que el 78% del personal técnico que, realizada las investigaciones de estos casos, no tiene conocimiento sobre las leyes que deben ser utilizadas para proceder ante un juzgado una vez se ha obtenido la información a través de la aplicación de la Informática Forense. Lo anterior, indica que la falta de conocimiento o falta de una ley establecida para judicializar un caso

delictivo que involucre la informática, es un factor que no permite se pueda concluir una investigación.

Figura 3. Interés por recibir capacitaciones relacionadas con Informática Forense

De acuerdo a los resultados de la encuesta como se evidencia en la Figura 3, se identificó que todo el personal técnico de investigaciones de casos con relación a informática están interesados en recibir capacitaciones que se relacionen a los temas Informática Forense, Delitos Informáticos y/o Evidencia Digital, lo que genera la oportunidad de crear e impartir diplomados, cursos o capacitaciones donde se pueda obtener dicho conocimiento o reforzar los mismos. Así también, en la Figura 4 se logró determinar las ciencias y áreas de la informática que son importantes para resolver casos delictivos donde se han involucrado componentes tecnológicos; esto en conjunto con los resultados de la Figura 3, es de gran importancia para poder crear un plan de estudios o capacitación para que alguna institución interesada en brindar servicio educativo pueda tomarlo como referencia.

Dentro de las ramas que fueron mencionadas en las encuestas, se debe señalar que en la opción “Otros”, los técnicos de investigación hicieron alusión a temas como auditoria informática, estenografía, red oscura, seguridad informática, análisis de información y de videos

forenses, que son tomados en consideración al momento de realizar una investigación pericial, permitiendo ampliar la gama de los cursos que se podrían impartir.

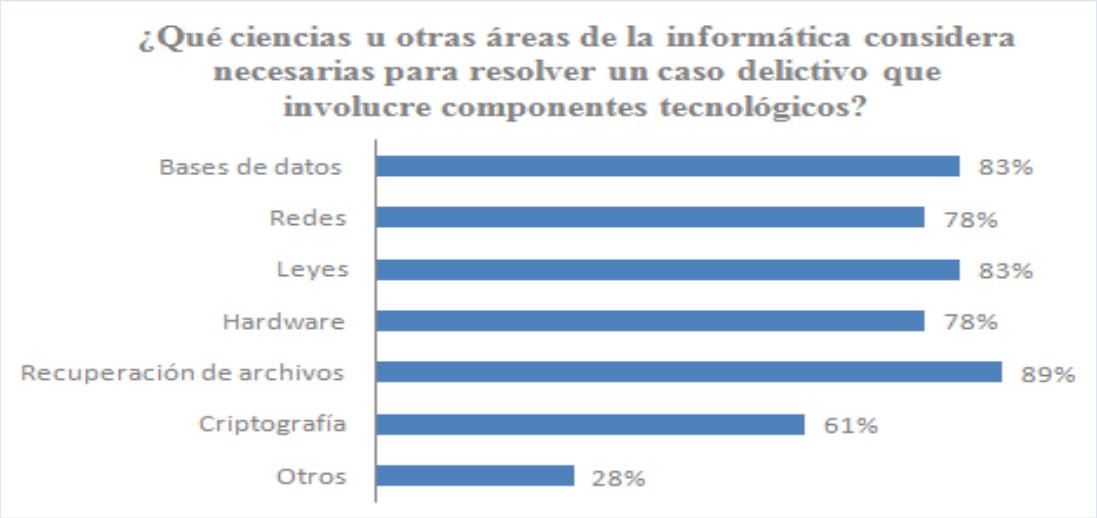


Figura 4. Ciencias y áreas de la informática para resolver casos delictivos

Con el fin de obtener información precisa y directa del personal a cargo de realizar investigaciones de actos delictivos con orientación a tecnología, se logró determinar los factores con los cuales se han visto afectados directamente en la aplicación de la Informática Forense al desempeñarse en sus labores. La información a detalle se muestra en la Figura 5 y en la misma se puede apreciar claramente que los factores principales se relacionan con el factor humano, cuando éste no es adecuado para desempeñar las funciones de cuales son responsables en una investigación, ya sea por falta de conocimiento que es generado por una escasa de capacitación al personal.

En la gráfica representada en la Figura 6, se da a conocer que los técnicos que realizan las investigaciones periciales informáticas han sido capacitados únicamente el 50%, lo que genera que en su mayoría el personal no tenga conocimientos sobre las buenas prácticas y metodologías que son aplicadas al momento del proceso de una investigación de esa índole.

También se logró identificar que alrededor del 45% los responsables de efectuar las investigaciones tienen desconocimiento de herramientas de hardware y software para los análisis de los componentes tecnológicos y como se hace la tipificación de los delitos informáticos.

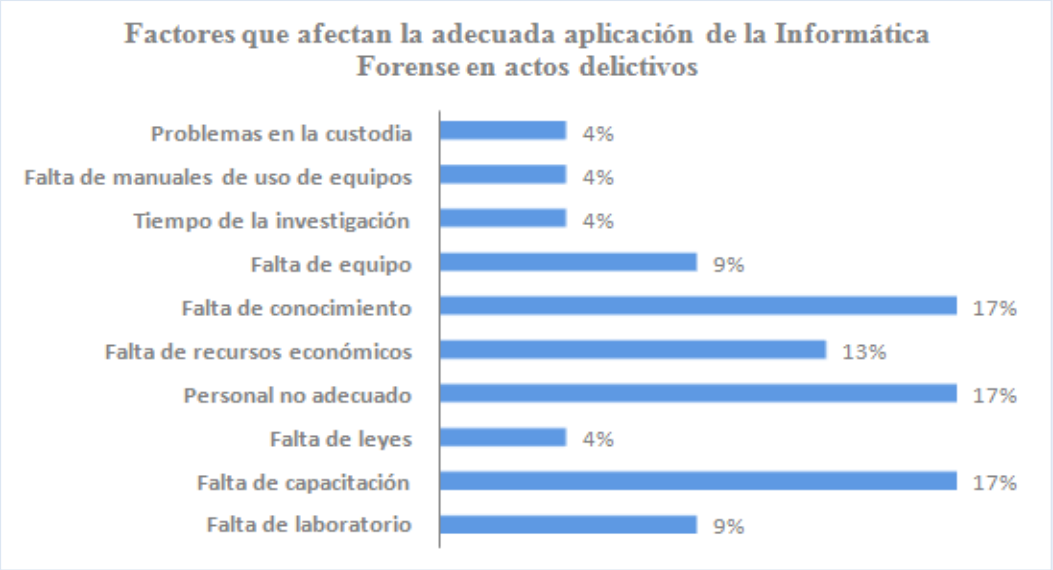


Figura 5. Factores que afectan la adecuada aplicación de la Informática Forense

Asimismo, se identificó que el 28% de los técnicos no tiene conocimiento de los cuidados de que debe tener la cadena de custodia para mantener su valor como evidencia. Con lo anterior se concluye que existe un alto grado de falta de preparación al personal responsable de generar la evidencia o información de un caso en investigación que debe ser llevado a juicio, por lo tanto, el sentido de la Informática Forense no está siendo tomado en consideración al momento de efectuarse un análisis o investigaciones de casos delictivos.

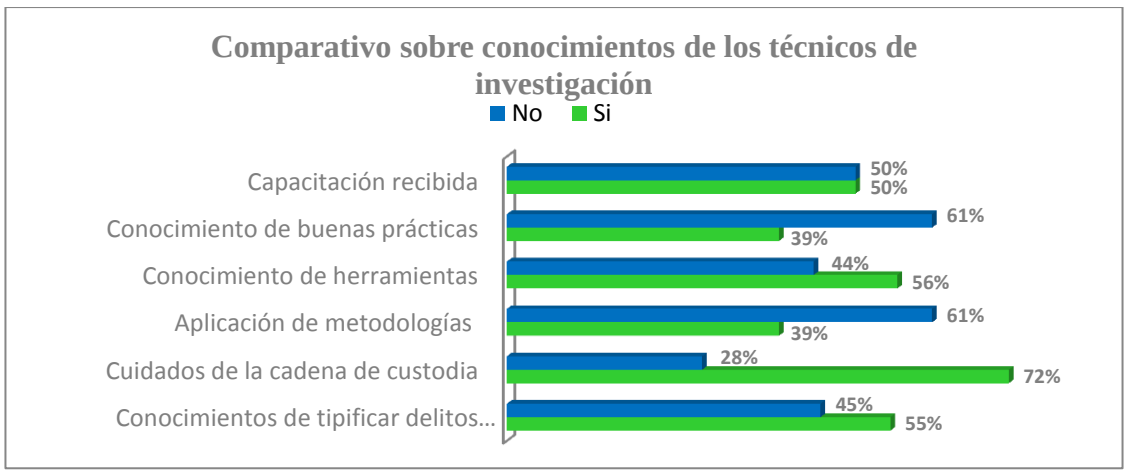


Figura 6. Comparativo sobre conocimientos de los técnicos de investigación

Para identificar si en el país se cuenta con los recursos necesarios para realizar investigaciones forenses tecnológicas, en la encuesta aplicada a los técnicos de investigación se le consultó sobre las instalaciones adecuadas y recursos suficientes para realizar investigaciones forenses en el campo informático, en base a los resultados de la encuestas, se determinó que en el país no se cuenta con las instalaciones adecuadas ya que no hay un laboratorio especializado para llevar a cabo las investigaciones, únicamente el 11% del personal encuestado considera que se tienen instalaciones apropiadas como se muestra en la Figura 7. También se identificó que el 56% de los técnicos encuestados cree que no se cuenta con los recursos necesarios para realizar sus funciones y el 18% no sabe si dichos recursos son suficientes.

Según lo indicado en las estadísticas, se pudo conocer que la falta de instalaciones y recursos son factores que están afectando actualmente a los técnicos de investigación de delitos periciales informáticos a aplicar adecuadamente la Informática Forense.

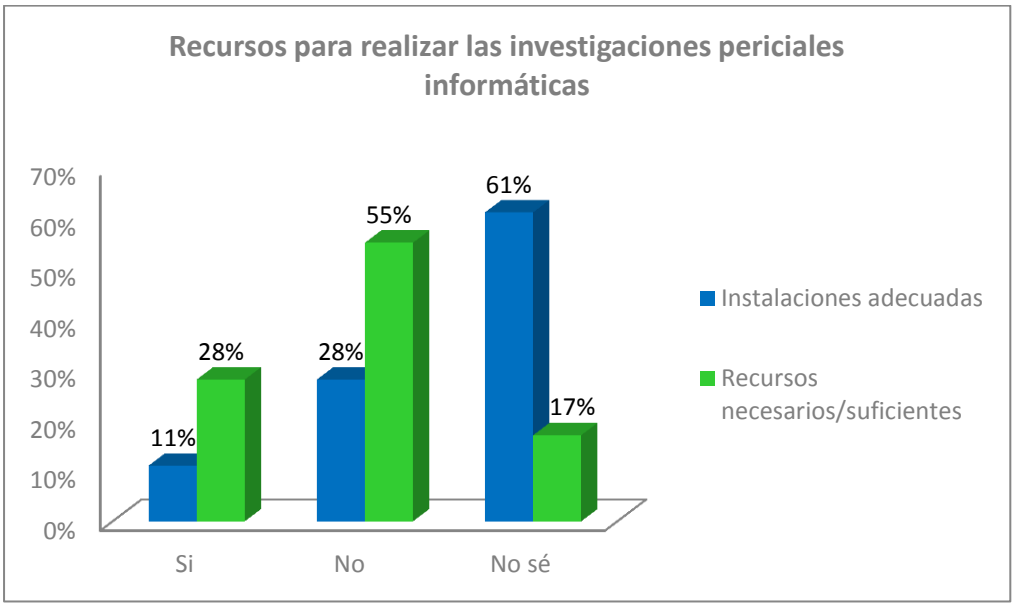


Figura 7. Recursos e instalaciones para realizar investigaciones periciales informáticas.

Al personal técnico se le consultó sobre las características que a su consideración debe tener un auditor que realice investigación de informática forense, dando como resultado que un alto porcentaje considera que el gusto por la investigación y la capacidad de análisis son de principales características con las que debe contar.

En la Figura 8 se muestra los resultados obtenidos, adicional a las características expuestas, mencionan que debe ser íntegro, acucioso, con conocimiento y apego a las leyes y respetuoso de ella, dinámico, ordenado, capaz, conocimiento sobre vinculación criminal y estar constantemente actualizándose sobre nuevas tecnologías.

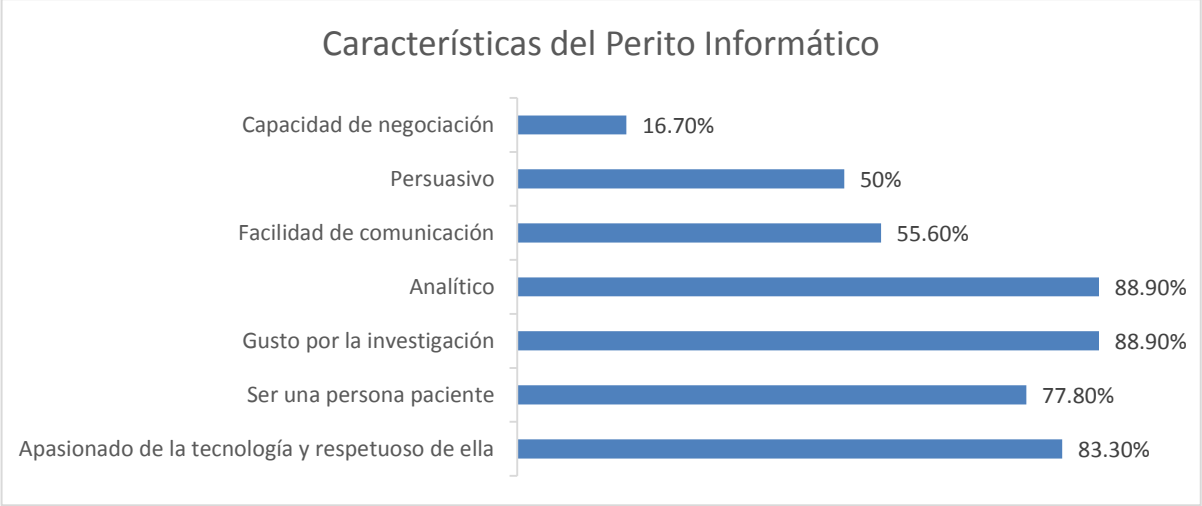


Figura 8. Características de un perito forense

4.3.2 ENCUESTAS APLICADAS A GERENTES DE TI, SEGURIDAD Y AUDITORIA DE SISTEMAS

Con el objetivo de investigar si las empresas de índole privado como público han sido víctimas de algún tipo de delito a través de la informática, cual fue el procedimiento ejecutado y la conclusión de estos casos, se aplicó encuestas a veintinueve personas que se desempeñan como Gerentes de TI, Seguridad Informática o Auditores de Sistemas. Los resultados se describen a continuación.

Según resultados de las encuestas aplicadas al personal que tiene conocimientos de ese tipo de casos ya sea por investigación interna o por administración de los componentes tecnológicos; se realizó un análisis a empresas que han sido víctimas de delitos con relación a la informática como se detalla en la Figura 8, se obtuvo un resultado del 45% de los encuestados que indico han experimentado algún tipo de acto delictivo en la empresa donde laboran.

Sin embargo, el 50% de estos casos no han sido reportados a las autoridades y el 61% no ha sido judicializado, a causa de falta de evidencia o leyes que respalden el delito del cual la empresa ha sido víctima.

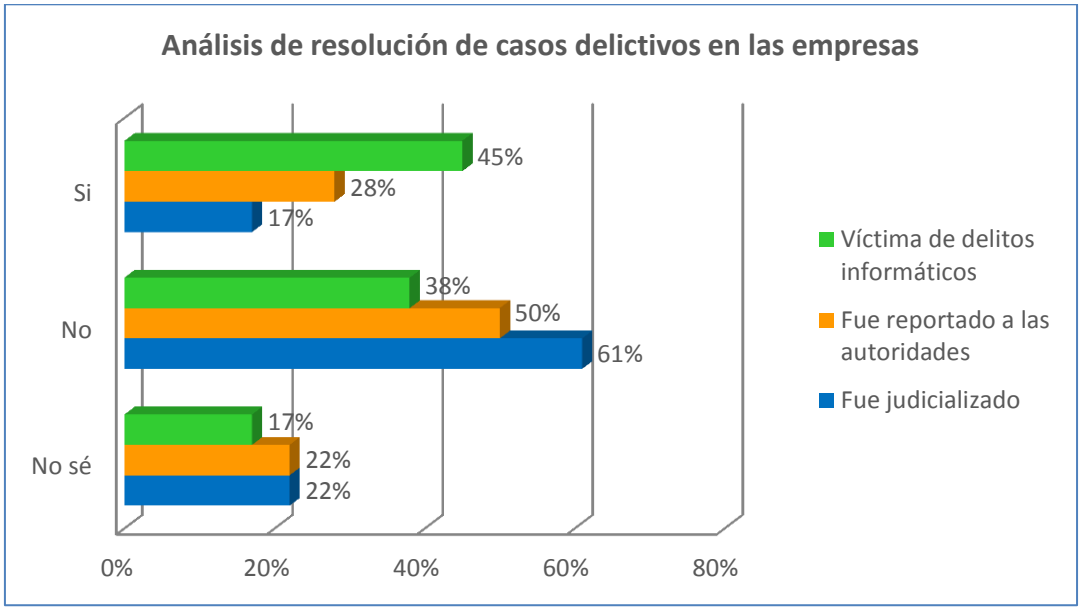


Figura 9. Análisis de resolución de casos delictivos en las empresas.

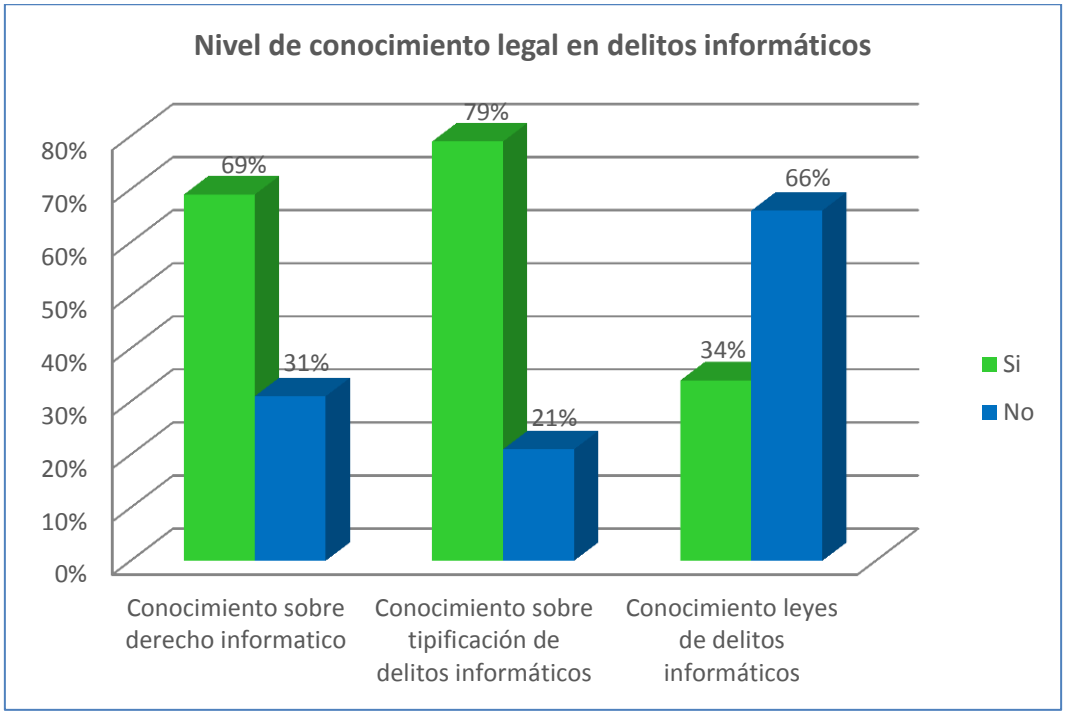


Figura 10. Nivel de conocimiento legal en delitos informáticos

En dicha encuesta también se realizaron preguntas sobre conocimiento legal que se aplique en casos donde se involucre a la informática, obteniendo como resultado de dichas preguntas, que pese a que el personal tenga conocimiento sobre derecho informático y la forma de tipificar los delitos de esa rama, desconocen las leyes que le pueden ser aplicados a casos de delitos informáticos como se ilustra en la Figura 10. Cabe hacer mención que este puede ser un factor por el cual las empresas no reportan los casos a las autoridades y no judicializan los mismos, según los resultados plasmados en la Figura 9.

A continuación, se detallan otros resultados de interés obtenidos de las encuestas aplicadas:

- El cien por ciento de los encuestados conoce sobre informática forense y muestran interés en recibir capacitación.
- Únicamente el 37.90% han recibido capacitación relacionadas con la materia, tanto dentro como fuera del país o de manera autodidacta. Siendo los cursos más relevantes los siguientes:

- Auditoria forense
- Computer Hacking Forensic Investigator v8
- Delito informático/investigación forense
- CobIT, Coso y auditoría interna de TI
- Análisis de Vulnerabilidades
- Certified Ethical Hacker
- Tipificación del delito financiero en el sistema bancario de Latinoamérica.
- Forense Hacking E-Council

- Un 51.7 % conoce sobre las buenas prácticas relacionadas con Informática forense, de los cuales un 66.7% es a nivel medio y un 33.3% principiante.
- Dentro de las limitantes especificadas por las personas que investigaron un hecho delictivo se encuentran:

    - Herramientas de Software
    - Tiempo
    - Personal poco capacitado
    - Falta de Leyes

4.3.3 ENCUESTAS APLICADAS A PROFESIONALES DE SISTEMAS Y DERECHO

Se aplicó una encuesta a setenta profesionales pertenecientes a las carreras de Informática y Derecho, esto con la finalidad de obtener información relacionada con el conocimiento que sobre informática forense tienen los profesionales.

Los resultados obtenidos, presentados en la Figura 11, muestran que un alto porcentaje (70%) de los profesionales encuestados conocen o han escuchado hablar sobre informática forense, sin embargo solamente un 54.3% conoce sobre derecho informático y un 57% sobre los delitos informáticos, lo que representa un riesgo, ya que al presentarse un caso de delito informático no contarán con todos los conocimientos básicos necesarios para llevar a cabo una adecuada investigación, sumado a que solamente un 21.4% tienen conocimiento sobre las buenas prácticas relacionadas con informática forense, incrementando así el riesgo anteriormente expuesto. Por otra parte, únicamente un 20% conocen sobre las leyes que pueden ser aplicadas en casos judiciales por delitos informáticos, lo que debilita la exposición del caso al no contar con conocimientos sólidos que permitan llevar a juicio el delito investigado.

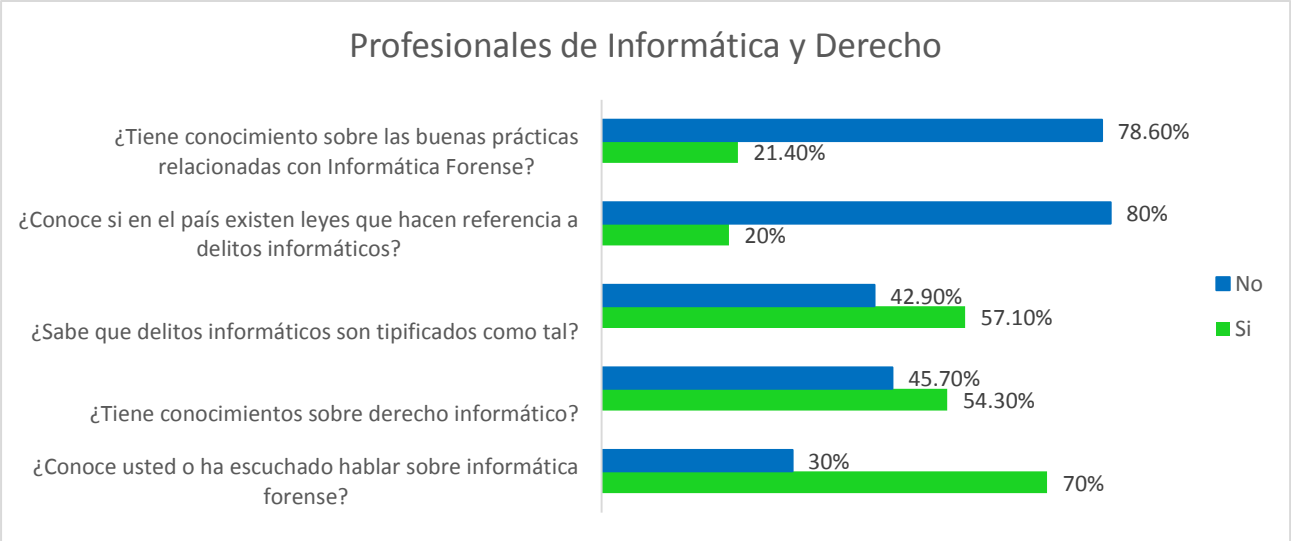


Figura 11. Conocimiento de los profesionales de Informática y Derecho

Cabe mencionar que de los profesionales encuestados que indican contar con algún conocimiento en las consultas anteriores, su nivel es principiante, lo que indica que aún y cuando

conocen sobre el tema se requiere capacitaciones para mejorar los niveles de conocimientos y aplicación, pues únicamente el 7.1% indica haber recibido capacitación sobre informática forense.

Otro resultado obtenido es sobre las ciencias u otras áreas de la informática que a criterio de los profesionales se consideran necesarias para resolver delitos informáticos, donde el 84.3% indica que es necesario conocimiento sobre Base de Datos, siendo la de mayor puntuación y conocimientos sobre Hardware con un 52.9% la menor. Adicionalmente a las ciencias expuestas en la Figura 12 mencionan que es necesario tener conocimientos sobre Seguridad Informática, Auditoria de Sistemas, evaluación de bitácoras de sistemas, circuito cerrado (sistemas de video vigilancia).

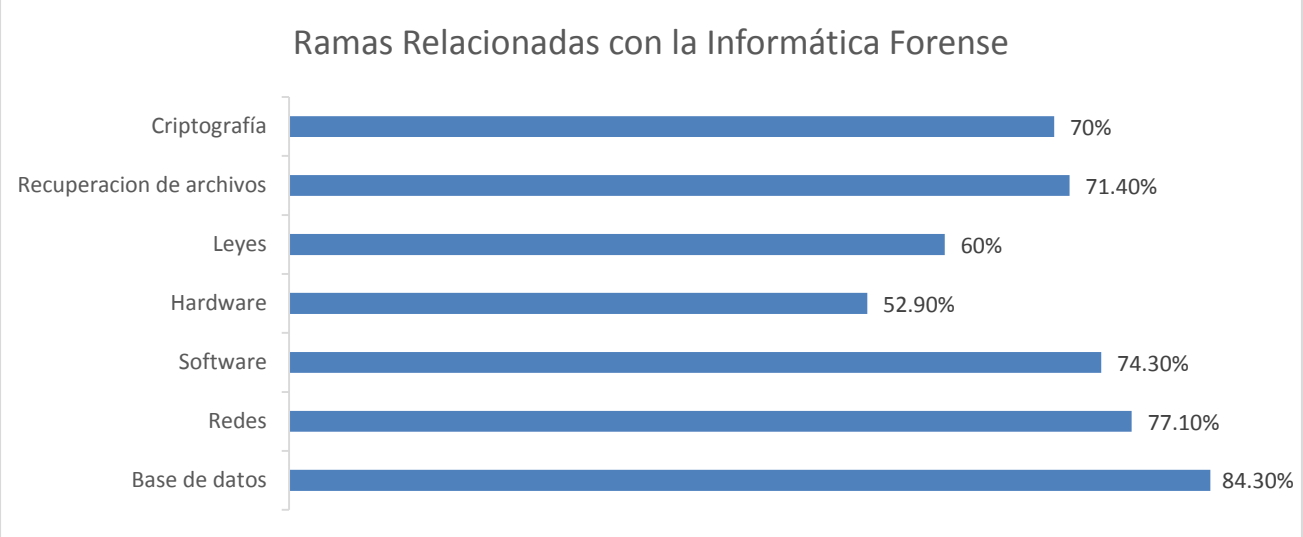


Figura 112. Ciencias o materias relacionadas con Informática Forense

Al consultarles sobre los factores que a su criterio afectan la adecuada aplicación de la Informática Forense los encuestados indicaron los siguientes:

- Desconocimiento/Poco conocimiento
- Falta de recursos humanos y material
- No existe personal capacitado para implementarla
- No se cuenta con la tecnología necesaria
- Falta de profesionales expertos en el área
- Atraso tecnológico en el país
- La cultura sobre los delitos informáticos y su símil a un crimen físico

- Poca confianza de utilizar métodos de investigación
- Capacidad del personal técnico
- Vacíos legales
- Desconocimiento de las herramientas y metodologías
- Uso de la información de manera incorrecta
- Factor económico en las empresas
- Corrupción

4.3.4 ENCUESTAS APLICADAS A POBLACIÓN EN GENERAL

A fin de recabar información sobre el conocimiento que la población en general y no relacionada con las profesiones de sistemas y derecho tienen acerca de informática forense y derecho informático, se realizó la aplicación de una encuesta a una muestra de setenta y tres personas (73), obteniendo resultados que se describen a continuación:

Según los resultados generados por medio de la aplicación de las encuestas y los cuales fueron analizados, se encontró que el 31.50% de las personas encuestadas conocen o han escuchado acerca de Informática Forense, y un 21.90% conocen sobre derecho informático; sin embargo, únicamente un 4.10% conoce sobre las leyes que se relacionan con los delitos informáticos y un 27.40% acerca de aquellos delitos que son tipificados como informáticos, como se muestra en la Figura 13.

A continuación, se detallan los factores que la población considera son riesgos para ser víctima de un delito informático:

- Fraude
- Por tanta persona que solo busca hacer un daño
- Por el acceso a la cuenta institucional que manejo, tarjetas de crédito, sucursales electrónicas.
- El robo de identidad o el clonaje de tarjetas de crédito son una moda hoy en día
- Por los diferentes servicios bancarios que utilizamos.

- Porque todos los días usamos la Informática en nuestras vidas
- Porque al desconocer el tema, puedo ser víctima o autor del hecho y sin saberlo
- La existencia de muchos hackers.
- Sí, si hubiese algún delito al usar la información personal que se pone en las redes sociales.
- Acceso constante a la web
- Por el constante avance tecnológico
- El uso de tarjetas de crédito en lugares no seguros, el robo de celulares ya que ahora todo está conectado al dispositivo, correos electrónicos, banca electrónica, etc.
- Muchas empresas informáticas y el gobierno no están tan adelantados como otros países, pero el esfuerzo es constante y la tendencia es seguir mejorando
- Los cambios en la forma de operar de los delincuentes

De igual manera a continuación se detallan los delitos identificados y descritos en las encuestas:

- Delitos relacionados a la violación de la confidencialidad y los relacionados a las patentes o derechos de autor
- Robo/suplantación de identidad
- Fraudes
- Robo/Manipulación/borrado de bases de datos (información)
- Falsificación de datos a través del uso de herramientas informáticas
- Bulling cibernético
- Difamación en sistemas redes sociales
- Invasión/hackeo de cuentas privadas
- Phishing
- Difusión o compra de pornografía infantil
- Piratería
- Falsificación de cuentas, robo electrónico
- Infiltración a sistemas
- Clonación de tarjetas

Cabe mencionar que el desconocimiento de estos temas en la mayoría de las personas encuestadas puede considerarse un factor que afecte la aplicación de la informática forense, pues como afectados pueden no realizar una denuncia de manera correcta o solicitar un debido proceso en las investigaciones.

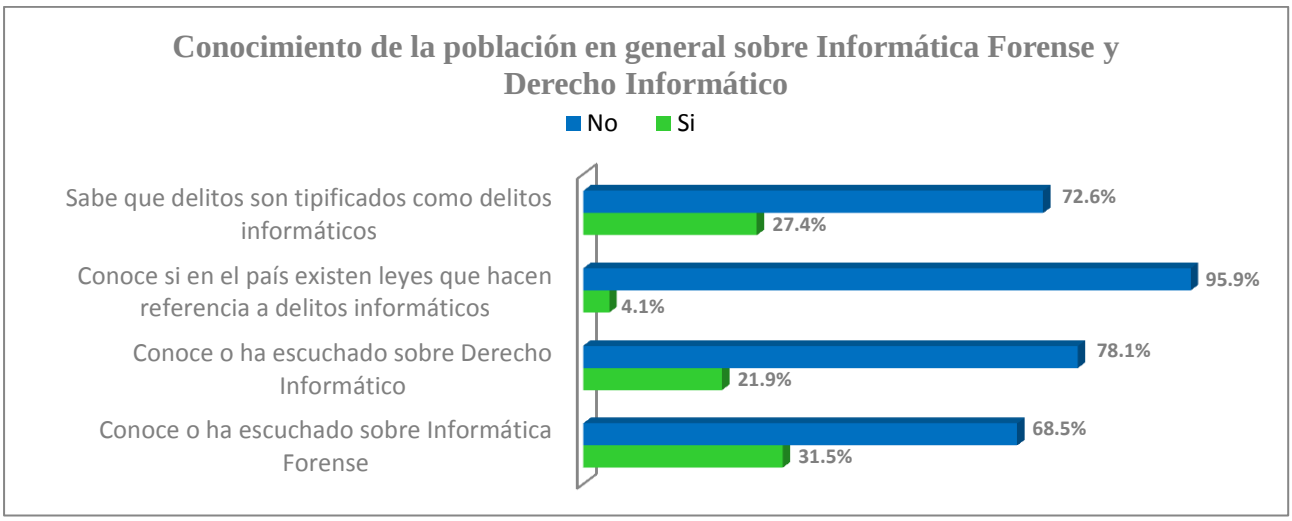


Figura 13. Conocimiento de la población sobre Informática Forense y Derecho Informático

Otro resultado obtenido de la población es el reflejado en la Figura 14, donde se muestra que la población es consciente del riesgo al que está expuesto de ser víctima de un delito relacionado con tecnología. Otro resultado muestra que el 45% de los encuestados han sido víctima o conocen a alguien que ha sufrido este tipo de delitos.

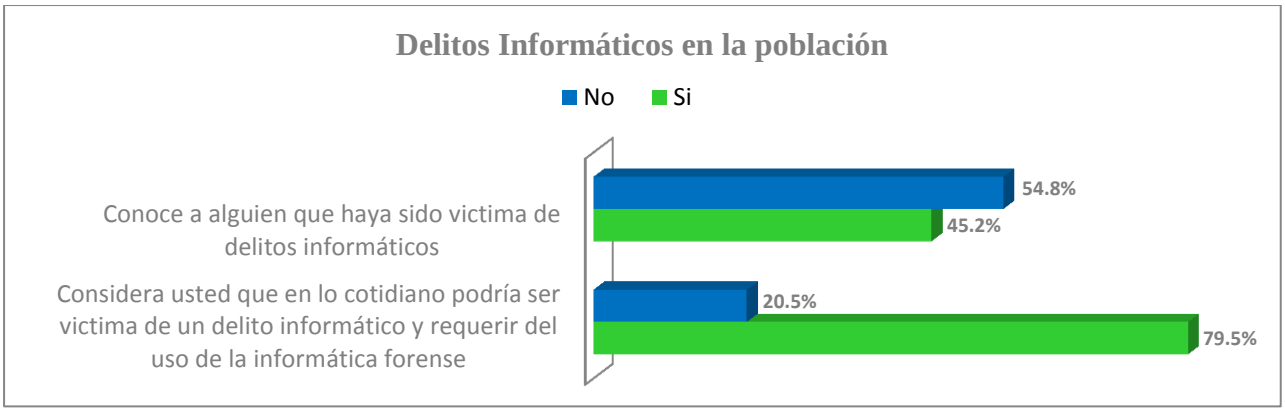


Figura 14. Percepción de la población con relación a los delitos informáticos

En la figura 15 se presenta los resultados que se obtuvieron a cerca de la percepción que la población encuestada tiene sobre la capacidad de investigación en Honduras. Al ser consultados sobre si considera que el país está preparado para hacer frente a los delitos informáticos únicamente el 9.6% considera que si y un 16.4% cree que se tiene la capacidad para aplicar correctamente la Informática Forense.

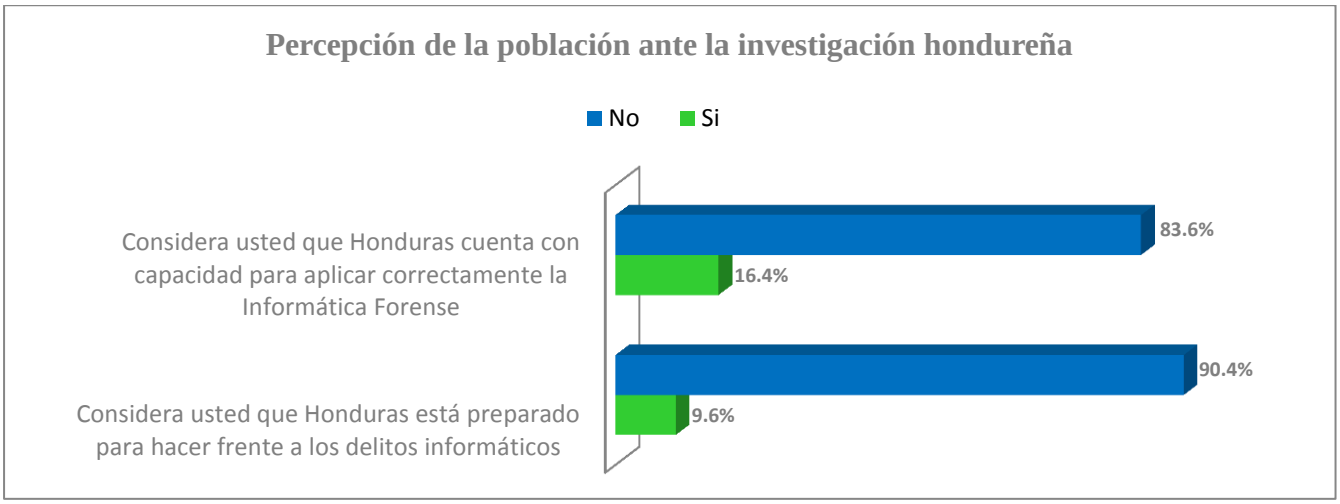


Figura 15. Percepción de la población sobre la investigación hondureña.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Una vez finalizada la investigación se puede concluir que entre los factores que afectan la adecuada aplicación de la informática forense están los siguientes:

- No se cuenta con suficiente equipo/herramientas de hardware y software y los laboratorios necesarios para realizar análisis de informática forense.
- El personal que realiza el peritaje no cuenta con toda la capacitación necesaria en tema de informática forense (metodologías, técnicas, cadena de custodia, etc.).
- Existe un alto grado de desconocimiento sobre informática forense y los delitos informáticos.
- La escasa legislación nacional relacionada con el tema y la no suscripción de Honduras a convenios internacionales.
- Limitadas opciones de capacitación a nivel nacional sobre temas de seguridad informática, auditoria de sistemas y derecho informático.
- Las pocas oportunidades de capacitación en informática forense (técnicas, herramientas, buenas prácticas, evidencia digital, entre otras).
- El poco conocimiento del tema por parte de fiscales en ocasiones afecta la realización de investigaciones forenses, por otra parte en muchas oportunidades los jueces desestiman los medios probatorios digitales, afectando así el resultado de las investigaciones.
- La falta de recursos económicos, es un factor que afecta la aplicación de la Informática Forense.
- Poca conciencia de los problemas y/o riesgos de la tecnología, en relación a ser víctima de algún delito informático, lo que conlleva que no siempre se denuncien los delitos o se haga la denuncia de la forma correcta.
- La percepción que la población tiene sobre la capacidad de la investigación hondureña para hacer frente a los delitos informáticos y aplicar correctamente la Informática Forense.

Para realizar una adecuada investigación forense es necesario contar con herramientas de hardware y software que permitan recolectar toda la información necesaria para dicha investigación. También se requiere un grupo de profesionales especialistas en diferentes áreas.

Al momento de realizar una auditoría forense y con la finalidad de obtener con mejores resultados se requiere el concurso de especialistas de las ramas del derecho, base de datos, redes, hardware, criptografía, finanzas, contabilidad, entre otros.

La aplicación de la Informática forense a nivel internacional se rige por una serie de normas y buenas prácticas, así como convenios de ciberseguridad que permiten una mejor y más amplia aplicabilidad de la misma.

Un auditor forense para realizar un mejor desempeño de sus funciones debe conocer sobre leyes, cuidados de la cadena de custodia, buenas prácticas y metodologías que permiten optimizar el uso de las herramientas con las que cuenta, de igual manera debe contar entre otras cualidades con capacidad de análisis, gusto especial por la investigación y ser respetuoso de la tecnología.

5.2 RECOMENDACIONES

Una vez finalizada la investigación se considera necesario emitir algunas recomendaciones orientadas a brindar oportunidades de mejora en el conocimiento y la aplicación de la informática forense.

1. Se requiere la apertura de espacios de estudio donde se brinde entrenamiento en Informática Forense y se capacite de manera adecuada y con los conocimientos necesarios a las personas involucradas en el proceso de una investigación forense que involucre componentes tecnológicos, de igual manera aquellos profesionales del campo de sistemas y derecho que deseen adquirir conocimiento en la materia.

Ejemplo de posibles temas a tratar:

- Informática Forense
- Delitos Informáticos y formas de operación de los criminales
- Cibercriminalidad y ciberseguridad
- Recolección de medios de prueba en la escena del crimen

- Medios de prueba Digital
- Cadena de custodia de la evidencia
- Análisis forense en ambiente Windows, Mac y Linux
- Análisis forense digital
- Análisis en aplicaciones
- Análisis en equipo de comunicación (ejemplo teléfonos celulares)
- Análisis de documentos digitales e impresos
- Análisis en archivos, memorias, discos
- Análisis forense en redes, mensajería, correo electrónico
- Herramientas, equipo, técnicas y metodologías para un análisis forense
- Temas legales, procesales y fundamentos de prueba
- Elaboración de informe pericial
- Dictamen forense y pericial
- Derechos y deberes de un forense informático

Adicionalmente, se propone se realicen capacitaciones en las materias relacionadas, como ser derecho, donde se abordan temas como ser:

- Derecho Informático
- Delitos Informáticos
- Aspectos legales relacionados con seguridad informática
- Validez de medios probatorios digitales
- Derechos civiles en temas relacionados con tecnología
- Legislación relacionada con la materia

2. Se debe capacitar a Fiscales y Jueces sobre delitos informáticos y medios de prueba relacionados y sobre la importancia que la informática forense tiene en la investigación de los mismos.

3. Es importante que la ciudadanía tome conciencia de los peligros que las tecnologías conllevan, así como de la existencia de los delitos relacionados con las mismas y la importancia que en caso de ser víctima de un delito informático el mismo sea denunciado a las autoridades.

4. Es necesario crear mecanismos de comunicación y acción entre los entes de investigación y los entes encargados de impartir justicia, de forma tal que las investigaciones sean llevadas a cabo de la mejor manera y por el personal.

5. Se debe realizar la aprobación del anteproyecto del código penal, de esta manera se tendrá un marco jurídico que sustente la investigación informática forense y la judicialización de manera adecuada de los casos de delitos informáticos.

6. Se recomienda la suscripción de Honduras a los Convenios Internacionales sobre Ciberseguridad y la adopción de las Normas y Guías de Buenas prácticas internacionales.

7. Creación de una Agencia especializada en Investigación de delitos informáticos, con un laboratorio Forense que cuente con todos los recursos necesarios que permita realizar las investigaciones con los más altos estándares de calidad y bajo las normas y guías de buenas prácticas existentes a nivel mundial.

   A continuación, se detallan algunos de los requerimientos que se deben de considerar para el laboratorio:

- Equipo (Hardware y Software) especializado y de última tecnología
- Profesionales especialistas en distintas ciencias y/o áreas de la informática
- Secciones especializadas dentro de la agencia. Ejemplo: Redes, celulares, rasgos biométricos, evidencia digital, etc.)
- Asignación de presupuesto
- Trabajo en conjunto con el resto de las Agencias de Investigación
- Apoyo a empresas gubernamentales, privadas y población en general

8. Definición de un marco de trabajo (metodología, buenas prácticas, herramientas a utilizar).

REFERENCIAS BIBLIOGRÁFICAS

Abog. Rodriguez Barreda, E. A. (2009). Delitos Informáticos y Delitos Informatizados. *Revista Electrónica del Trabajador Judicial* .

ACPO. (24 de Abril de 2014). *Good Practice Guide for Digital Evidence: ACPO*. Obtenido de ACPO Web Site: http://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/

Acurio Del Pino, D. S. Delitos Informáticos: Generalidades.

Acurio Del Pino, D. S. (2009). Informática Forense en el Ecuador. *Fiscalía General del Estado* , 21.

Americanos, O. d. (2016). *Informe del Observatorio 2015: Seguridad cibernética en América Latina y el Caribe*. Obtenido de http://observatoriociberseguridad.com/

Arias Chaves, M. (2007). Panorama general de la Informática Forense y de los delitos informáticos en Costa Rica. *Inter Sedes* , 143.

Balanta, H. (2009). APROXIMACIÓN LEGAL A LOS DELITOS INFORMÁTICOS UNA VISIÓN DE DERECHO COMPARADO. *Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal.* Colombia.

Banco Interamericano de Desarrollo. (2016). *BID y OEA instan a América Latina y Caribe a mayores esfuerzos en ciberseguridad.* BID.

Canedo Estrada, A. (2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano* .

Cañaveral, S. P. (Mayo de 2015). *Herramientas más Populares de la Informática Forense*. Obtenido de http://patriciakanaveral.blogspot.com/2015/05/herramientas-mas-populares-de.html

Cellebrite Mobile Synchronization LTD. (2014). *On retrieval*. Obtenido de On retrieval Web Site: http://www.onretrieval.com/wp-content/uploads/Cellebrite_UFED-OnRetrieval-Distribuidor-Spain.pdf

Council of Europe. (Noviembre de 2016). Obtenido de Council of Europe Web Site: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185)

CRU Inc. (2016). *CRU Inc - Dito*. Obtenido de CRU Inc Web Site: www.cru-inc.com/ditto/

Darahuge, M. E., & Arellano González, L. E. (2011). *Manual de Informática Forense.* Buenos Aires: Erreper.

Decreto 144-83 Código Penal. (15 de Marzo de 2006). *Diario Oficial La Gaceta* . Honduras.

Decreto No. 211-2006 Código Procesal Civil . (26 de Mayo de 2007). *Diario Oficial La Gaceta* .

DNII. (s.f.). *Quienes Somos: DNII*. Obtenido de DNII Web Site: http://www.dnii.gob.hn/quienes-somos.html

ENFSI. (Noviembre de 2015). *BPM for the Forensic Examination of Digital Technology: ENFSI.* Obtenido de ENFSI Web Site: http://www.enfsi.eu/sites/default/files/documents/enfsi-bpm-fit-01_2.pdf

Estrada Garavilla, M. (s.f.). *Delitos Informáticos: UNIFR.* Obtenido de UNIFR Sitio Web: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Evidence Technology Magazine . (2008). Obtenido de Evidence Technology Magazine Web Site: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=920

Federal Bureau of Investigation. (Abril de 2000). *Forensic Science Communications: FBI*. Obtenido de The FBI Federal Bureau of Investigation Web Site: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

Gómez, Á. B. (2012). *La figura del Perito Judicial Informático.* Madrid: El Derecho.

Gomez, M. M. (2001). *Introducción a la Metodología de la Investigación Científica.* Córdoba: Editorial Brujas.

Guidance Software. (1997). *Guidance Software Tableau*. Obtenido de Guidance Software Web Site: https://www2.guidancesoftware.com/products/Pages/tableau/products/tableau-password-recovery.aspx?cmpid=nav_r

i zone-h unrestricted information. (s.f.). Obtenido de i zone-h unrestricted information: Web Site: http://www.zone-h.org/archive/filter=1

Ignacio, M. G. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. *Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral* .

Informática Legal. (2016). Obtenido de http://www.informaticalegal.com.ar/derecho-informatico/

Insa Mérida, F., Lázaro Herrero, C., & García González, N. (2008). Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo. *Enlace* .

Internet Security Auditors. (2016). Obtenido de Internet Security Auditors Web Site: www.isecauditors.com/informatica-forense-peritajes

ISFS. (Agosto de 2009). *Computer Forensics Part 2: Best Practices: ISFS.* Obtenido de ISFS Web Site: http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf

ISO. (2012). *ISO/IEC 27037:2012: ISO*. Obtenido de ISO Web Site: https://www.iso.org/obp/ui/#iso:std:44381:en

ISO. (2015). *ISO/IEC 27042:2015: ISO*. Obtenido de ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en

J. C., N. R., A. R., J. P., Á. R., M. S., y otros. (2010). *El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas.* Bogotá, Colombia: Ediciones Uniandes.

JDMESALOSADA. (2015). *Kit de Herramientas para el Análisis Forense*. Obtenido de https://informaticaforenseunad.wordpress.com/author/jdmesalosada/

Jeimy J. Cano, P. C. (s.f.). Introducción a la informática forense - Una disciplina técnico-legal. *dos* .

Jiménez Rojas, J. R. (2016). Delitos informáticos en México. *Revista .Seguridad* .

Juristas Forenses y Asociados. (15 de Marzo de 2012). Obtenido de http://delitinfom.blogspot.com/: http://delitinfom.blogspot.com/2012/03/concepto-objetivos-y-herramientas-de-la.html

Kaspersky. (9 de Noviembre de 2012). *Blog de Kaspersky.* Obtenido de Blog de Kaspersky: La geografía del ciberdelito: América Latina: http://latam.kaspersky.com/geografiaciberdelitolatam

Krone, T. *High Tech Crime Brief.* Canberra, Australia.

Krone, T. (2005). High Tech Crime Brief. Canberra, Australia: Australian Institute of Criminology.

LBA Group. (s.f.). *LBA Group EMFaraCage*. Obtenido de LBA Group Web Site: https://www.lbagroup.com/products/faraday-cage-rf-shielding-enclosure

Ley 906. (01 de Septiembre de 2004). *Diario Oficial No. 45.658* . Colombia.

Ley No. 53-07. (23 de Abril de 2007). Santo Domingo, República Dominicana.

Lima de la Luz, M. (1984). *Delitos Electrónicos.* México: Ediciones Porrua.

López, J. P. (s.f.). *Del disco flexible a la nube:pasado, presente y futuro de la Informatica Forense.* Obtenido de Temas Avanzados en Seguridad y Sociedad de la Información.

López, Ó., Amaya, H., & León, R. (2001). INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS. *Universidad de Los Andes Bogotá, Colombia* .

McKemmish, R. (1999). What is Forensic. *Australian Institute of Criminology* , 1-2.

McKennish, R. (1998). *Study Overseas Developments in Forensic Computing.* Australia: Donald Mackay Churchill Fellowship.

Ministerio Público. (23 de Agosto de 2016). *Fiscalía General: Ministerio Público*. Obtenido de Ministerio Público Web Site: https://www.mp.hn/index.php/fiscalia-general

Ministerio Público. (2014). *Quienes Somos: Ministerio Público*. Obtenido de Ministerio Público Web Site: https://www.mp.hn/index.php/about

NCJRS. (Abril de 2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement: NCJRS.* Obtenido de NCJRS Web Site: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Observatorio de Delitos Informáticos de Latinoamérica. (28 de Junio de 2016). *Reporte 2016.* Obtenido de www.odila.org: https://www.odila.org/pdf/Informe_ODILA_2016.pdf

Observatorio de la Ciberseguridad en América Latina y el Caribe. (2016). Obtenido de Observatorio de la Ciberseguridad en América Latina y el Caribe: Web Site: http://observatoriociberseguridad.com/country/hn

OJP. (19 de Enero de 2009). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders: OJP.* Obtenido de OJP Web Site: http://ojp.gov/newsroom/pressreleases/2010/NIJ10038.htm

Ondata Internacional. (2016). *Ondadata - Equipos Forensic.* Obtenido de Ondata Web Site: http://www.ondata.es/recuperar/equipos-forensics.htm

Pagès López, J. (2013). Del disco flexible a la nube: pasado, presente y futuro de la Informatica Forense. *Temas Avanzados en Seguridad y Sociedad de la Información* (págs. 7-18). Madrid: http://www.criptored.upm.es/descarga/ConferenciaJavierPagesTASSI2013.pdf.

Pino, D. S. (s.f.). *Delitos Informéticos: Generalidades.* Obtenido de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Prandini, P., & Maggiore, M. L. (2013). CIBERDELITO EN AMÉRICA LATINA Y EL CARIBE. *LACNIC* .

Público, M. (s.f.). Obtenido de https://www.mp.hn/.

RFC 3727. (Febrero de 2002). *Guidelines for Evidence Collection and Archiving: RFC 3727.* Obtenido de RFC 3727 Web Site: https://www.rfc-editor.org/rfc/rfc3227.txt

Roberto Hernández Sampieri, C. F. (2014). *Metodología de la Investigación.* México: MacGraw-Hill Education.

Ros, A. J. (2015). Clasificación y estudio de herramientas. *Escuela Técnica Superior de Ingeniería Informática Universidad Politécnica de Valencia* , 37-38.

Salmerón, A. (2015). Criminalística para informáticos forenses y peritos. *Formación en el Campus Internacional de Inteligencia y Pericia (CIIP)* .

Sampieri, R. H., Collado, C. F., & Baptista, P. L. (2010). *Metodología de la Investigación.* México: McGraw Hill.

SWGDE. (14 de Septiembre de 2013). *Best Practices for Computer Forensics: SWGDE.* Obtenido de SWGDE Web Site: https://www.swgde.org/documents/Archived%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20v3-0

Téllez Valdes, J. (2004). *Derecho Informático.* México: McGraw-Hill.

Viega Rodríguez, D. E. (2011). Un nuevo desafío jurídico: Los Delitos Informáticos.

X-Ways. (2015). *X-Ways Forensics: Integrated Computer Forensics Software*. Obtenido de X-Ways Web Site: http://www.x-ways.net/forensics/

ANEXOS

6.1 INVESTIGACIÓN EMPRESA HONDUREÑA

Contenido

Introducción

El presente informe tiene como propósito describir detalladamente el incidente de seguridad ocurrido el día 15 de octubre del presente año a través de nuestra pagina web físicamente ubicada en Toronto Canadá en hosting con la empresa WSI. Además provee un instrumento valioso para la toma de decisiones en relación a los servicios profesionales de la compañía Hosting Walt Disney quien actualmente es la encargada de mantener el hosting de la página web y el servidor de correos ACME.com, de igual manera incita a revisión de los contratos de servicios con otros proveedores.

Además de lo expuesto anteriormente, el presente informe detalla una muestra de las amenazas a las que todo sistema de información se encuentra expuesto hoy en día y por tal razón de la importancia de tomar las medidas necesarias para evitar este tipo de incidentes.

En el transcurso del incidente y mientras se desarrollaban las investigaciones del caso se emitieron dos comunicaciones internas a la Gerencia General, informando acerca de acciones realizadas y de los resultados preliminares de la investigación.

Por la importancia de la información que en este informe se presenta, este debe ser considerado como información confidencial y de uso exclusivo interno.

Alcance

El alcance de este informe se limita a describir las acciones ejecutadas durante y después de la ocurrencia del evento y por la Administración de Seguridad Informática. Algunas de las acciones investigativas acerca del autor o posibles implicados en la ejecución de esta agresión se mantendrán en carácter confidencial y para uso exclusivo de la Gerencia General.

Descripción del incidente

El día 14 de octubre de 2008, Empresa ACME, S. A. fue victima de un ataque a la página web por persona desconocida y no autorizada provocando cambios no autorizados en la información publicada en la página y denegación de servicios a personal autorizado.

Como parte del ataque el mismo atacante realizo el envió de múltiples correos electrónicos haciéndose pasar por la gerencia de Empresa ACME, S. A. con la cuenta ggerencia@acme.com con palabras insultantes y degradantes en contra de nuestros clientes. A este tipo de ataque se le conoce como e-mail spoofing. Este correo fue enviado a un número aun no determinado de personas dentro de las que se incluían algunos clientes y colaboradores de ACME. (Anexo 1)

Además de ello el atacante, envió un correo electrónico a tres de los principales gerentes de la institución en el cual acreditaba sus acciones y amenazaba con realizar mas daño a la institución. (Anexo 5)

Acciones Realizadas (Cronología)

La siguiente es una lista de las acciones llevadas a cabo durante el desarrollo del incidente:

1. Al recibir notificación de nuestros clientes acerca de la circulación de un correo electrónico de la gerencia de ACME, se trato de ingresar a la administración de la página web mediante el usuario y la contraseña que ha sido administrada por el personal de investigación y desarrollo de mercadeo, obteniendo resultados fallidos.

2. Se contactó al señor Silver Surfer quien es Senior Marketing Consultant de la Corporación Hosting Walt Disney para solicitar de su colaboración y resolver el problema.

3. El señor Silver Surfer mediante comunicación telefónica con la compañía WSI solicito reiniciar las contraseñas para la administración de la página web; una vez obtenida la conformación de estas acciones por la empresa WSI, se logro ingresar a la administración de la página web y remover la imagen con el mensaje insultante. Además de ello se solicito las bitácoras del servidor que aloja la página web.

4. El Gerente General acordó dar de baja momentáneamente la página web, hasta que exista una garantía de que este tipo de incidentes no se repitan ya sea por el atacante conocido o cualquier otro.

5. Se recibieron las bitácoras del sistema unos minutos después de la solicitud (30 min aproximadamente). Al revisar las bitácoras del sistema se encontraron los siguientes datos:
    a. El atacante cambio contraseña del usuario *admin* desde la dirección IP 204.249.101.134 que según las investigaciones pertenecen a la empresa Multidata, S. A. (Anexo 2)
    b. El atacante coloco la imagen ACME.jpg desde la dirección IP 204.249.101.134. (Anexo 2)

6. Se cambiaron las contraseñas administrativas de todos los servidores y equipos de comunicaciones, como medida de prevención a los sistemas de información.

7. Se revisaron las bitácoras de los sistemas de las instalaciones de ACME en Tegucigalpa, en busca de pistas o evidencias de eventos que pudieran comprometer la seguridad de los sistemas de información, acción que produjo resultados satisfactorios ya que no se encontró evidencia alguna o intento de penetración del atacante al menos de las direcciones IP mencionadas en el punto 5. Además se han hecho revisiones constantes de bitácoras en busca de actividades anormales e intentos de penetración en la red de ACME.

8. Se notifico mediante el envió de correo electrónico a las siguientes autoridades en la CNBS:
    a. Luis Lupiac Gerente de Informática
    b. Jeiky Tovar Sub Gerente de Informática

c. Manuel Luna Jefe de Auditoria

Esto en base al artículo 68 y 69 de la normativa de seguridad de la CNBS. (Anexo 6)

9. Se solicito la colaboración de una persona conocida a quien le llego el correo electrónico de forma directa. Ello con el fin de determinar mediante la cabecera del mensaje el remitente real del correo electrónico. En los datos arrojados mediante esta investigación vuelve a aparecer la dirección IP 204.249.101.134. (Anexo 4)

10. Se notifico al personal de la institución acerca del incidente y se explico de forma breve, clara y concisa las posibles razones por las cuales había ocurrido incidente. Esta notificación con el consentimiento de la Gerencia General.

Conclusiones

Debido a la falta de controles de seguridad en la sección especial para administrar la página web, los posibles mecanismos utilizados por el intruso para acceder a la pagina web pueden ser varios; sin embargo y con base en el análisis de las bitácoras del sistema generadas por la empresa WSI, se puede determinar que:

- El atacante obtuvo el usuario y contraseña mediante un programa conocido como sniffer que realiza la función de interceptar el tráfico entrante o saliente de un dispositivo (servidor, router, computadora, etc.) cuando este pasa de forma clara. Es decir que de haber existido un certificado de seguridad web en la sección administrativa esta opción se descartaría.

- El atacante pudo haber utilizado un programa para adivinar la contraseña administrativa de la pagina web comúnmente conocido como ataque de diccionario. Esto debido a que la contraseña era muy débil y fácil de adivinar, carecía de los componentes que vuelven robusta una contraseña.
  Además la sección administrativa no tenía un control de tal forma que bloqueara la aplicación después de un número determinado de intentos fallidos (3), es decir que el atacante pudo intentar una y otra vez hasta encontrar la contraseña.

Recomendaciones

Se hace énfasis en las recomendaciones sugeridas en la comunicación del día 17 de octubre de 2008, las cuales indican lo siguiente:

- La página web de la institución debe estar en una ubicación especial de la red interna de Empresa ACME de manera tal que se puedan implementar los controles físicos y lógicos necesarios y que la administración dependa totalmente del Departamento de Informática.
- La contratación de los servicios profesionales por entes especializados en ethical haching para realizar las pruebas de penetración y análisis de vulnerabilidades desde la red interna y desde la web (red externa) y de esta manera reducir al mínimo la posibilidad a otro incidente.

Además de ello y para evitar la amenaza de suplantación de identidad (spoofing) ya sea mediante correo electrónico, pagina web, DNS, direcciones IP y otros medios, se están realizando las investigaciones necesarias para contrarrestar estas amenazas, que conllevan la implementación de controles técnicos distintos y que deben estar acordes a nuestra infraestructura física y lógica.
Una vez hechas las investigaciones se recomendaran las medidas necesarias y así evitar que personas o compañías de forma malintencionada pretendan usar la identidad de Empresa ACME para hacer daño o cualquier tipo de acción que atente contra la ética humana.

Administrador de Seguridad Informática

Anexos

1. Correo electrónico enviado a clientes

Esta es uno de los correos electrónicos que fue enviado varias personas entre las que coinciden algunos clientes de la institución.

From: ggerencia@acme.co
Sent: Miércoles, 15 de Octubre de 2008 12:04 a.m.
To: clientes
Subject: - NUESTROS CLIENTES

si no puede ver esta imagen haga clic AQUI

Este es un correo se lo envia la gerencia de ":
ha sido enviado a la direccion
Si desea ser removido de esta lista MALA SUERTE.. no puede porque s una Mierda:

7

2. Bitácoras de Walt Disney Hosting

Esta información fue extraída de las bitácoras de acceso a la página web donde:

- Como primera evidencia se puede observar la acción del cambio de password desde dirección IP 204.249.101.134.

```
2008-10-14 15:50:25 W3SVC5190 WEB007 204.92.106.7 GET /ATMT40UC/admin/tmt_changepwd.asp - 80 - 204.249.101.134 HTTP/1.1
Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US)+AppleWebKit/525.13+(KHTML,+like+Gecko)+Chrome/0.2.149.30+Safari/525.13
segurosACMELanguageID=1;+__utmz=224250441.1221238655.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none);+ASPSESSIONIDASBD
DADB=HIHHEHECJEIGNBONCGKADNGL;+__utma=224250441.1016713574.1221238655.1221238655.1223998778.2;+__utmc=224250441;+__utmb=
224250441 http://www.ACME.com/ATMT40UC/admin/leftnav.asp?lm=4 www.ACME.com 302 0 0 369 755 812
```

- Como segunda evidencia se muestra el acceso a la aplicación admin_gallery que es usada para hacer cambios en las imágenes de la página web, acceso que solo puede ser realizado mediante el usuario admin y la contraseña para el personal autorizado. En este punto se vuelve a observar que esta aplicación fue utilizada desde dirección IP 204.249.101.134.

```
2008-10-14 17:25:48 W3SVC5190 WEB007 204.92.106.7 GET /ATMT40UC/admin/admin_Gallery.asp - 80 - 204.249.101.134 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322;+.NET+CLR+2.0.50727;+InfoPath.2)
ASPSESSIONIDASBDDADB=GLHHEHECDEHBACCIEKFJBEAP;+ASPSESSIONIDCQABBCCA=NKANLDGCEDGEPEJGHECKPBCM
http://www.ACME.com/ATMT40UC/admin/admin_Gallery.asp?action=addimage www.ACME.com 200 0 0 3895 492 562
```

- Finalmente se muestra la adición de la imagen ACME.jpg desde dirección IP 204.249.101.134.

```
2008-10-14 17:25:51 W3SVC5190 WEB007 204.92.106.7 GET /ATMT40UC/DynamicData/ImagesUploaded/ACME.jpg - 80 -
204.249.101.134 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322;+.NET+CLR+2.0.50727;+InfoPath.2)
ASPSESSIONIDASBDDADB=GLHHEHECDEHBACCIEKFJBEAP;+ASPSESSIONIDCQABBCCA=NKANLDGCEDGEPEJGHECKPBCM
http://www.ACME.com/ATMT40UC/admin/admin_Gallery.asp www.ACME.com 200 0 0 58853 472 2687
```

3. Correo electrónico enviado a clientes en la actualidad

Esta es la forma en la que se visualiza el correo electrónico enviado a nuestros clientes en la actualidad. Nótese que no se muestra ninguna imagen sin embargo la leyenda al final del mensaje electrónico continua.

4. Cabecera del correo electrónico original

Esta cabecera fue obtenida gracias a la colaboración de Darwin Incognito encargado de aplicaciones de la empresa Grupo NovoMundo, a quien le llego el mensaje de forma directa.

```
Return-Path: <mezcla@ferrari.websitewelcome.com>
X-Original-To: dIncognito@NovoMundo.hn
Delivered-To: dIncognito@NovoMundo.hn
Received:    from    gateway14.websitewelcome.com    (gateway14.websitewelcome.com
[67.18.71.9])
           by gtisatgu.NovoMundo.hn (Postfix) with SMTP id ECDFC605284
           for <dIncognito@NovoMundo.hn>; Wed, 15 Oct 2008 10:29:14 -0600 (CST)
Received: (qmail 5261 invoked from network); 15 Oct 2008 16:45:19 -0000
Received: from ferrari.websitewelcome.com (67.18.54.176)
  by gateway14.websitewelcome.com with SMTP; 15 Oct 2008 16:45:19 -0000
Received: from mezcla by ferrari.websitewelcome.com with local (Exim 4.68)
           (envelope-from <mezcla@ferrari.websitewelcome.com>)
           id 1Kq9FI-0003Ry-9Z
           for dIncognito@NovoMundo.hn; Wed, 15 Oct 2008 11:29:12 -0500
To: dIncognito@NovoMundo.hn
Subject: EMPRESA ACME - NUESTROS CLIENTES
X-PHP-Script: www.mezclamusic.com/admin/cron.php for 204.249.101.134
MIME-Version: 1.0
Content-Type: text/html; charset="ISO-8859-1"
From: EMPRESA ACME <ggerencia@ACME.com>
Reply-To: ggerencia@ACME.com
X-Sender: EMPRESA ACME <ggerencia@ACME.com>
X-Priority: 3
Date: Wed, 15 Oct 2008 11:29:12 -0500 (CDT)
Message-ID: <5d677bad545207075fe88ec3a351ee26>@ACME.com
Organization: EMPRESA ACME
X-AntiAbuse: This header was added to track abuse, please include it with any
abuse report
X-AntiAbuse: Primary Hostname - ferrari.websitewelcome.com
X-AntiAbuse: Original Domain - NovoMundo.hn
X-AntiAbuse: Originator/Caller UID/GID - [34760 34763] / [47 12]
X-AntiAbuse: Sender Address Domain - ferrari.websitewelcome.com
X-NOVOMUNDO-MailScanner-Information: Please contact the ISP for more information
X-NOVOMUNDO-MailScanner: Found to be clean
X-NOVOMUNDO-MailScanner-SpamScore: ssss
X-NOVOMUNDO-MailScanner-From: mezcla@ferrari.websitewelcome.com
X-Spam-Status: No
```

5. Correo electrónico enviado a gerentes.

Este es el mensaje que fue enviado a algunos de los gerentes de la institución.

----- Original Message -----
From: White Boxes
To: agraciacar@ACME.hn ; petrikliombio@ACME.hn ; ggerencia@ACME.hn
Sent: Wednesday, October 15, 2008 11:14 AM
Subject: ¿Les gusto?

Les gusto el mensajito?

bueno sigan tratando mal a los clientes..
y veran la informacion muy interesante que encontre en uno de sus servidores....
otras empresas me darian mucho dinero por ellas, pero si vuelvo a ir y me tratan mal como lo hicieron la semana pasada.. creame se las enviare a todas de gratis jeje

ahh otra cosa.. hoy que juega la seleccion, no tengo mucho que hacer asi que cuando heche un gol cualquier equipo
algo pasara con su sitio web..

esten pendientes.

saludos

6. Notificación a la Comisión Nacional de Banca y Seguros

Este es el correo electrónico que se envió a las autoridades correspondientes de la CNBS. En la normativa de seguridad, en el artículo 69 hace mención de que este tipo de incidentes deberán ser registrados en una sección especial en la interconexión financiera, sin embargo esta sección aun no esta disponible, por lo que esta comunicación cumple con los artículos 68 y 69 según se constato mediante conversación telefónica con el Sr. Manuel Luna Jefe de Auditoria.

7. **Comunicaciones a la Gerencia General**

COMUNICACIÓN INTERNA

13

6.2 ENCUESTAS APLICADAS

GERENTES DE TI, AUDITORES DE SISTEMAS, GERENTES SEGURIDAD INFORMATICA

UNITEC Facultad de Postgrado Proyecto Tesis, Máster en:"Gestión de Tecnologías de la Información"

Dirigida a: Gerentes TI, Oficiales de Seguridad de la Información y Auditores

Objetivo: Conocer su opinión sobre la informática forense en la aplicación de sus funciones para la resolución de casos delictivos que involucran componentes tecnológicos.

Nota: La información recolectada es confidencial y será utilizada para nuestra investigación sobre "Factores que Afectan la aplicación de Informática Forense en casos delictivos".

*Obligatorio

1. **1. ¿Conoce usted o ha escuchado hablar sobre informática forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

2. **2. ¿Tiene conocimientos sobre derecho informático?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

3. **Si su respuesta es Sí a la pregunta N° 2. Marque la casilla que mejor represente su conocimiento. Si su respuesta es No, pase a la pregunta N° 3**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

4. **3. ¿Sabe que delitos informáticos son tipificados como tal?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

5. **Si su respuesta es Sí a la pregunta N° 3. Marque la casilla que mejor represente su conocimiento. Si su respuesta es No, pase a la pregunta N° 4**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

6. **4. ¿Ha recibido capacitación sobre informática forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

7. **Si su respuesta es Sí a la pregunta N° 4. Indique donde la recibió. Si su respuesta es No, pase a la pregunta N° 6**
   Selecciona todos los que correspondan.
   - ☐ Dentro del país
   - ☐ Fuera del país
   - ☐ Autodidacta

8. **5. ¿Cuál fue el curso más relevante que recibió?**

   .....

   .....

   .....

   .....

9. **6. ¿Estaría interesado en recibir capacitación sobre el Informática Forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

10. **7. ¿Conoce si en el país existen leyes que hacen referencia a delitos informáticos?** *
    Marca solo un óvalo.
    - ◯ Sí
    - ◯ No

11. **Si su respuesta es Sí a la pregunta N° 7. Especifique que ley o leyes conoce. Si su respuesta es No, pase a la pregunta N° 8**

    .....

    .....

    .....

12. **8. ¿Tiene conocimiento sobre las buenas prácticas relacionadas con Informática Forense?** *
    Marca solo un óvalo.
    - ◯ Sí
    - ◯ No

13. **Si su respuesta es Sí a la pregunta N° 8. Marque la casilla que mejor represente su conocimiento. Si su respuesta es No, pase a la pregunta N° 9**
Marca solo un óvalo.

- ◯ Principiante
- ◯ Medio
- ◯ Experto

14. **9. ¿En su empresa han sido víctimas de algún tipo de delito informático? *En caso que su respuesta sea sí, favor continúe con la pregunta 10, si su respuesta es No ó No sé finaliza la encuesta.** *
Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No sé

15. **10. El hecho delictivo, ¿fue reportado a las autoridades del gobierno?**
Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No sé

16. **11. El hecho delictivo, ¿fue judicializado?**
Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No sé

17. **12. ¿En caso de haber sufrido algún delito, la investigación forense la hicieron a nivel interno o con personal externo (Ministerio Público, organización privada de investigación, bufetes especializados en delitos informáticos, entre otros)?**
Selecciona todos los que correspondan.

- ☐ Nivel Interno
- ☐ Nivel Externo
- ☐ No sé
- ☐ Otro (Especifique)

18. **Especifique "Otra" de la pregunta N° 12**

.....

Si su respuesta a la pregunta N° 12 fue "Nivel Interno" responda las siguiente preguntas, de lo contrario pase a la pregunta N° 17

19. **13. ¿Usted participo en la investigación? Si su respuesta es Sí continúe con la pregunta N ° 14, si su respuesta es No, pase a la pregunta N° 17.**
Marca solo un óvalo.

- ◯ Sí
- ◯ No

20. **14. ¿Qué herramientas utilizaron en la investigación?**
Selecciona todos los que correspondan.

- ☐ Encase
- ☐ Caine
- ☐ Cellebrite
- ☐ Bulk Extractor
- ☐ Digital Forensic Framework
- ☐ Otra (Especifique)

21. **Especifique "Otra" de la pregunta N° 14**

.....

.....

.....

.....

22. **15. ¿Qué metodología de investigación fue utilizada?**
Selecciona todos los que correspondan.

- ☐ Casey, E
- ☐ Palmer, G
- ☐ Reith, M.; Carr, C.; Gunsch, G
- ☐ Carrier, B.; Spafford, E.H.
- ☐ Baryamureeba, V.; Tushabe, F.
- ☐ Otra (Especifique)

23. **Especifique "Otra" de la pregunta N° 15**

.....

.....

.....

.....

24. **16. ¿Cuáles fueron las limitantes para realizar la investigación?**
Selecciona todos los que correspondan.

- [ ] Herramientas de hardware
- [ ] Herramientas de software
- [ ] Personal poco capacitado
- [ ] Recursos económicos
- [ ] Tiempo
- [ ] Otra (Especifique)

25. **Especifique "Otra" de la pregunta N° 16**

.....

26. **17. ¿Ha sufrido la empresa pérdidas monetarias o de reputación por causa de delitos informáticos?**
Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No sé

PROFESIONALES DE SISTEMAS Y DERECHO

UNITEC Facultad de Postgrado Proyecto Tesis, Máster en:"Gestión de Tecnologías de la Información"

Dirigida a: Profesionales de Informática, Sistemas y Derecho

Objetivo: Conocer su opinión sobre la informática forense en la aplicación de sus funciones para la resolución de casos delictivos que involucran componentes tecnológicos.

Nota: La información recolectada es confidencial y será utilizada para nuestra investigación sobre "Factores que Afectan la aplicación de Informática Forense en casos delictivos".

*Obligatorio

1. **1. ¿Conoce usted o ha escuchado hablar sobre informática forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

2. **Si su respuesta es Sí a la pregunta N° 1. Marque la casilla que mejor represente su conocimiento. Si su respuesta es No, pase a la pregunta N° 2**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

3. **2. ¿Tiene conocimientos sobre derecho informático?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

4. **Si su respuesta es Sí a la pregunta N° 2. Marque la casilla que mejor represente su conocimiento. Si su respuesta es No, pase a la pregunta N° 3**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

5. **3. ¿Sabe que delitos informáticos son tipificados como tal?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

6. **Si su respuesta es Sí a la pregunta N° 3. Marque la casilla que mejor represente su conocimiento. Si su respuesta es No, pase a la pregunta N° 4**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

7. **4. ¿Ha recibido capacitación sobre informática forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

8. **Si su respuesta es Sí a la pregunta N° 4. Indique donde la recibió. Si su respuesta es No, pase a la pregunta N° 6**
   Selecciona todos los que correspondan.
   - ☐ Dentro del país
   - ☐ Fuera del país
   - ☐ Autodidacta

9. **5. ¿Cuál fue el curso más relevante que recibió?**

10. **6. ¿Estaría interesado en recibir capacitaciones sobre la Informática Forense?** *
Marca solo un óvalo.
- ◯ Sí
- ◯ No

11. **7. ¿Conoce si en el país existen leyes que hacen referencia a delitos informáticos?** *
Marca solo un óvalo.
- ◯ Sí
- ◯ No

12. **Si su respuesta es Sí a la pregunta N° 7. Especifique que ley o leyes conoce. Si su respuesta es No, pase a la pregunta N° 8**

13. **8. ¿Tiene conocimiento sobre las buenas prácticas relacionadas con Informática Forense?** *
Marca solo un óvalo.
- ◯ Sí
- ◯ No

14. **9. ¿Qué ciencias u otras áreas de la informática considera necesarias para resolver un caso delictivo que involucre componentes tecnológicos?** *
Selecciona todos los que correspondan.
- ☐ Base de datos
- ☐ Redes
- ☐ Software
- ☐ Hardware
- ☐ Leyes
- ☐ Recuperación de archivos
- ☐ Criptografía
- ☐ Otros (Especifique)

15. **Especifique "Otra" de la pregunta N° 9**

16. **10. ¿Cuales son los factores que considera usted que afectan la adecuada aplicación de la Informática Forense en actos delictivos?** *

PERSONAL TECNICO / INVESTIGADORES

UNITEC Facultad de Postgrado Proyecto Tesis, Máster en:"Gestión de Tecnologías de la Información"

Dirigida a: Personal Técnico de Investigación

Objetivo: Conocer su opinión sobre la informática forense en la aplicación de sus funciones para la resolución de casos delictivos que involucran componentes tecnológicos.

Nota: La información recolectada es confidencial y será utilizada para nuestra investigación sobre "Factores que Afectan la aplicación de Informática Forense en casos delictivos".

*Obligatorio

1. **1. ¿Cuenta con estudios en el campo de informática?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

2. **2. ¿Ha recibido capacitación relacionada con Informática Forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

3. **Si su respuesta fue Sí a la pregunta N° 2. Indique donde la recibió. Si su respuesta fue No, pase a la pregunta N° 4**
   Selecciona todos los que correspondan.
   - ☐ Dentro del país
   - ☐ Fuera del país
   - ☐ Autodidacta

4. **3. ¿Cuál fue el curso más relevante que recibió acerca de Informática Forense?**

   .....
   .....
   .....

5. **4. ¿Como definiría su nivel de conocimiento en Informática Forense?** *
   Marca solo un óvalo.
   - ◯ Nulo
   - ◯ Principiante
   - ◯ Intermedio
   - ◯ Experto

6. **5. ¿Estaría interesado en recibir capacitación sobre Informática Forense, Delitos Informáticos y/o Evidencia Digital?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

7. **6. ¿Conoce que leyes nacionales se aplican en casos de delitos informáticos?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

8. **Si su respuesta fue Sí a la pregunta N° 6. Especifique que ley o leyes conoce. Si su respuesta fue No, pase a la pregunta N° 7**

   .....
   .....
   .....

   .....

9. **7. ¿Tiene conocimiento sobre las buenas prácticas relacionadas con la informática forense?** *
   Marca solo un óvalo.
   - Sí
   - No

10. **Si su respuesta es Sí a la pregunta N° 7. Indique las buenas prácticas que conoce. Si su respuesta es No, pase a la pregunta N° 8**

11. **8. ¿Conoce herramientas de hardware y software para realizar investigaciones aplicando Informática Forense?** *
    Marca solo un óvalo.
    - Sí
    - No

12. **Si su respuesta fue Sí a la pregunta N° 8. Indique las herramientas de hardware y software que conoce. Si su respuesta es No, pase a la pregunta N° 9**

13. **9. En las investigaciones periciales ¿Se aplica o conoce algún tipo de metodología?** *
    Marca solo un óvalo.
    - Sí
    - No

14. **Si su respuesta es Sí a la pregunta N° 9. Indique la metodología que ha aplicado. Si su respuesta es No, pase a la pregunta N° 10**

15. **10. ¿El proceso de la investigación se lleva a cabo de manera tal que pueda asegurarse la integridad de las pruebas y cumpliendo con todo lo establecido en el mismo?** *
    Marca solo un óvalo.
    - Sí
    - No

16. **11. ¿Conoce los cuidados que debe tener la cadena de custodia para mantener su valor como evidencia?** *
    Marca solo un óvalo.
    - Sí
    - No

17. **13. ¿Sabe que delitos informáticos son tipificados como tal?** *
    Marca solo un óvalo.
    - Sí
    - No

18. **14. ¿Qué ciencias u otras áreas de la informática considera necesarias para resolver un caso delictivo que involucre componentes tecnológicos?** *

Selecciona todos los que correspondan.

- [ ] Base de datos
- [ ] Redes
- [ ] hardware
- [ ] Leyes
- [ ] Recuperación de archivos
- [ ] Criptografía
- [ ] Otros (Especifique)

19. **Especifique "Otros" de la pregunta N° 14**

.....

.....

.....

.....

20. **15. ¿Cuales son los factores que considera usted que afectan la adecuada aplicación de la Informática Forense en las investigaciones periciales de actos delictivos?** *

.....

.....

.....

.....

.....

21. **16. ¿Se cuenta en el país con instalaciones adecuadas para realizar investigaciones forenses del campo informático?** *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No sé

22. **17. ¿Se cuenta con los recursos necesarios/suficientes para llevar a cabo las investigaciones de índole informático?** *

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ No sé

23. **18. ¿Que características considera usted debe tener un auditor que lleve a cabo investigaciones de informática forense?** *

Selecciona todos los que correspondan.

- [ ] Apasionado de la tecnología y respetuoso de ella.
- [ ] Ser una persona paciente
- [ ] Gusto por la investigación
- [ ] Analítico
- [ ] Facilidad de comunicación
- [ ] Persuasivo
- [ ] Capacidad de negociación
- [ ] Otros

24. **Especifique "Otros" de la pregunta N° 18**

.....

POBLACIÓN GENERAL

UNITEC Facultad de Postgrado Proyecto Tesis, Máster en:"Gestión de Tecnologías de la Información"

Dirigida a: Población en General

Objetivo: Recabar información sobre el conocimiento que la población en general tiene acerca de informática forense y derecho informático.

Nota: La información recolectada es confidencial y será utilizada para nuestra investigación sobre "Factores que Afectan la aplicación de Informática Forense en casos delictivos".

*Obligatorio

1. **1. ¿Conoce usted o ha escuchado hablar sobre Informática Forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

2. **Si su respuesta a la pregunta N°1 fue Sí, favor indicar su nivel de conocimiento, si su respuesta fue No continúe con la pregunta N°2**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

3. **2. ¿Conoce usted o ha escuchado sobre Derecho Informático?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

4. **Si su respuesta a la pregunta N°2 fue Sí, favor indicar su nivel de conocimiento, si su respuesta fue No continúe con la pregunta N°3**
   Marca solo un óvalo.
   - ◯ Principiante
   - ◯ Medio
   - ◯ Experto

5. **3. ¿Sabe que delitos son tipificados como delitos informáticos?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

6. **Si su respuesta a la pregunta N° 3 fue Sí, favor indicar los delitos informáticos que conoce, si su respuesta fue No continúe con la pregunta N° 4**

   .....

   .....

   .....

7. **4. ¿Conoce si en el país existen leyes que hacen referencia a delitos informáticos?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

8. **Si su respuesta a la pregunta N°4 fue Sí, favor indicar las leyes que conoce, si su respuesta fue No continúe con la pregunta N°5**

   .....

   .....

   .....

   .....

9. **5. ¿Considera usted que en lo cotidiano podría ser víctima de un delito informático y requerir del uso de la informática forense?** *
   Marca solo un óvalo.
   - ◯ Sí
   - ◯ No

10. **¿Por qué? Por los avances informaticos**

11. **6. ¿Conoce a alguien que haya sido victima de delitos informáticos (Robo de información, robo o hurto de dinero mediante medios electrónicos, entre otros)** *
    Marca solo un óvalo.
    - ◯ Sí
    - ◯ No

Si su respuesta a la pregunta 6 fue Sí continúe con la pregunta 7, si su respuesta fue No, continúe con la pregunta 8

12. **7. ¿El delito fue denunciado, investigado y judicializado?**
    Selecciona todos los que correspondan.
    - ☐ Denunciado
    - ☐ Investigado
    - ☐ Judicializado
    - ☐ No sé

13. **8. ¿Considera que en Honduras estamos preparados para hacer frente a los delitos informáticos?** *
    Marca solo un óvalo.
    - ◯ Sí
    - ◯ No

14. **9. ¿En su opinión, Honduras cuenta con capacidad para aplicar correctamente la Informática Forense (Análisis Forense Tecnológico)?** *
    Marca solo un óvalo.
    - ◯ Sí
    - ◯ No

6.3 PLANES DE ESTUDIOS UNIVERSIDADES

UNIVERSIDAD NACIONAL AUTONOMA DE HONDURAS

PRIMER PERÍODO

Código	Asignatura	UV	Requisito
SC-101	Sociología	4	Ninguno
EG-011	Español General	4	Ninguno
FF-101	Filosofía	4	Ninguno
HH-100	Historia de Honduras	4	Ninguno
MM-100	Introducción a la Estadistica Social	4	Ninguno

SEGUNDO PERÍODO

Código	Asignatura	UV	Requisito
	Optativa Humanidades	3	Ninguno
	Optativa Ciencias Naturales	3	Ninguno
CDE-012	Met. Tec. Invest. e Informática	4	MM-100
CDE-022	Ética General.	3	FF-101
CDE-032	Lógica Jurídica	3	FF-101
CDE-042	Interpretación Jurídica	3	SC-101

TERCER PERÍODO

Código	Asignatura	UV	Requisito
	Optativa Lenguas Extranjeras	3	Ninguno
	Optativa arte o Deporte	3	Ninguno
CDE-053	Derecho Romano	4	CDE-012
CDE-063	Introducción al estudio de Derecho	5	CDE-022 CDE-032
CDE-073	Teoría General del Estado	4	CDE-042

CUARTO PERÍODO

Código	Asignatura	UV	Requisito
CDE-084	Derecho de Familia	3	CDE-053
CDE-094	Teoría General del Proceso	4	CDE-063
CDE-104	Derecho Penal I	4	CDE-063
CDE-114	Teoría de la Constitución	4	CDE-073
CDE-124	Derecho Forestal y de aguas	4	CDE 063, 073

CUARTO PERÍODO

Código	Asignatura	UV	Requisito
CDE-135	Derecho Privado I (bienes)	4	CDE-084
CDE-145	Derecho Procesal civil I	4	CDE-094
CDE-155	Derecho Penal II	4	CDE-104
CDE-165	Derecho Niñez, Adolescente, Mujer	4	CDE-084
CDE-175	Historia Const. e Institu. Política	4	CDE 114

SEXTO PERÍODO

Código	Asignatura	UV	Requisito
CDE-186	Derecho Laboral I	4	CDE-175
CDE-206	Derecho Privado II (Sucesiones)	4	CDE-135
CDE-216	Derecho Procesal Civil II	4	CDE-145
CDE-226	Criminología	4	CDE-155
CDE-236	Derecho Constitucional	3	CDE-175
CDE-196	Derecho Intern. Público I	4	CDE-114

SÉPTIMO PERÍODO

Código	Asignatura	UV	Requisito
CDE-247	Derecho Ejecución Penal	3	CDE-226
CDE-257	Derecho Privado III (Teoría de la obligaciones)	5	CDE-206
CDE-267	Derecho Laboral II	4	CDE-186
Código	Asignatura	U.V	Requisitos
CDE-277	Derecho Inter. Público II	4	CDE-196
CDE-287	Derecho Administrativo I	4	CDE-236

OCTAVO PERÍODO

Código	Asignatura	UV	Requisito
CDE-298	Derecho Priv. IV (Teoría de los Contr.)	5	CDE-257
CDE-308	Medicina Forense	3	CDE-247
CDE-318	Derecho Mercantil I	4	CDE-257
CDE-328	Derecho Ambiental	4	CDE-287
CDE-338	Derecho seguridad social	4	CDE-267
CDE-348	Derecho Administrativo II	4	CDE-287

NOVENO PERÍODO

Código	Asignatura	UV	Requisito
CDE-359	Derecho Mercantil II	4	CDE-318
CDE-369	Derecho Agrario	3	CDE-287
CDE-379	Derecho Admin. Especial	4	CDE-348
CDE-389	Derecho de Integración	3	CDE-277
CDE-399	Derecho Laboral Especial	4	CDE-338
CDE-409	Derecho Humano y humanitario	4	CDE-277

NOVENO PERÍODO

Código	Asignatura	UV	Requisito
CDE-359	Derecho Mercantil II	4	CDE-318
CDE-369	Derecho Agrario	3	CDE-287
CDE-379	Derecho Admin. Especial	4	CDE-348
CDE-389	Derecho de Integración	3	CDE-277
CDE-399	Derecho Laboral Especial	4	CDE-338
CDE-409	Derecho Humano y humanitario	4	CDE-277

DÉCIMO PERÍODO

Código	Asignatura	UV	Requisito
CDE-4110	Derecho Internac. Privado	4	CDE-298
CDE-4210	Filosofía Derecho	4	CDE-298
CDE-4310	Derecho Notar. y registro inmob.	4	CDE-298
CDE-4410	Derecho Mercantil Especial	4	CDE-359
CDE-4510	Propiedad Intelectual	4	CDE-359

DÉCIMO PRIMER PERÍODO

Código	Asignatura	UV	Requisito
CDE-4611	Derecho Procesal Laboral	4	CDE-399
CDE-4711	Derecho Procesal Penal	4	CDE-308
CDE-4811	Justicia Administrativa.	4	CDE-379
CDE-4911	Ética Profesional	3	CDE-4210
	Seminario de investigación		Haber aprobado todas las asignaturas previas al último período académico.

Mediante Acuerdo CUO-010-02-2009, el Consejo Universitario reformó el orden en que debian aprobarse los módulos pero conservando los códigos de asignatura que tenian hasta el momento. A partir de dicha reforma los módulo ahora denominados Talleres o Laboratorios Jurídicos se organizan en pasantías con una duración temporal de siete semanas cada una.

DÉCIMO SEGUNDO PERÍODO

PASANTÍA A

CDE-5012	Taller de Práctica Procesal Civil	4
CDE-5413	Taller de Practica Procesal Laboral	4
CDE-5212	Taller de Criminalistica.	4

PASANTÍA B

CDE-5112	Taller de Práctica procesal penal	4
CDE-5513	Taller de Practica Procesal. Administ.	4
CDE-5613	Taller de Métodos Alternativos y Solucion de conflictos.	4

DÉCIMO SEGUNDO PERÍODO

PASANTÍA C

CDE-5713	Taller de Práctica Judicial Internacional.	4
CDE-5813	Modulo Derecho Notarial y Derecho Registral.	4
CDE-5312	Taller de Justicia Constitucional	4

PRACTICA FORENSE OBLIGATORIA

Requisito: haber aprobado todas las asignaturas profesionalizantes

PLAN DE ESTUDIOS
CARRERA EN DERECHO

www.unah.edu.hn

LUCEM ASPICIO

UNAH

PRIMER PERÍODO

Código	Asignatura	UV	Requisito
EG-011	Español	4	Ninguno
FF-101	Filosofía.	4	Ninguno
SC-101	Sociología.	4	Ninguno
DET-175	Métodos Cuantitativos I	5	Ninguno
EQ-025	Redacción General.	4	Ninguno

SEGUNDO PERÍODO

Código	Asignatura	UV	Requisito
IN-101	Ingles I	4	Ninguno
HH-101	Historia de Honduras	4	Ninguno
RR-150-170	Educación Artística ó	3	Ninguno
RR-171-190	Cultura física		
BI-130	Educación Ambiental.	3	Ninguno
IA-012	Introducción a la Informática	4	DET-175

TERCER PERÍODO

Código	Asignatura	UV	Requisito
DET-280	Métodos cuantitativos II.	5	DET-175
CF-014	Contabilidad I	4	DET-175
CE-020	Principios de Economía	4	DET-175
IA-023	Taller de Hardware I.	4	IA-012
IA-033	Metodología de la Programación	4	IA-012 DET-175

CUARTO PERÍODO

Código	Asignatura	UV	Requisito
DET-385	Métodos cuantitativos III.	5	DET-280
IA-044	Lenguaje de Programación I.	4	IA-033
CF-030	Métodos Cuantitativos en Finanzas	4	DET-280
DAE-300	Administración I.	4	SC-101
IA-054	Taller de Hardware II	4	IA-023

QUINTO PERÍODO

Código	Asignatura	UV	Requisito
IA-065	Lenguaje de Programación II	4	IA-044
IA-075	Sistemas Operativos I	4	IA-054
DAE-400	Administración II.	4	DAE-300
DET-395	Análisis Numérico en la informática	5	DET-385
CF-035	Contabilidad II.	5	CF-014

SEXTO PERÍODO

Código	Asignatura	UV	Requisito
IA-086	Lenguaje de Programación III	4	IA-065
IA-096	Sistemas Operativos II.	4	IA-075
DAE-610	Análisis Cuantitativo I.	4	DET-385
IA-106	Base de Datos I.	4	IA-065, IA-075
CE-240	Microeconomía	4	CE-020,DET-280

SEPTIMO PERÍODO

Código	Asignatura	UV	Requisito
IA-117	Lenguaje de Programación IV.	4	IA-086
IA-127	Teoría de Sistemas.	4	IA-086, IA-096
IA-137	Base de Datos II	4	IA-106
DAE-505	Contabilidad Administrativa I	4	CE-035

OCTAVO PERÍODO

Código	Asignatura	UV	Requisito
F-110	Finanzas de Empresas.	4	CF-035
IA-148	Comunicación Electrónica de Datos.	4	IA-096,IA-086
IA-158	Análisis y Diseño de Sistemas.	4	IA-117, IA-127, IA-137
IA-168	Recursos Humanos en Informática.	4	DAE-400
DAE-710	Análisis Cuantitativo II.	4	DAE-610

NOVENO PERÍODO

Código	Asignatura	UV	Requisito
IA-179	Redes de Computadoras.	4	IA-148
IA-189	Programación e Implementación de Sistemas.	4	IA-158
IA-199	Admón. .Publica y Política Informática.	4	IA-158
CE-075	Macroeconomía.	4	CE-040

DÉCIMO PERÍODO

Código	Asignatura	UV	Requisito
IA-200	Organización y Métodos en Informática.	4	IA-189
IA-210	Gerencia Informática I.	4	IA-179,IA-189
IA-220	Evaluación de Sistemas.	4	IA-189
DAE-605	Contabilidad Administrativa II.	4	DAE-505

DÉCIMO PRIMER PERÍODO

Código	Asignatura	UV	Requisito
A-231	Perspectiva de la Tecnología Informática.	4	IA-189
IA-241	Auditoria en Informática.	4	IA-220
IA-251	Gerencia Informática II.	4	IA-210
IA-261	Admón. y Evaluación de Proyectos en Informática.	4	IA-220
IA-271	Seminario de Investigación.	4	IA-220, IA-210, IA-200,DAE-605

Total Unidades Valorativas: 210

Total Asignaturas: 52

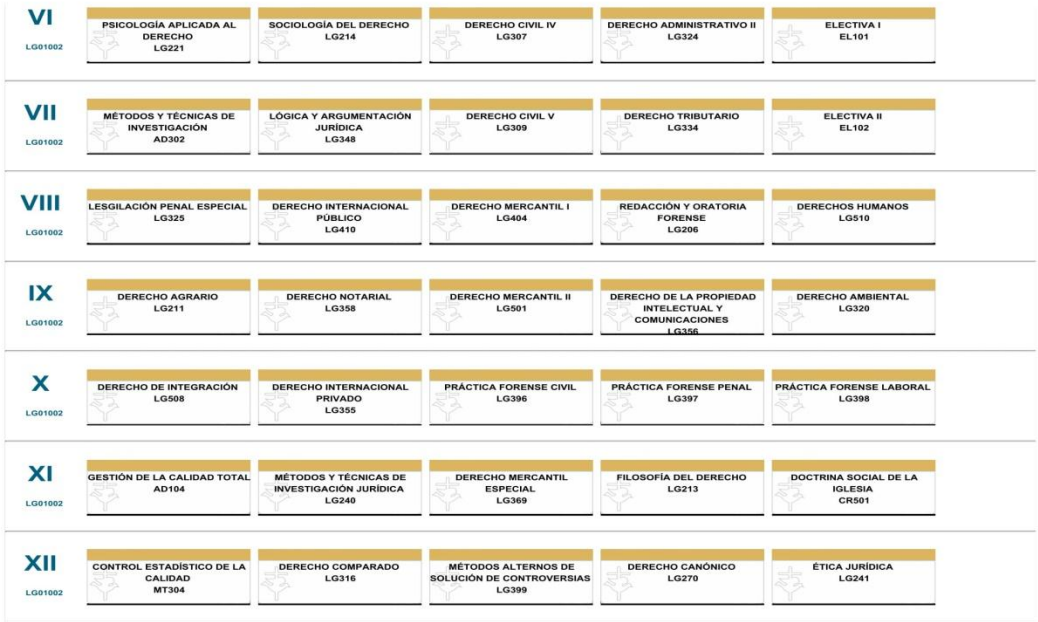
PLAN DE ESTUDIOS
CARRERA INFORMÁTICA ADMINISTRATIVA

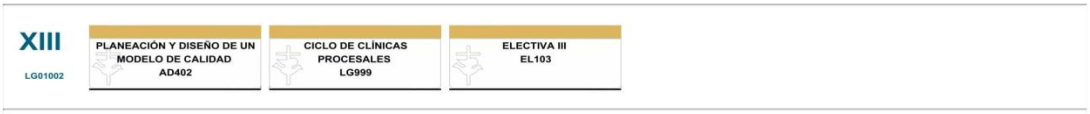
www.unah.edu.hn

LUCEM ASPICIO

UNAH
UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS

UNIVERSIDAD CATOLICA DE HONDURAS





Periodo I

Codigo	Materia	Creditos	Requisitos
MT101	MATEMÁTICAS	4	
SC101	SOCIOLOGÍA	3	
LG101	INTRODUCCIÓN AL ESTUDIO DEL DERECHO	3	
FI101	FILOSOFÍA	3	
ES101	ESPAÑOL	3	

Periodo II

Codigo	Materia	Creditos	Requisitos
MT202	ESTADÍSTICA I	4	MT101 MATEMÁTICAS
LG207	TEORÍA GENERAL DEL PROCESO	4	LG101 INTRODUCCIÓN AL ESTUDIO DEL DERECHO
LG204	DERECHO ROMANO	4	LG101 INTRODUCCIÓN AL ESTUDIO DEL DERECHO
LG212	TEORÍA POLÍTICA	4	SC101 SOCIOLOGÍA
ES201	EXPRESIÓN ORAL Y ESCRITA	3	ES101 ESPAÑOL

Periodo III

Codigo	Materia	Creditos	Requisitos
HS101	HISTORIA DE HONDURAS	3	
LG205	DERECHO PENAL I	4	LG101 INTRODUCCIÓN AL ESTUDIO DEL DERECHO
LG303	DERECHO CIVIL I	4	LG204 DERECHO ROMANO
LG308	TEORÍA DEL ESTADO	3	LG212 TEORÍA POLÍTICA
LG209	DERECHO DEL TRABAJO Y SEGURIDAD SOCIAL I	3	LG101 INTRODUCCIÓN AL ESTUDIO DEL DERECHO

Periodo IV

Codigo	Materia	Creditos	Requisitos
LG306	DERECHO PROCESAL CIVIL I	4	LG207 TEORÍA GENERAL DEL PROCESO
LG305	DERECHO PENAL II	4	LG205 DERECHO PENAL I
LG402	DERECHO CIVIL II	4	LG303 DERECHO CIVIL I
LG318	DERECHO CONSTITUCIONAL	4	LG308 TEORÍA DEL ESTADO
LG310	DERECHO DEL TRABAJO Y SEGURIDAD SOCIAL II	3	LG209 DERECHO DEL TRABAJO Y SEGURIDAD SOCIAL I

Periodo V

Codigo	Materia	Creditos	Requisitos
LG317	DERECHO PROCESAL CIVIL II	4	LG306 DERECHO PROCESAL CIVIL I
LG414	DERECHO DE LA NIÑEZ Y LA MUJER	4	LG303 DERECHO CIVIL I
LG304	DERECHO CIVIL III	4	LG402 DERECHO CIVIL II
LG314	DERECHO ADMINISTRATIVO I	4	LG308 TEORÍA DEL ESTADO
CR201	EL HOMBRE FRENTE A LA VIDA	3	FI101 FILOSOFÍA

Periodo VI

Codigo	Materia	Creditos	Requisitos
LG221	PSICOLOGÍA APLICADA AL DERECHO	3	
LG214	SOCIOLOGÍA DEL DERECHO	3	SC101 SOCIOLOGÍA
LG307	DERECHO CIVIL IV	4	LG304 DERECHO CIVIL III
LG324	DERECHO ADMINISTRATIVO II	4	LG314 DERECHO ADMINISTRATIVO I
EL101	ELECTIVA I	3	

Periodo VII

Codigo	Materia	Creditos	Requisitos
AD302	MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN	3	MT202 ESTADÍSTICA I
LG348	LÓGICA Y ARGUMENTACIÓN JURÍDICA	3	LG307 DERECHO CIVIL IV
LG309	DERECHO CIVIL V	4	LG307 DERECHO CIVIL IV
LG334	DERECHO TRIBUTARIO	3	LG324 DERECHO ADMINISTRATIVO II
EL102	ELECTIVA II	3	

Periodo VIII

Codigo	Materia	Creditos	Requisitos
LG325	LESGILACIÓN PENAL ESPECIAL	3	LG305 DERECHO PENAL II
LG410	DERECHO INTERNACIONAL PÚBLICO	3	LG308 TEORÍA DEL ESTADO
LG404	DERECHO MERCANTIL I	3	LG309 DERECHO CIVIL V

LG206	REDACCIÓN Y ORATORIA FORENSE	3	LG402 DERECHO CIVIL II
LG510	DERECHOS HUMANOS	3	LG318 DERECHO CONSTITUCIONAL

Periodo IX

Codigo	Materia	Creditos	Requisitos
LG211	DERECHO AGRARIO	3	LG324 DERECHO ADMINISTRATIVO II
LG358	DERECHO NOTARIAL	4	LG404 DERECHO MERCANTIL I
LG501	DERECHO MERCANTIL II	3	LG404 DERECHO MERCANTIL I
LG356	DERECHO DE LA PROPIEDAD INTELECTUAL Y COMUNICACIONES	3	LG404 DERECHO MERCANTIL I
LG320	DERECHO AMBIENTAL	3	LG510 DERECHOS HUMANOS

Periodo X

Codigo	Materia	Creditos	Requisitos
LG508	DERECHO DE INTEGRACIÓN	3	LG410 DERECHO INTERNACIONAL PÚBLICO
LG355	DERECHO INTERNACIONAL PRIVADO	4	LG410 DERECHO INTERNACIONAL PÚBLICO
LG396	PRÁCTICA FORENSE CIVIL	4	LG309 DERECHO CIVIL V LG317 DERECHO PROCESAL CIVIL II
LG397	PRÁCTICA FORENSE PENAL	3	LG305 DERECHO PENAL II LG317 DERECHO PROCESAL CIVIL II
LG398	PRÁCTICA FORENSE LABORAL	3	LG310 DERECHO DEL TRABAJO Y SEGURIDAD SOCIAL II LG317 DERECHO PROCESAL CIVIL II

Periodo XI

Codigo	Materia	Creditos	Requisitos
AD104	GESTIÓN DE LA CALIDAD TOTAL	3	
LG240	MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN JURÍDICA	3	AD302 MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN
LG369	DERECHO MERCANTIL ESPECIAL	3	LG501 DERECHO MERCANTIL II
LG213	FILOSOFÍA DEL DERECHO	3	FI101 FILOSOFÍA
CR501	DOCTRINA SOCIAL DE LA IGLESIA	3	

Periodo XII

Codigo	Materia	Creditos	Requisitos
MT304	CONTROL ESTADÍSTICO DE LA CALIDAD	3	AD104 GESTIÓN DE LA CALIDAD TOTAL
LG316	DERECHO COMPARADO	3	LG355 DERECHO INTERNACIONAL PRIVADO

LG399	MÉTODOS ALTERNOS DE SOLUCIÓN DE CONTROVERSIAS	3	LG396 PRÁCTICA FORENSE CIVIL LG397 PRÁCTICA FORENSE PENAL LG398 PRÁCTICA FORENSE LABORAL
LG270	DERECHO CANÓNICO	3	LG213 FILOSOFÍA DEL DERECHO
LG241	ÉTICA JURÍDICA	3	LG213 FILOSOFÍA DEL DERECHO

Periodo XIII

Codigo	Materia	Creditos	Requisitos
AD402	PLANEACIÓN Y DISEÑO DE UN MODELO DE CALIDAD	3	MT304 CONTROL ESTADÍSTICO DE LA CALIDAD
LG999	CICLO DE CLÍNICAS PROCESALES	8	
EL103	ELECTIVA III	3	

Universidad Católica de Honduras
"Nuestra Señora Reina de la Paz"

INGENÍERIA EN CIENCIAS DE LA COMPUTACIÓN

I IG03002	ESPAÑOL ES101	MATEMÁTICAS MT101	PRINCIPIOS DE COMPUTACIÓN IF103	SOCIOLOGÍA SC101	FILOSOFÍA FI101
II IG03002	EXPRESIÓN ORAL Y ESCRITA ES201	PRE- CÁLCULO MT201	ALGORÍTMOS Y DIAGRAMACIÓN IF205	LÓGICA FORMAL FI203	EL HOMBRE FRENTE A LA VIDA CR201
III IG03002	ADMINISTRACIÓN I AD101	CÁLCULO I MT303	PROGRAMACIÓN ESTRUCTURADA I IF317	CIENCIA Y TECNOLOGÍA FI102	CONTABILIDAD I CT201
IV IG03002	ESTADÍSTICA I MT202	CÁLCULO II MT401	FÍSICA I FS201	PROGRAMACIÓN ESTRUCTURADA II IF413	CONTABILIDAD DE COSTOS PARA INGENIERÍA CT304
V IG03002	DISEÑO GRÁFICO IF318	ÁLGEBRA LINEAL MT301	FÍSICA II FS301	BASE DE DATOS I IF104	MATEMÁTICA FINANCIERA MT204
VI IG03002	INVESTIGACIÓN DE OPERACIONES APLICADAS A LA ADMINISTRACIÓN PR408	ANÁLISIS Y DISEÑO DE SISTEMAS IF206	PRINCIPIOS DE ELECTRÓNICA IF414	BASE DE DATOS II IF207	ADMINISTRACIÓN FINANCIERA I FZ301
VII IG03002	ADMINISTRACIÓN DE SISTEMAS DE SOFTWARE IF313	DESARROLLO DE SOFTWARE IF314	CIRCUITOS LÓGICOS IF311	REDES I IF105	PROGRAMACIÓN CIENTÍFICA I IF106
VIII IG03002	PROGRAMACIÓN DE NEGOCIOS IF409	PRUEBA DOCUMENTACION E IMPLEMENTACIÓN DE SOFTWARE IF410	SISTEMAS OPERATIVOS I IF107	ARQUITECTURA DE COMPUTADORAS IF406	PROGRAMACIÓN CIENTÍFICA II IF208
IX IG03002	PSICOLOGÍA I PS101	HERRAMIENTAS TECNOLÓGICAS IF108	SISTEMAS OPERATIVOS II IF209	REDES II IF210	PROGRAMACIÓN ORIENTADA A OBJETOS IF315
X IG03002	GESTIÓN DE LA CALIDAD TOTAL AD104	SISTEMAS INTELIGENTES PARA NEGOCIOS IF211	SEMINARIO DE HARDWARE Y ELECTRICIDAD IF512	DESARROLLO DE PORTALES WEB IF316	INTELIGENCIA ARTIFICIAL IF411
XI IG03002	CONTROL ESTADÍSTICO DE LA CALIDAD MT304	HISTORIA DE HONDURAS HS101	ÉTICA PROFESIONAL FI501	NEGOCIOS WEB IF412	ADMINISTRACIÓN DE CENTROS DE COMPUTO IF310
XII IG03002	PLANEACIÓN Y DISEÑO DE UN MODELO DE CALIDAD AD402	AUDITORÍA DE SISTEMAS DE INFORMACIÓN IF109	DOCTRINA SOCIAL DE LA IGLESIA CR501	SEMINARIO DE SOFTWARE IF505	GESTIÓN DE PROYECTOS INFORMÁTICOS IF110

Periodo I

Codigo	Materia	Creditos	Requisitos
ES101	ESPAÑOL	3	
MT101	MATEMÁTICAS	4	
IF103	PRINCIPIOS DE COMPUTACIÓN	3	
SC101	SOCIOLOGÍA	3	
FI101	FILOSOFÍA	3	

Periodo II

Codigo	Materia	Creditos	Requisitos
ES201	EXPRESIÓN ORAL Y ESCRITA	3	ES101 ESPAÑOL
MT201	PRE- CÁLCULO	4	MT101 MATEMÁTICAS
IF205	ALGORÍTMOS Y DIAGRAMACIÓN	3	IF103 PRINCIPIOS DE COMPUTACIÓN
FI203	LÓGICA FORMAL	3	MT101 MATEMÁTICAS
CR201	EL HOMBRE FRENTE A LA VIDA	3	

Periodo III

Codigo	Materia	Creditos	Requisitos
AD101	ADMINISTRACIÓN I	3	
MT303	CÁLCULO I	4	MT201 PRE- CÁLCULO
IF317	PROGRAMACIÓN ESTRUCTURADA I	3	IF205 ALGORÍTMOS Y DIAGRAMACIÓN
FI102	CIENCIA Y TECNOLOGÍA	3	
CT201	CONTABILIDAD I	3	MT101 MATEMÁTICAS

Periodo IV

Codigo	Materia	Creditos	Requisitos
MT202	ESTADÍSTICA I	4	MT101 MATEMÁTICAS
MT401	CÁLCULO II	4	MT303 CÁLCULO I
FS201	FÍSICA I	3	MT101 MATEMÁTICAS
IF413	PROGRAMACIÓN ESTRUCTURADA II	3	IF317 PROGRAMACIÓN ESTRUCTURADA I
CT304	CONTABILIDAD DE COSTOS PARA INGENIERÍA	3	CT201 CONTABILIDAD I

Periodo V

Codigo	Materia	Creditos	Requisitos
IF318	DISEÑO GRÁFICO	3	
MT301	ÁLGEBRA LINEAL	3	MT201 PRE- CÁLCULO
FS301	FÍSICA II	3	FS201 FÍSICA I
IF104	BASE DE DATOS I	3	
MT204	MATEMÁTICA FINANCIERA	3	MT101 MATEMÁTICAS

Periodo VI

Codigo	Materia	Creditos	Requisitos
PR408	INVESTIGACIÓN DE OPERACIONES APLICADAS A LA ADMINISTRACIÓN	3	MT303 CÁLCULO I
IF206	ANÁLISIS Y DISEÑO DE SISTEMAS	3	IF104 BASE DE DATOS I
IF414	PRINCIPIOS DE ELECTRÓNICA	3	FS301 FÍSICA II
IF207	BASE DE DATOS II	3	IF104 BASE DE DATOS I
FZ301	ADMINISTRACIÓN FINANCIERA I	3	MT204 MATEMÁTICA FINANCIERA

Periodo VII

Codigo	Materia	Creditos	Requisitos
IF313	ADMINISTRACIÓN DE SISTEMAS DE SOFTWARE	3	IF206 ANÁLISIS Y DISEÑO DE SISTEMAS
IF314	DESARROLLO DE SOFTWARE	3	IF206 ANÁLISIS Y DISEÑO DE SISTEMAS IF207 BASE DE DATOS II
IF311	CIRCUITOS LÓGICOS	3	
IF105	REDES I	3	
IF106	PROGRAMACIÓN CIENTÍFICA I	3	

Periodo VIII

Codigo	Materia	Creditos	Requisitos
IF409	PROGRAMACIÓN DE NEGOCIOS	3	IF314 DESARROLLO DE SOFTWARE
IF410	PRUEBA DOCUMENTACION E IMPLEMENTACIÓN DE SOFTWARE	3	IF314 DESARROLLO DE SOFTWARE
IF107	SISTEMAS OPERATIVOS I	3	
IF406	ARQUITECTURA DE COMPUTADORAS	3	IF311 CIRCUITOS LÓGICOS
IF208	PROGRAMACIÓN CIENTÍFICA II	3	IF106 PROGRAMACIÓN CIENTÍFICA I

Periodo IX

Codigo	Materia	Creditos	Requisitos
PS101	PSICOLOGÍA I	3	
IF108	HERRAMIENTAS TECNOLÓGICAS	3	
IF209	SISTEMAS OPERATIVOS II	3	IF107 SISTEMAS OPERATIVOS I
IF210	REDES II	3	IF105 REDES I
IF315	PROGRAMACIÓN ORIENTADA A OBJETOS	3	IF208 PROGRAMACIÓN CIENTÍFICA II

Periodo X

Codigo	Materia	Creditos	Requisitos
AD104	GESTIÓN DE LA CALIDAD TOTAL	3	
IF211	SISTEMAS INTELIGENTES PARA NEGOCIOS	3	IF108 HERRAMIENTAS TECNOLÓGICAS
IF512	SEMINARIO DE HARDWARE Y ELECTRICIDAD	3	IF406 ARQUITECTURA DE COMPUTADORAS
IF316	DESARROLLO DE PORTALES WEB	3	IF208 PROGRAMACIÓN CIENTÍFICA II
IF411	INTELIGENCIA ARTIFICIAL	3	IF315 PROGRAMACIÓN ORIENTADA A OBJETOS

Periodo XI

Codigo	Materia	Creditos	Requisitos
MT304	CONTROL ESTADÍSTICO DE LA CALIDAD	3	AD104 GESTIÓN DE LA CALIDAD TOTAL MT202 ESTADÍSTICA I
HS101	HISTORIA DE HONDURAS	3	
FI501	ÉTICA PROFESIONAL	3	
IF412	NEGOCIOS WEB	3	IF316 DESARROLLO DE PORTALES WEB
IF310	ADMINISTRACIÓN DE CENTROS DE COMPUTO	3	

Periodo XII

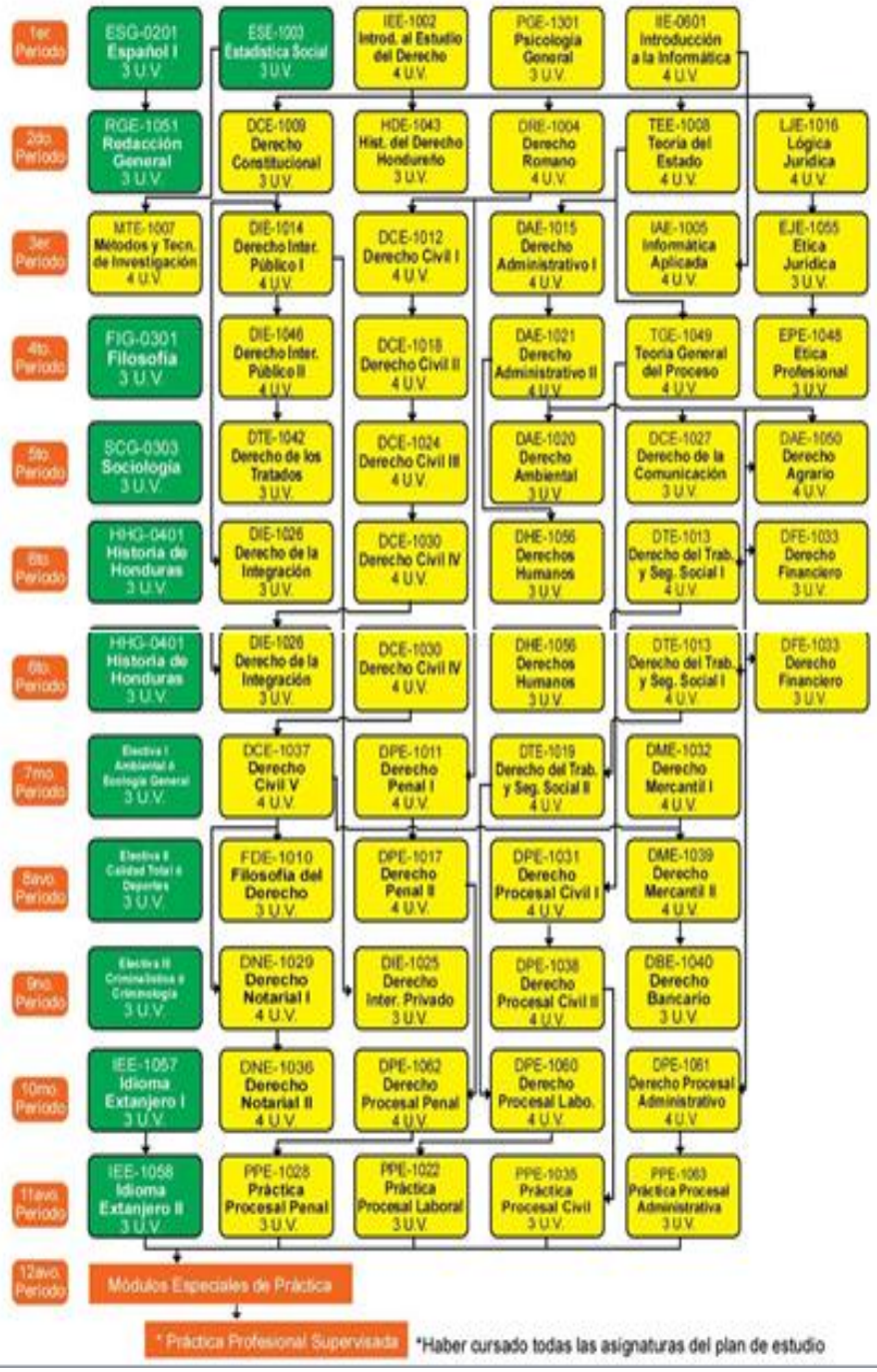
Codigo	Materia	Creditos	Requisitos
AD402	PLANEACIÓN Y DISEÑO DE UN MODELO DE CALIDAD	3	MT304 CONTROL ESTADÍSTICO DE LA CALIDAD
IF109	AUDITORÍA DE SISTEMAS DE INFORMACIÓN	3	
CR501	DOCTRINA SOCIAL DE LA IGLESIA	3	
IF505	SEMINARIO DE SOFTWARE	3	IF412 NEGOCIOS WEB
IF110	GESTIÓN DE PROYECTOS INFORMÁTICOS	3	

}

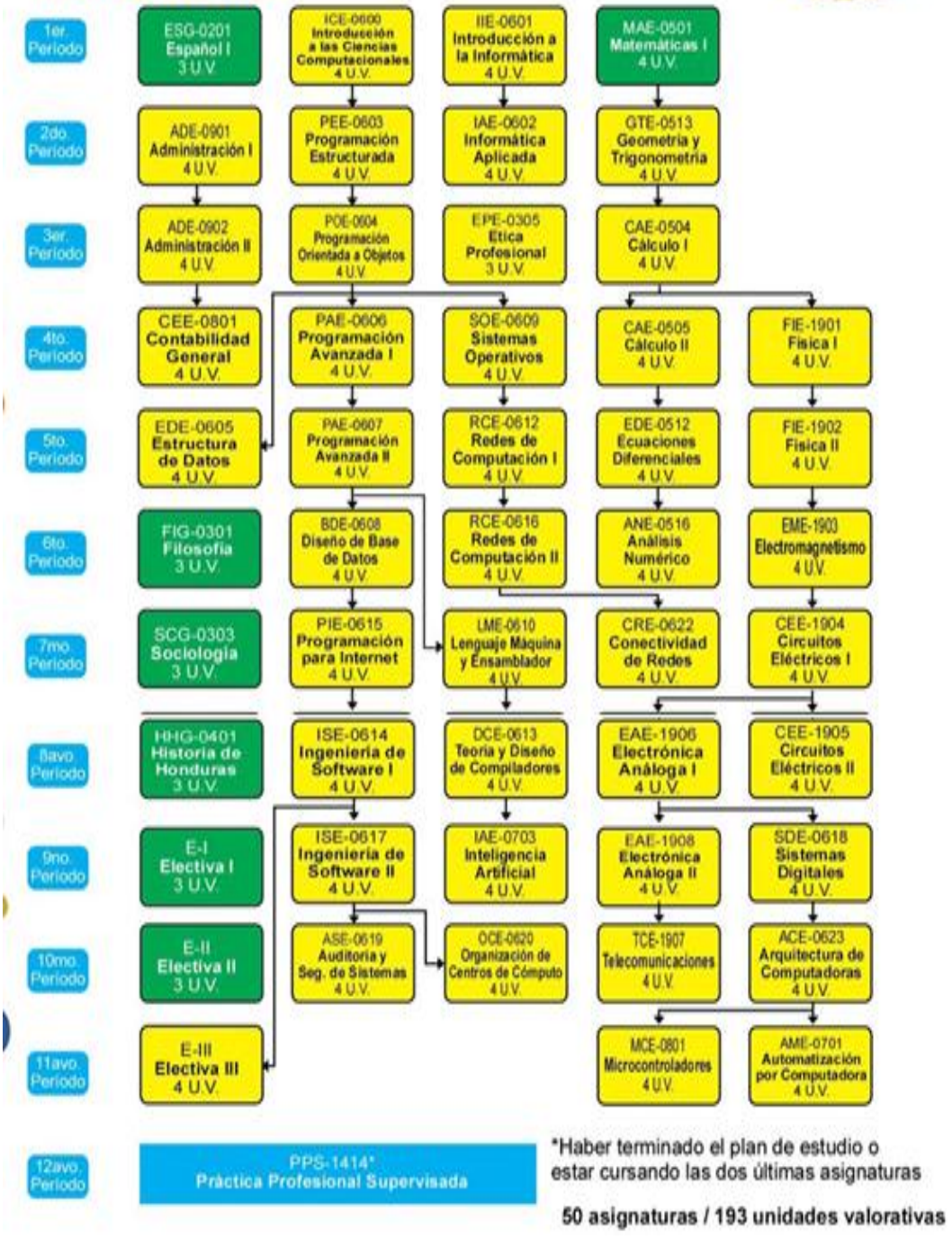
UNIVERSIDAD TECNOLOGICA DE HONDURAS

DERECHO

PLAN DE ESTUDIO



INGENIERÍA EN COMPUTACIÓN
PLAN DE ESTUDIO



*Haber terminado el plan de estudio o estar cursando las dos últimas asignaturas

50 asignaturas / 193 unidades valorativas

Temario de Investigación Forense de Delitos Cibernéticos y Digitales.

Lesson 1: Computer Forensics and Investigations as a Profession

Lesson 2: Understanding Computer Investigations

Lesson 3: Working with Windows and DOS Systems

Lesson 4: Macintosh and Linux Boot Processes and Disk Structures

Lesson 5: The Investigators Office and Laboratory

Lesson 6: Current Computer Forensics Tools

Lesson 7: Digital Evidence Controls

Lesson 8: Processing Crime and Incident Scenes

Lesson 9: Data Acquisition

Lesson 10: Computer Forensic Analysis

Lesson 11: E-mail Investigations

Lesson 12: Recovering Image Files

Lesson 13: Writing Investigation Reports

Lesson 14: Becoming an Expert Witness

Lesson 15: Computer Security Incident Response Team

Lesson 16: Logfile Analysis

Lesson 17: Recovering Deleted Files

Lesson 18: Application Password Crackers

Lesson 19: Investigating E-Mail Crimes

Lesson 20: Investigating Web Attacks

Lesson 21: Investigating Network Traffic

Lesson 22: Investigating Router Attacks

Lesson 23: The Computer Forensics Process

Lesson 24: Data Duplication

Lesson 25: Windows Forensics

Lesson 26: Linux Forensics

Lesson 27: Investigating PDA

Lesson 28: Investigating Trademark and Copyright Infringement

New Horizons
Computer Learning Centers

C)NFE™

Content

Comprised of 20 modules and 9 labs. The C)NFE will enhance your digital forensic competence by adding more advanced network forensics expertise and experience through discussions and practice.

Modules	
1: Digital Evidence Concepts	11: Layer 2 Protocol
2: Network Evidence Challenges	12: Wireless Access Points
3: Network Forensics Investigative Methodology	13: Wireless Capture Traffic and Analysis
4: Network-Based Evidence	14: Wireless Attacks
5: Network Principles	15: NIDS_Snort
6: Internet Protocol Suite	16: Centralized Logging and Syslog
7: Physical Interception	17: Investigating Network Devices
8: Traffic Acquisition Software	18: Web Proxies and Encryption
9: Live Acquisition	19: Network Tunneling
10: Analysis	20: Malware Forensics
Labs	
1: Working with captured files	6: NIDS/NIPS
2: Layer 2 Attacks & Active Evidence Acquisition	7: Syslog Exercise
3: Preparing for Packet Inspection	8: Network Device Log
4: Analyzing Packet Captures	9: SSL
5: Case Study: ABC Real Estate	

Certified Network Forensics Examiner

Delivery Method: Instructor-led (Classroom or Online live)

Duration: 4 Days

Description

The Certified Network Forensics Examiner was created when a U.S. Government Agency contracted us to train their team on advanced forensics in computer networks. The C)NFE will take your digital forensic skill set to the next level by navigating through over twenty modules of network forensic topics and providing you with hands-on, practical experience through our lab exercises that walk you through real-world situations that are solved with investigation and recovery of data in networks.

With the skill set of a C)NFE, students can understand exactly what is going on in a network to ensure its proper use by those intrusted with access. Every organization can benefit by employing a C)NFE to audit their network; everyone deserves to know how their resources are being used.

The course requires that students meet the following prerequisites:

The C)NFE course is a Network forensics course teaches people how to perform forensic investigations on networks. We advise that students have a knowledge and skill set of digital forensics equivalent to our C)DFE: Digital Forensics Examiner course. This is the advanced course in our forensics track. Feel free to contact us if you have any questions about this course or how we can accomidate your training needs.

At Course Completion:

Students will:

- Have knowledge to perform network forensic examinations.
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)NFE Exam

Content

With 17 modules and 2 appendices, the C)DFE will bring you up to speed on digital forensics in a fast, effective way.

1: Introduction	11: CF Processing Techniques
2: Computer Forensic Incidents	12: Digital Forensics Reporting
3: Investigation Process	13: Specialized Artifact Recovery
4: OS Disk Storage Concepts	14: eDiscovery and ESI
5: Digital Acquisition and Analysis	15: Cell Phone Forensics
6: Forensic Examination Protocols	16: USB Forensics
7: Digital Evidence Protocols	17: Incident Handling
8: CFI Theory	A1: PDA Forensics
9: Digital Evidence Presentation	A2: Investigating Harassment
10: Computer Forensics Lab Protocols	

Certified Digital Forensics Examiner

Delivery Method: Instructor-led (Classroom or Online live)

Duration: 5 Days

Description

Digital Forensics is the investigation and recovery of data contained in digital devices. This data is often the subject of investigations in litigation, proof of guilt, and corrective action in an organization. When the time comes that you need to investigate your organization, will you have the skill set necessary to gather the digital data that you need? The Certified Digital Forensics Examiner course will benefit organizations, individuals, government offices, and law enforcement agencies in performing these investigations and reporting their findings.

To illustrate, let's say an employee needs to be terminated for a violation of computer usage rules. To do so the organization must furnish an irrefutable burden of proof based on digital evidence. If not irrefutable, an attorney knowledgeable about Digital Forensics could have the case thrown out of court. Government and investigative agencies need proper training to succeed in cases like the above as well as those including acts of fraud, computer misuse, illegal pornography, counterfeiting, and so forth. A C)DFE is aptly prepared to handle these types of situations.

At Course Completion:

Students will:

- Have knowledge to perform digital forensic examinations.
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)DFE Exam

The course requires that students meet the following prerequisites:

The C)DFE course is a digital forensics course teaches people how to perform digital investigations. In order to do this effectively we require students to have a basic proficiency with using computers and an interest in digital forensics. If a student is unsure about whether or not they are ready to take this course, we recommend our C)SS: Certified Secruity Sentinel course as a prerequisite and confidence booster to those just getting into digital forensics and cyber security.
After you complete the C)DFE we encourage you to further develop your digital forensics skill set by taking the C)NFE: Network Forensics Examineer course and certification exam.

Temario de Investigación Forense de Delitos Cibernéticos y Digitales.

Lesson 1: Computer Forensics and Investigations as a Profession

Lesson 2: Understanding Computer Investigations

Lesson 3: Working with Windows and DOS Systems

Lesson 4: Macintosh and Linux Boot Processes and Disk Structures

Lesson 5: The Investigators Office and Laboratory

Lesson 6: Current Computer Forensics Tools

Lesson 7: Digital Evidence Controls

Lesson 8: Processing Crime and Incident Scenes

Lesson 9: Data Acquisition

Lesson 10: Computer Forensic Analysis

Lesson 11: E-mail Investigations

Lesson 12: Recovering Image Files

Lesson 13: Writing Investigation Reports

Lesson 14: Becoming an Expert Witness

Lesson 15: Computer Security Incident Response Team

Lesson 16: Logfile Analysis

Lesson 17: Recovering Deleted Files

Lesson 18: Application Password Crackers

Lesson 19: Investigating E-Mail Crimes

Lesson 20: Investigating Web Attacks

Lesson 21: Investigating Network Traffic

Lesson 22: Investigating Router Attacks

Lesson 23: The Computer Forensics Process

Lesson 24: Data Duplication

Lesson 25: Windows Forensics

Lesson 26: Linux Forensics

Lesson 27: Investigating PDA

Lesson 28: Investigating Trademark and Copyright Infringement

Apéndice A. Herramientas de Software para Informática Forense

HERRAMIENTA DE SOFTWARE	CODIGO	LICENCIA	CARACTERÍSTICAS	SITIO WEB
Marco Forense Digital	Código Abierto	Licencia Pública General	Se puede utilizar en la cadena de custodia y su uso es tanto en ambiente Windows como Linux, permite acceder a dispositivos locales o remotos, hace posible la recuperación de archivos que han sido escondidos o eliminados, realiza de igual manera búsquedas rápidas de los metadatos de archivos (Cañaveral, 2015).	http://www.digital-forensic.org/
Arquitectura Abierta para Informática Forense (OCFA)	Código Abierto	Licencia Pública General	Herramienta construida por la Agencia Nacional de Policía Holandesa, con el fin de automatizar el proceso de análisis forense digital. Utiliza base de datos PostgreSQL (Cañaveral, 2015).	http://sourceforge.net/projects/ocfa/
Ambiente Investigativo Guiado por Computadora (CAINE)	Código Abierto	Licencia Pública General	Ofrece un ambiente integrado de herramientas de software existentes, como módulos de software de una manera de uso fácil (Caine-Live, 2016).	http://www.caine-live.net/
HELIX	Código Abierto	Gratuita o de carga	Permite ser ejecutada el equipo sospechoso con su sistema operativo nativo latente. Es útil también para auditorías de red al poderse ejecutar desde casi cualquier máquina en el segmento de red (JDMESALOSADA, 2015).	http://www.e-fense.com/products.php
X-Ways Forense	Windows	Pagada, costo aproximado $1025.00	Permite realizar imágenes (copias) de disco y clonación, cuenta con capacidad de lectura de las estructuras del sistema de archivo, detecta automáticamente una partición de disco duro que haya sido borrada o perdida, realiza cálculo de hash a granel, auténtica datos, analiza memoria RAM (X-Ways, 2015).	http://www.x-ways.net/forensics/

Continuación Apéndice A				
HERRAMIENTA DE SOFTWARE	CODIGO	LICENCIA	CARACTERÍSTICAS	SITIO WEB
Kit de Herramientas de Investigación Forense (SANS)	Código Abierto	Gratuita o de carga	Sistema forense de múltiples usos, está provisto de todas las herramientas necesarias para ser utilizadas en un proceso de investigación forense digital (Cañaveral, 2015).	http://digital-forensics.sans.org
EnCase	Windows	Pagada, costo aproximado $ 1000.00	Realiza una recopilación rápida de datos de varios dispositivos que pueden ser potencial evidencia y realiza generación de informes (Cañaveral, 2015).	https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
Kit Detective (Sleuth Kit)	Código Abierto	Licencia Pública de IBM (IPL) Licencia Pública Común (CPL), Licencia Pública General (GPL)	Está provista de varias herramientas que apoyan el análisis forense digital mediante el análisis de sistemas de archivos a profundidad (Cañaveral, 2015).	http://www.sleuthkit.org/
Volatilidad	Código Abierto	Licencia Pública General	Permite dar respuesta a incidentes y realizar un análisis de malware, adicionalmente extrae información de los procesos en ejecución, conexiones de red, archivos DLL y secciones de registro, igualmente se puede utilizar para extraer información de archivos de volcado o en hibernación de Windows (Ros, 2015).	http://code.google.com/p/volatility/
WindowsSCOPE	Sistema Operativo Windows	Pagada, costo aproximado $ 7700.00	Esta herramienta es utilizada para realizar ingeniería de malware. Provee la capacidad de análisis del núcleo de Windows, controladores, archivos DLL, memoria virtual y física (Ros, 2015).	http://www.windowsscope.com

Continuación Apéndice A				
HERRAMIENTA DE SOFTWARE	CODIGO	LICENCIA	CARACTERÍSTICAS	SITIO WEB
Suite OxygenForensic	Unicode	Pagada, costo aproximado 2500.00	Este software que reúne pruebas desde un teléfono móvil. Permite la recopilación de información como ser el registro de llamadas, contactos y mensajes aún cuando estos hayan sido borrados. Genera informes que facilitan la interpretación de los resultados del análisis (Ros, 2015).	http://www.oxygen-forensic.com
Xplico	Código Abierto	Licencia Pública General	Permite la extracción de datos de las aplicaciones que hacen uso de protocolos de Internet y de red ya que es compatible con la mayoría de los mismos (HTTP, IMAP, POP, TCP, IPv4 e IPv6, entre otros) (Ros, 2015).	http://www.xplico.org
XRY	Sistema Operativo Windows		Recupera y analiza información (llamadas, imágenes, SMS y mensajes) desde cualquier dispositivo móvil, aún aquellos que han sido borrados (Ros, 2015).	http://www.msab.com/xry/what-is-xry
Extractor de Mayor (Bulk Extractor)	Multi - Sistema Operativo	Gratuita	Realiza análisis de imágenes de discos duros, archivos o directorios de archivos. Debido a que no considera la estructura del sistema de archivos este proceso lo realiza con mayor rapidez que otras herramientas similares (Ros, 2015).	http://digitalcorpora.org/downloads/bulk_extractor/
Kit de Herramientas Forense de Acceso de datos (Access data Forensic Toolkit (FTK))	Sistema Operativo Windows	Pagada, costo aproximado 4000.00	Plataforma de investigación digital que proporciona velocidad, estabilidad y fácil uso, igualmente el filtrado y búsqueda de información es más rápido debido a que el procesamiento y la indexación es delantera (Ros, 2015).	http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

Apéndice B. Herramientas de Hardware para Informática Forense

Hardware Forense	Descripción	Tipo	Características	Enlace para compra
Write-Blockers	Dispositivo que permite grabar información en una unidad, sin que exista la posibilidad de dañar accidentalmente su contenido. Esto se permite permitiendo únicamente los comandos de lectura, y denegando comandos de escritura.	IDE - IDE	• Permite únicamente conexiones de tipo: Dispositivo Almacenamiento – Dispositivo Almacenamiento (LBA Group).	www.epos.ua/view.php/en/products_epos_write_protector
		Firewire/USB – IDE	• Permite únicamente conexiones de tipo: Dispositivo Externo – Dispositivo Almacenamiento (LBA Group).	www.mykeytech.com/
Estación Forense	Es una estación forense de gran rendimiento, pensada para acelerar la obtención de resultados y profundizar en las investigaciones. Está diseñada para ejecutar diferentes aplicaciones forenses al mismo tiempo.	Velociraptor 7	• Almacenamiento de evidencias de 32TB en Raid 5. • SSD de 2TB en Raid 0 para el S.O. RAM de 256GB. • DeepSpar para recuperación de archivos en discos dañados. • Puertos bloqueados contra escritura FireWire, USB 3.0, SATA, eSATA. • Refrigeración líquida, menos ruido y máximo rendimiento (Ondata Internacional, 2016).	www.ondata.es/recuperar/equipos-forensics.htm
		Velociraptor 5	• Almacenamiento desde 12TB a 32TB. • Discos SSD para máxima velocidad del SO. • RAM de 128-256GB para optimizar la multitarea. • Puertos bloqueados contra escritura FireWire, USB 3.0, SATA, eSATA. • Menos ruido y máximo rendimiento (Ondata Internacional, 2016).	www.ondata.es/recuperar/equipos-forensics.htm

Continuación Apéndice B				
Hardware Forense	Descripción	Tipo	Características	Enlace para compra
		Velociraptor 3	• Almacenamiento de hasta 24TB. • Discos SSD de hasta 500GB para máxima velocidad del SO • Memoria RAM de 32 a 256GB para optimizar la multitarea. • Puertos bloqueados contra escritura FireWire, USB 3.0, SATA, eSATA. • Refrigeración líquida, menos ruido y máximo rendimiento (Ondata Internacional, 2016).	www.ondata.es/recuperar/equipos-forensics.htm
Kit-Telefonía	Herramientas avanzadas de auditoría forense móvil que extraen, decodifican y analizan datos de todo tipo de celulares, aparatos de GPS, tabletas y teléfonos fabricados con chipsets chinos.	UFED Touch	• Permite hacer extracciones físicas, de sistema de archivos, lógicas y de claves en profundidad de datos pericialmente seguros a partir de los más diversos dispositivos móviles (Cellebrite Mobile Synchronization LTD, 2014).	www.cellebrite.com/
		UFED 4PC	• Brinda a los usuarios la posibilidad de extraer, decodificar y analizar datos en un mismo PC o laptop. Se trata de una solución flexible, conveniente y con buena relación costo-beneficio para cualquier profesional investigador o de inteligencia que necesite tener una herramienta forense móvil en su PC o laptop (Cellebrite Mobile Synchronization LTD, 2014).	www.cellebrite.com/
Duplicador de Unidades de disco	Es una herramienta que ofrece a los investigadores duplicar o copiar información de manera rápida y eficiente. Permite copiar la información	ImageMASSter Solo-4	• Soporte de manera nativa conexiones SAS, SATA y USB, y asegura las conexiones mediante cifrados. Contiene una conexión giga Ethernet. La autenticación se realiza mediante sha-1, sha-2 y md5 (Evidence Technology Magazine, 2008).	ics-iq.com/

Continuación Apéndice B				
Hardware Forense	Descripción	Tipo	Características	Enlace para compra
	sospechosa en 2 unidades separadas simultáneamente. Incluso 2 unidades en una única copia de evidencia.	Startech 1:3	• Duplicador de unidades que permite a los usuarios realizar una copia de 1 a 3, sector a sector copiando de una sola unidad SATA a otros 3 de manera simultánea (Evidence Technology Magazine, 2008).	www.StarTech.com
Recuperador de Contraseñas	Hardware que permite descifrar información protegida por contraseña de manera rápida y sencilla	TableauPasswordRecovery	• Permite recuperar contraseñas más rápido. • Contiene cuatro tarjetas de Tableau TACC2 (Guidance Software, 1997).	www.guidancesoftware.com/
Optimizador de Imágenes	Hardware que permite adquirir solamente la data necesaria. Auto selecciona cualquier tipo de archivo para copiar. Permite crear rutinas costumizables.	Ditto DX Imager	• Unidad de 8 TB • Discos SSDs que ayudan a limitar responsabilidades de la data. • Puede ser utilizada de manera virtual. • Soporta muchas entradas de escritura de conexiones SATA, eSATA, PATA y USB2.0 (CRU Inc., 2016).	www.cru-inc.com/ditto/
Capturador de Pantalla	Fue diseñado para fines de eficiencia y uso fácil cuando se conduce examinaciones manuales en un laboratorio forense. Permite al usuario tomar pantallas, grabar audio, video, y anotar evidencia.	Eclipse 3	• Cámara Canon T3i DSLR • Base Metálica EDEC con Brazo Mágico Manfrotto • Sistema de Captura limpia • Filtro Polarizado (Evidence Technology Magazine, 2008).	www.edecdf.com/promo/eclipse/eclipse.php
Jaulas Electromagnéticas	Es una caja de almacenamiento seguro que es efectiva contra las radio frecuencias arriba de los 6000 MHz, HEMP, luz solar, y campos eléctricos producidos por cables de energía.	EMFaraCage	• Puede ser configurado solamente para almacenamiento y conexión para uso de pruebas de evidencia o funciones “blackhat” (Evidence Technology Magazine , 2008)	www.lbagroup.com/products/faraday-cage-rf-shielding-enclosure

Apéndice C. Metodologías Utilizadas en Informática Forense

METODOLOGÍA	DESCRIPCIÓN
Casey, E; 2000	Metodología general, puede ser aplicada en computadoras que se encuentran aisladas -individuales- y/o computadoras que pertenecen a un entorno de red. Es recomendada para casos que no cuentan con mucha complejidad.
Ashcroft, J.; 2001 y Mukasey, M.B.; Sedgwick, J.L.; Hagy, D.W.; 2008	Metodología que fue propuesta por el Departamento de Justicia de los Estados Unidos, cuenta con dos ediciones. Fue concebida como una guía que da respuesta a delitos informáticos, por lo que es de apoyo a los informáticos forenses, ya que proporciona una guía para la selección de pruebas digitales más adecuadas según el delito investigado Las primeras fases de la investigación del delito son el centro de esta metodología.
Palmer, G.; 2001	Se utiliza como punto de partida para elaborar otras propuestas de metodología. No se considera como una metodología definitiva, pues sus fases no son descritas completamente, sino que se describen por medio de sus características y las posibles técnicas que pueden emplearse.
Reith, M.; Carr, C.; Gunsch, G.; 2002	Esta metodología puede ser considerada como una especificación de la metodología de Palmer. En esta se agregan nuevas fases y los ciclos de retroalimentación. Puede ser aplicada a cualquier tipo de tecnología y delito informático.
Carrier, B.; Spafford, E.H.; 2003b	La metodología de Carrier y Spafford presentan a detalle cinco fases que en total conllevan diecisiete tareas que son aplicadas en la investigación. En la investigación realiza una integración de las pruebas digitales con las físicas.

Continuación Apéndice C	
METODOLOGÍA	DESCRIPCIÓN
Baryamureeba, V.; Tushabe, F.; 2004	Metodología de 5 fases, con ciclos de realimentación entre ellas, está basada en la metodología de Carrier.
Ciardhuáin, S.Ó.; 2004	La integran trece fases que se encuentran en forma de cascada, por lo que la información fluye de una fase (actividad) a la siguiente. La cadena de custodia es formada por una lista que contiene la totalidad de aquellos que han formado parte de la investigación y han manipulado las pruebas digitales. De igual manera debe establecerse los flujos de información y los puntos de control del proceso.
Casey, E.; 2004	Segunda versión de la metodología de Casey, posee 8 fases las cuales representan un punto de equilibrio entre metodologías cortas y largas.
Rifà, H.; Serra, J.; Rivas, J.L.; 2009	Metodología de 3 fases con un enfoque para casos no complejos.
Casey, E.; 2011	Tercera versión de la metodología de Casey, puede ser aplicada en casos complejos.

Fuente: (Salmerón, 2015)

Apéndice D. Países Relacionados con el Convenio sobre Ciberdelincuencia

País	Fecha Firma	FechaRatificado	Entrada en Vigor	Nota	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/06/2002	01/07/2004				A.			
Andorra	23/04/2013	16/11/2016			R.	D.	A.			
Armenia	23/11/2001	12/10/2006	01/02/2007				A.			
Austria	23/11/2001	13/06/2012	01/10/2012		R.	D.	A.			
Azerbaijan	30/06/2008	15/03/2010	01/07/2010		R.	D.	A.	T.		
Bélgica	23/11/2001	20/08/2012	01/12/2012		R.	D.	A.			
Bosnia y Herzegovina	09/02/2005	19/05/2006	01/09/2006				A.			
Bulgaria	23/11/2001	07/04/2005	01/08/2005		R.	D.	A.			
Croacia	23/11/2001	17/10/2002	01/07/2004				A.			
Chipre	23/11/2001	19/01/2005	01/05/2005				A.			
República Checa	09/02/2005	22/08/2013	01/12/2013		R.	D.	A.			
Dinamarca	22/04/2003	21/06/2005	01/10/2005		R.		A.	T.		
Estonia	23/11/2001	12/05/2003	01/07/2004				A.			
Finlandia	23/11/2001	24/05/2007	01/09/2007		R.	D.	A.			
Francia	23/11/2001	10/01/2006	01/05/2006		R.	D.	A.			

ContinuaciónApéndice D										
País	Fecha Firma	FechaRatificado	Entrada en Vigor	Nota	R.	D.	A.	T.	C.	O.
Georgia	01/04/2008	06/06/2012	01/10/2012			D.				
Alemania	23/11/2001	09/03/2009	01/07/2009		R.	D.	A.			
Grecia	23/11/2001									
Hungria	23/11/2001	04/12/2003	01/07/2004		R.	D.	A.			
Islandia	30/11/2001	29/01/2007	01/05/2007		R.		A.			
Irlanda	28/02/2002									
Italia	23/11/2001	05/06/2008	01/10/2008				A.			
Letonia	05/05/2004	14/02/2007	01/06/2007		R.		A.			
Liechtenstein	17/11/2008	27/01/2016	01/05/2016		R.	D.	A.			
Lituania	23/06/2003	18/03/2004	01/07/2004		R.	D.	A.			
Luxembourg	28/01/2003	16/10/2014	01/02/2015				A.			
Malta	17/01/2002	12/04/2012	01/08/2012			D.				
Moldovia	23/11/2001	12/05/2009	01/09/2009			D.	A.	T.		
Monaco	02/05/2013									
Montenegro	07/04/2005	03/03/2010	01/07/2010	55	R.		A.			
Holanda	23/11/2001	16/11/2006	01/03/2007				A.	T.		

Continuación Apéndice D										
País	Fecha Firma	FechaRatificado	Entrada en Vigor	Nota	R.	D.	A.	T.	C.	O.
Noruega	23/11/2001	30/06/2006	01/10/2006		R.	D.	A.			
Polonia	23/11/2001	20/02/2015	01/06/2015		R.		A.			
Portugal	23/11/2001	24/03/2010	01/07/2010			D.	A.			
Rumania	23/11/2001	12/05/2004	01/09/2004				A.			
Serbia	07/04/2005	14/04/2009	01/08/2009	55			A.			
Eslovaquia	04/02/2005	08/01/2008	01/05/2008		R.	D.	A.			
Eslovenia	24/07/2002	08/09/2004	01/01/2005				A.			
España	23/11/2001	03/06/2010	01/10/2010			D.	A.			
Suecia	23/11/2001									
Suiza	23/11/2001	21/09/2011	01/01/2012		R.	D.	A.			
Macedonia	23/11/2001	15/09/2004	01/01/2005				A.			
Turquía	10/11/2010	29/09/2014	01/01/2015							
Ucrania	23/11/2001	10/03/2006	01/07/2006		R.	D.	A.			
Reino Unido	23/11/2001	25/05/2011	01/09/2011		R.		A.			
Países no Miembros del Consejo de Europa										
Australia		30/11/2012 a	01/03/2013		R.		A.			

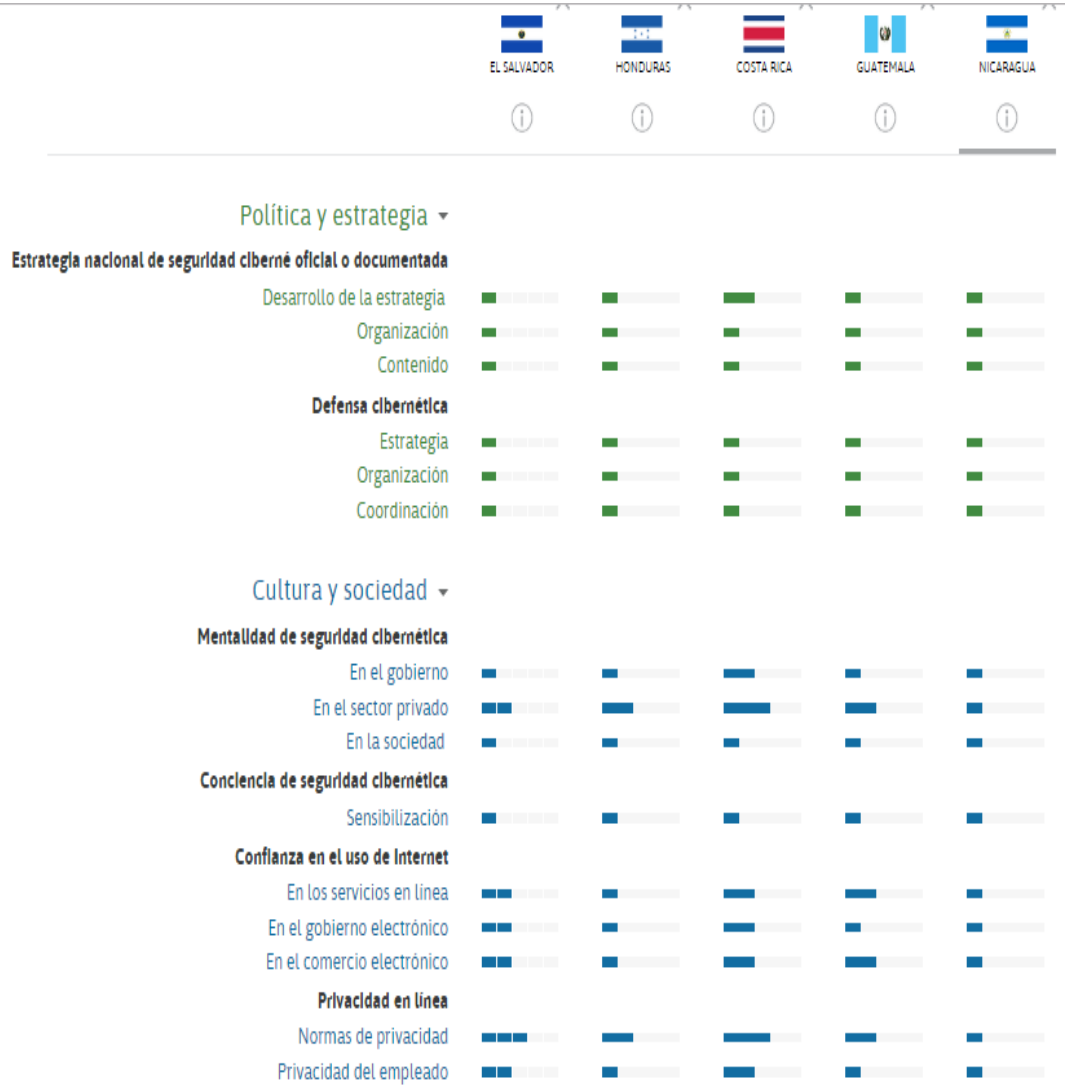
Continuación Apéndice D										
País	Fecha Firma	FechaRatificado	Entrada en Vigor	Nota	R.	D.	A.	T.	C.	O.
Canadá	23/11/2001	08/07/2015	01/11/2015		R.	D.	A.			
República Dominicana		07/02/2013 a	01/06/2013			D.	A.			
Israel		09/05/2016 a	01/09/2016		R.		A.			
Japón	23/11/2001	03/07/2012	01/11/2012		R.	D.	A.			
Islas Mauricio		15/11/2013 a	01/03/2014				A.			
Panamá		05/03/2014 a	01/07/2014				A.			
Sudáfrica	23/11/2001									
Sri Lanka		29/05/2015 a	01/09/2015		R.	D.	A.			
Estados Unidos de América	23/11/2001	29/09/2006	01/01/2007		R.	D.	A.			

Indicadores
(55) Fecha de la firma por la unión del estado de Serbia y de Montenegro.
a: Adhesión
s: Firma sin reserva de ratificación
su: Sucesión
r: Firma "ad referendum".

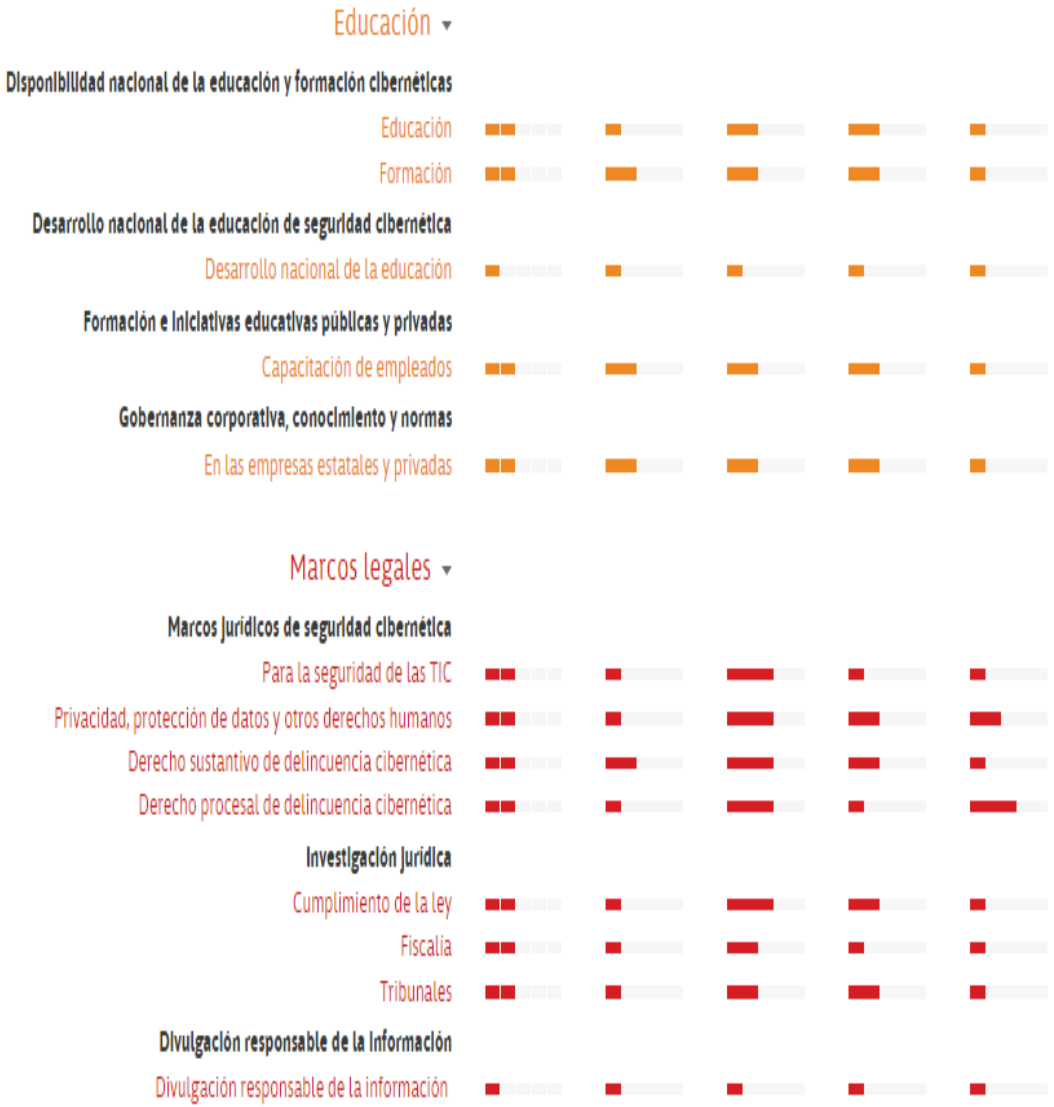
R .: Reservas
D .: Declaraciones
A .: Autoridades
T .: Aplicación Territorial
C .: Comunicación
O .: Objeción.

Fuente: (Council of Europe, 2016)

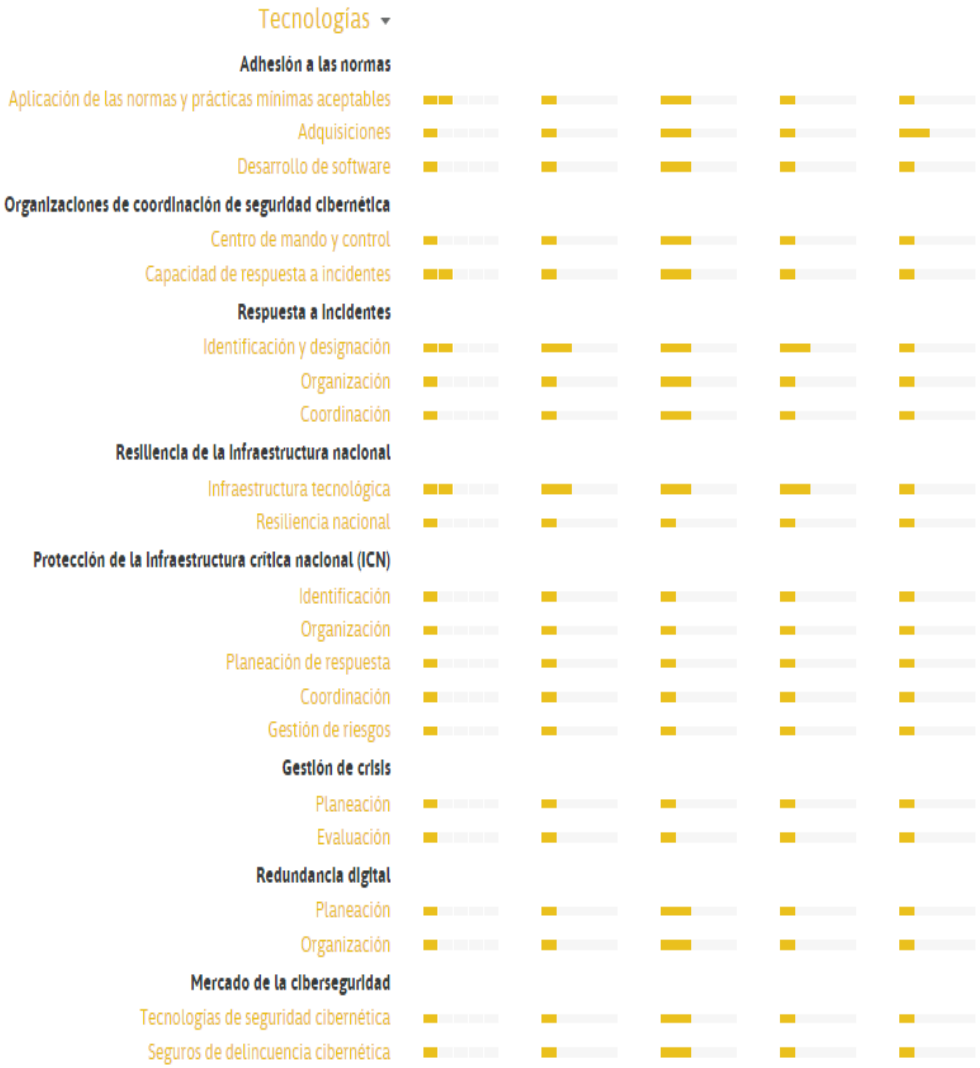
Apéndice E. Comparativo sobre Ciberseguridad países de Centroamérica



Continuación Apéndice E



Continuación Apéndice E



Fuente: (Observatorio de la Ciberseguridad en América Latina y el Caribe, 2016)