**Universidad Militar Nueva Granada**

# Impactos positivos de los métodos para prevenir la limpieza de rastros de acceso por daño informático en las empresas en Colombia

**Jasson Andres Marin Rincon**

**Director**

**Cr. Jesus Maria Diaz Jaimes**

**Especialización en Administración de la Seguridad**

**Ensayo Final**

**Cali – Colombia**

**2016**

# Contenido

# Resumen

Entrar en el contexto de la tecnología informática, las vulnerabilidades electrónicas a los que los usuarios están expuestos, las penalidades a los atacantes según la legislación Colombiana y las formas en las que los delincuentes buscan eliminar las evidencias que sirven para identificarlos o encontrarlos, son los temas de mayor interés en las empresas.

Se muestra la ley y las clasificaciones de los delitos que están definidos por el estado en Colombia en términos de seguridad de la información, al igual que las cifras de delitos informáticos para el año 2015. De acuerdo a las tipificaciones de los delitos, se aprecian los perfiles básicos que podrían tener un delincuente y la responsabilidad de las políticas de las empresas como generadoras de motivación a nuevos atacantes con mayores oportunidades de materializar riesgos y fraudes.

De la misma forma, se identifican algunas técnicas utilizadas por los delincuentes en forma de ataque estructurado con métodos de evasión de seguridad o técnicas Anti-Forenses que buscan eliminar cualquier método de rastreo, seguimiento o pistas de los delitos cometidos.

**Palabras Clave:** Delito informático, evidencias digitales, gestión de riesgos, seguridad de la información, técnicas anti-forenses

## Abstract

Entering in the context of technology information the electronic vulnerabilities that the users are exposed to the penalties to the offenders according to the Colombian legislation and the forms in which the offenders find a way to remove the evidence which help to identify and find, are the topics of mayor interests in businesses.

It shows the law and the classifications of the offenses that are defined by the state in Colombia, in terms of security of the information as well as the number of computer offenses for the year 2015. According to the typifications of the crimes, the basic profiles that could have a delinquent and the responsibility of the business politics are appreciated as motivation to new attackers with major opportunities of materializing risks and frauds.

In the same way, some techniques used are identified by the delinquents in form of a structured attack with methods of safety evasion or anti-forensic techniques that remove any tracking method, tracing or tracks of committed crimes.


**Key words:** computer crime, digital evidence, Risk management, security of the information, Anti-forensic techniques

# Abreviaturas

Self Monitoring Analysis and Reporting Technology SMART

Tecnologías de la Información y la Comunicación TIC.

Traducción Trad.

Organización para la Cooperación y el Desarrollo Económico (en adelante: ODCE)

Consejo Nacional de Política Económica y Social (en adelante: CONPES)

Departamento Administrativo Nacional de Estadística (en adelante: DANE)

Página p.

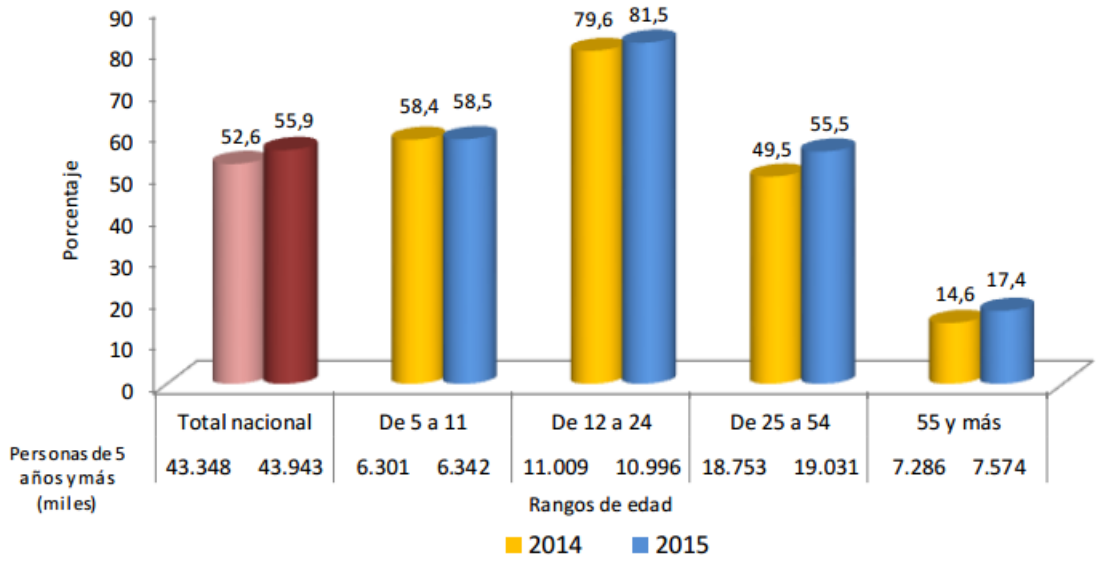
# Introducción

Desde hace ya varias década atrás, la inteligencia humana y el arduo deseo de realizar labores más rápidamente, al menor costo y más eficientemente justifican la creación de tecnología electrónica como forma de simulación del espacio físico y la transformación de la información como elemento vital para tomar decisiones como mencionan Gaitan y Uyaban:

> Nuestra era se encuentra determinada para la transformación de la información en conocimiento, por su marcada dependencia por lo tecnológico. Este factor que ha permitido un evidente progreso, asimismo, se ha convertido en la puerta de entrada de una amenaza y un riego contra la seguridad nacional. (Gaitan & Uyaban, 2012, p.5)

Estos riesgos toman especial atención cuando a través de las estadísticas se evidencia que existe un alto porcentaje de usabilidad de esta tecnología electrónica digital, no solo por parte de usuarios básicos o usuarios domésticos, como lo refleja la Ilustración 1:

**Ilustración 1.** *Proporción de las personas que usaron internet en cualquier lugar y desde cualquier dispositivo, por rangos de edad. Total Nacional 2014 y 2015*



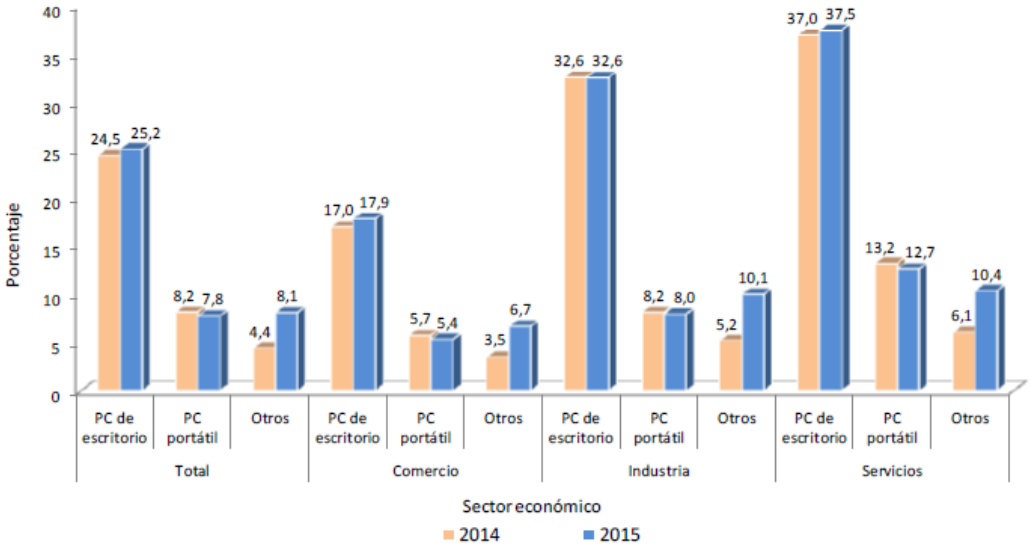

**Fuente:** *DANE - Encuesta Nacional de calidad de vida - ECV*

Las cifras muestran que las edades de los usuarios de internet van desde los 5 años hasta personas mayores de 55 años, permitiendo afirmar que internet está al alcance de todas las personas y los usuarios no tienen distinción de edad; por esta razón se genera un interrogante

asociado a las amenazas a las que está expuesta la población y la efectividad de las medidas de seguridad informática implementadas en los dispositivos a través de los cuales acceden al servicio de internet.

Tomando un interés más a fondo de las personas que hacen uso de la red mundial, otra gráfica estadística dentro del mismo estudio se enfoca en las empresas pequeñas o micro-establecimientos en Colombia en donde se evidencia el porcentaje de utilización de la tecnología electrónica digital de acuerdo a los sectores económicos más representativos en la Ilustración 2:

**Ilustración 2.** *Proporción de micro-establecimientos que usaban computador de escritorio, computador portátil u otros bienes TIC. Total Industria, Comercio y Servicios 2014-2015*




**Fuente 1.** *DANE - Encuesta de Micro-establecimientos - Resultados módulo TIC Panel 2014-2015*
*Nota 1: Las empresas pueden usar distintos bienes TIC; es decir, la respuesta es incluyente.*

*Nota 2: Otros incluye: Smartphone y tableta y PDA-DMC*

Con estos porcentajes es posible tener presente que esta adopción de la tecnología digital en las empresas se realiza buscando mejorar la eficiencia en términos de productividad y alta disponibilidad de los datos para el análisis y toma oportuna de decisiones.

De los resultados mostrados anteriormente podemos evidenciar que el estado colombiano crea unas normas que delimitan el tratamiento de la información personal que en varios casos se encuentra expuesta en los usos de la tecnología electrónica a través de Ley Estatutaria 1581:

> La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Colombia, Congreso de la Republica, Octubre 17 de 2012, Ley Estatutaria 1581, Art. 1)

Teniendo como referente la Ley 1581 es necesario dimensionar que los administradores de T.I. y usuarios de estaciones de trabajo o dispositivos móviles, actualmente pueden ser atacados sin que sean percibidos por los programas antivirus free u otro software de identificación de vulnerabilidades de los sistemas de información no licenciados. Algunos de esos ataques se completan bajo la ignorancia del usuario al permitir o aceptar algún tipo de información (script oculto) que para ellos puede ser normal o inofensivo, por ejemplo al acceder a un link de envío de correo, un link de video de Facebook o youtube, entre los más comunes y utilizados por los usuarios o en los casos que no se tenga ningún tipo de software de detección de amenazas.

En esta gran ámbito de la tecnología electrónica el panorama de seguridad pone en manifiesto que “La experiencia práctica derivada de la investigación de numerosos casos de fraude y del empleo fraudulento de equipos informáticos muestra que los ordenadores se limitan a modificar la naturaleza de los riesgos (…)” (Corner, 2009, p. 174).

Esta opinión nos permite enmarcar la tecnología Electronica digital dentro de las líneas de investigación de seguridad física, teniendo en cuenta que los sistemas electrónicos digitales, buscan simular en gran medida la realidad humana.

Estos incrementos de delitos también pueden tener su origen en la utilización de la misma tecnología sin controles, por esto es recomendable inicialmente tener presente de que o quien nos protegernos, según lo clasificado por la ley en cuanto a los delitos reconocidos. Posteriormente se requiere identificar cuáles son las técnicas que utilizan los delincuentes para pasar desapercibidos en los intentos de delitos informáticos como forma de evasión de la ley en Colombia y por ultimo conocer la importancia de los métodos que sirven como apoyo para contrarrestar las técnicas anti-forenses.

# Impactos positivos de los métodos para prevenir la limpieza de rastros de acceso por daño informático en las empresas en Colombia[*]

## Los delitos informáticos y la normatividad colombiana

"La esencia de cualquier fraude bien conseguido es que las personas honradas no sospechen: el mal triunfa cuando la gente de bien no actúa" (Corner, 1993, p.18). Ésta conceptualización nos alerta a estar en un estado de vigía permanente en términos de seguridad en el diario vivir, en el hogar, en las calles y sobretodo en las empresas sin importar el tamaño, la actividad económica, la cantidad de ingresos, cantidad de empleados o el estatus económico que la identifique; Para estos casos y teniendo en cuenta que en nuestra sociedad cualquier individuo puede ser delincuente o víctima de fraude de cualquier nivel, se aprecia que la percepción de inseguridad se ve influenciada por la cultura acelerada que ha causado la era de la electrónica digital.

Cuando hablamos de fraudes informáticos por si solos, no se puede percibir a simple vista cuales son los impactos que puede generar la ausencia de tratamiento a las vulnerabilidades en los sistemas electrónicos digitales con resultados directos hacia las personas, empresas pymes o grandes compañías.

Sin embargo, según un estudio del Bank of América con la compañía Merrill Lynch (2015) en el año. "Se calcula que el delito cibernético cuesta actualmente a la economía mundial $ 500 billones anuales" (p.2) (traducido a través de Traductor Google). y para complementar, la empresa Cisco en otro estudio informa que "En Colombia, la cifra que pueden estar perdiendo las empresas mediante fraudes electrónicos a través de distintos medios se calcula, para 2015, más o menos en mil millones de pesos" Garzón(como se citó en ELTIEMPO, 2016).

[*] Para la elaboración del ensayo se tuvieron en cuenta como referencia las asignaturas Investigación en Seguridad, Manejo del Talento Humano y Seguridad Informática las cuales combinan la identificación de amenazas y las procesos legales en las investigaciones informáticas.

Es apenas lógico que esta cifra capte la atención de cualquier persona que al menos tenga vínculo con alguna compañía que posea un sistema electrónico básico para el tratamiento de datos o manejo de información.

Ningún Propietario, Presidente, Gerente, Administrador, Contador, Encargado y demás cargos responsables de toma de decisiones de gran trascendencia y repercusiones directas al objetivo principal de las compañías (obtener utilidades), puede hacer la vista a un lado a este tipo de prácticas delincuenciales que ponen en riesgo las operaciones de la compañía e incluso la continuidad del negocio, en la mayoría de los casos, de forma silenciosa.

Sin embargo el panorama Colombiano no se queda atrás, debido que actualmente se está prestando una gran atención a los delitos informáticos que empiezan a tener un incremento en la misma medida que la tecnología es acogida y está al alcance de cualquier ciudadano, al punto que el estado a través del Congreso de la Republica de Colombia publican una Ley que decreta:

> Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Colombia, Congreso de la República, 2009, Ley 1273).

De esta forma, el estado crea leyes que permiten identificar que a través del mal uso de las tecnologías de la información y comunicación se pueden cometer actos delictivos que atentan con la integridad personal, el estado financiero y la continuidad de las compañías.

La ley define los delitos informáticos que pueden ser denunciados a la autoridad y tienen penas que combinan prisión y multas económicas de acuerdo al tipo de delito entre los que están:

**Tabla No. 1.** *Delitos Informáticos Definidos en el Código Penal*

| CONDUCTA PUNIBLE |
|---|
| **VII BIS. DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS** |
| Acceso abusivo a un sistema informático |
| Obstaculización ilegítima de sistema informático o red de telecomunicación |
| Interceptación de datos informáticos |
| Daño informático |
| Uso de software malicioso |
| Violación de datos personales |
| Suplantación de sitios web para capturar datos personales |
| Hurto por medios informáticos y semejantes |
| Transferencia no consentida de activos |

**Fuente.** *Revista Criminalidad. Volumen 58, Numero 2. Mayo-Agosto 2016.*

En tan solo 6 años de entrar en vigencia esta ley de tipificación de delitos, se puede apreciar que en Colombia para el año 2015 los Delitos De la Protección de la Informacion y de los Datos, tienen una participación el 0.95% equivalentes a 7.338 delitos de los 779.801 denunciados a la Policía Nacional para el mismo año, tal como lo refleja la siguiente tabla:

**Tabla No. 2.** *Comparativo Delitos por Títulos del Código Penal 2014-2015*

| TÍTULO | BIEN JURÍDICO | 2014 | 2015 | VARIACIÓN PORCENTUAL | % PARTICIPACIÓN 2015 |
|---|---|---|---|---|---|
| I. | Delitos contra la vida y la integridad personal | 140.968 | 147.865 | 4,89% | 18,96% |
| II. | Delitos contra personas y bienes protegidos por el Derecho Internacional Humanitario | 246 | 208 | -15,45% | 0,03% |
| III. | Delitos contra la libertad individual y otras garantías | 4.683 | 12.726 | 171,75% | 1,63% |
| IV. | Delitos contra la libertad, integridad y formación sexuales | 12.650 | 21.737 | 71,83% | 2,79% |
| V. | Delitos contra la integridad moral | 6.658 | 23.771 | 257,03% | 3,05% |
| VI. | Delitos contra la familia | 63.591 | 95.722 | 50,53% | 12,28% |
| VII. | Delitos contra el patrimonio económico | 199.548 | 213.241 | 6,86% | 27,35% |
| VII BIS. | De la protección de la información y de los datos | 3.675 | 7.388 | 101,03% | 0,95% |
| VIII. | Delitos contra los derechos de autor | 37.109 | 38.578 | 3,96% | 4,95% |
| IX. | Delitos contra la fe pública | 15.064 | 20.721 | 37,55% | 2,66% |
| X. | Delitos contra el orden económico social | 42.523 | 43.735 | 2,85% | 5,61% |
| XI. | Delitos contra los recursos naturales y el medio ambiente | 2.501 | 3.175 | 26,95% | 0,41% |
| XII. | Delitos contra la seguridad pública | 52.759 | 62.951 | 19,32% | 8,07% |
| XIII. | Delitos contra la salud pública | 79.215 | 68.664 | -13,32% | 8,81% |
| XIV. | Delitos contra mecanismos de participación democrática | 142 | 593 | 317,61% | 0,08% |
| XV. | Delitos contra la administración pública | 6.759 | 8.772 | 29,78% | 1,12% |
| XVI. | Delitos contra la eficaz y recta impartición de justicia | 6.120 | 9.639 | 57,50% | 1,24% |
| XVII. | Delitos contra la existencia y seguridad del estado | 1 | 3 | 100,00% | 0,00% |
| XVIII. | Delitos contra el régimen constitucional y legal | 443 | 312 | -29,57% | 0,04% |
| **TOTAL DELITOS** | | **674.655** | **779.801** | **15,59%** | **100%** |

**Fuente.** *Revista Criminalidad. Volumen 58, Numero 2. Mayo-Agosto 2016.*
Nota: Las cifras presentadas en esta publicación están sujetas a variación por denuncias que ingresan por el sistema de Denuncias y Contravenciones (Sidenco) al Sistema Penal Oral Acusatorio.

Aunque es una cifra pequeña en relación con la cantidad de denuncias de otros delitos en el país, se entiende que una de las variables que impide que los delitos informáticos denunciados sea mayor es que aunque "La legislación colombiana de delitos informáticos es suficiente, el problema es de conocimiento en la materia de parte de jueces, fiscales y organismos de policía judicial" Guzman (como se citó en Perez, 2013), además del posible desconocimiento de las leyes que se han promulgado para este tema por parte de las personas naturales y algunas empresas que no dan importancia o sencillamente no creen posible que los delincuentes puedan ser identificados por las autoridades.

En muchas empresas se tiene y se muestra la percepción que la ley de seguridad de la información solo viene relacionada a la ley del Habeas Data o la Ley de Tratamiento de Datos

Personales y no se evidencian consultas e investigación que les permita descubrir esta nueva ayuda que proporciona el estado en términos de penalidad a los atacantes.

De la misma forma, la Policía ha presentado los respectivos informes estadísticos detallados de la cantidad de delitos informáticos para Colombia en el 2015 en la siguiente tabla:

**Tabla No. 3.** *Delitos Registrados en Colombia 2015*

| VII BIS. DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS | | | |
|---|---|---|---|
| BIEN JURÍDICO | | CONDUCTA PUNIBLE | |
| **ARTICULO** | **DESCRIPCION** | **CANTIDAD** | **%** |
| 269I | Hurto por medios informáticos y semejantes | 4810 | 65.1% |
| 269F | Violación de datos personales | 972 | 13.2% |
| 269A | Acceso abusivo a un sistema informático | 1103 | 14.9% |
| 269J | Transferencia no consentida de activos | 280 | 3.8% |
| 269G | Suplantación de sitios web para capturar datos personales | 127 | 1.7% |
| 269D | Daño informático | 40 | 0.5% |
| 269C | Interceptación de datos informáticos | 29 | 0.4% |
| 269E | Uso de software malicioso | 19 | 0.3% |
| 269B | Obstaculización ilegítima de sistema informático o red de telecomunicación | 8 | 0.1% |
| | **SUBTOTAL** | **7388** | **100.0%** |

**Fuente:** *Revista Criminalidad. Volumen 58, Numero 2. Mayo-Agosto 2016.*

Estas cifras dejan en evidencia que el 65,1% de los delitos informáticos están relacionados en obtener un beneficio financiero y que además refleja que la población que comete estos delitos, ven en el fraude informático un gran negocio y una solución más fácil para el sostenimiento económico con niveles de exposición a riesgos contra la integridad física muy bajos o casi nulos. En otras palabras, los delincuentes no exponen su salud o su vida para obtener dinero a través de un hurto a través de la informática, como si podría darse al enfrentar a una persona cuerpo a cuerpo en busca de sus pertenencias con algún tipo de arma.

Sim embargo se genera la inquietud acerca de quiénes o de donde provienen los posibles atacantes a la información, para donde Corner muestra una identificación de amenaza a través de la siguiente tabla:

**Tabla No. 4.** *Categorías de Fraude según la fuente del riesgo y la vía de ocultación*

| | FUENTE Y TIPO |
|---|---|
| A | Interno: por directivos |
| B | Interno: por trabajadores manuales |
| C | Externo: por personas partícipes en contactos empresariales |
| D | Externo: por oportunistas |
| E | Por colusión: organizado |

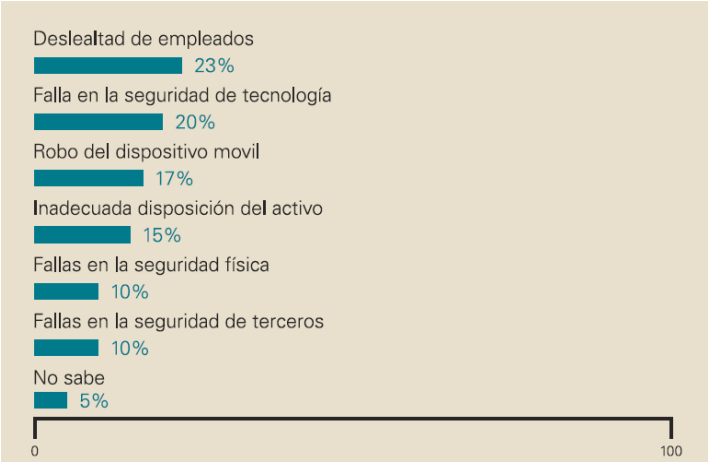
**Fuente:** Corner, M, *El fraude en la empresa.* (2009), p. 49.

Bajo esta clasificación de Corner ubica los posibles atacantes de forma interna en las organizaciones (empleados - directivos) y la delincuencia externa, proporcionando de esta forma campos de análisis y acción diferentes entre ellos pero con fines probablemente comunes.

Por otra parte, Vasquez (2011) nos muestra los perfiles de los delincuentes como: "Amateur, Cracker, Cibercriminal Profesional y Terrorista/Hacktivista" (p.36-37) con el fin de mostrar una variable importante que requiere especial atención a la hora de medir el nivel exposición a los riesgos de la información de acuerdo a grado de conocimiento de los atacantes.

Para ampliar más el panorama de los delitos informáticos en el año 2013 la firma KPMG realizó una encuesta de fraude en Colombia especificando las causas más comunes de cibercrimen denunciado:

**Ilustración 3.** *Causas más comunes de Cibercrimen*




**Fuente.** *KPMG Advisory Services Ltda (2013),* Encuesta de Fraude en Colombia 2013

Con todos los resultados mencionados se deduce que los delitos informáticos pueden ser cometidos por casi cualquier persona con acceso a la tecnología y que las intenciones, además de las motivaciones de los agresores, evidencian un amplio universo de posibles amenazas a las compañías y su información.

**Amenazas y nuevas técnicas aplicadas a delitos informáticos**

Ya teniendo claras algunas de las amenazas y las motivaciones para producir un delito informático es necesario aclarar que aunque la exposición a los riesgos de muerte o integridad humana de un delincuente informático son muy bajos o mínimos, no significa que al cambiar el entorno del delito no se generen algunos riesgos que traen repercusiones determinantes para él. Al entrar al medio digital, los delincuentes pasen a ser blanco permanente de empresas dedicadas a la seguridad informática que destinan grandes recursos para identificar las vulnerabilidades en los sistemas y las practicas inseguras de los usuarios, además de buscar la interceptación de atacantes que estén tratando o que hayan realizado algún atentado contra los clientes que contratan sus servicios.

Anualmente, algunas de estas empresas de tecnología y seguridad informática en el mundo, publican artículos que describen sus predicciones acerca de las tendencias que tendrán presencia en el año venidero. Para el año en curso, Ventas de Seguridad (2016) Fortiguard Labs (Laboratorios Fortiguard), presentaron el Top 5 de Predicciones de Amenazas (The Top 5 Threat Predictions For 2016) en el cual realizaron especial énfasis a los inminentes ataques con la utilización de Ghostware (técnicas para ocultar los indicadores de compromiso) como complemento a los delitos informáticos que ocurren a nivel mundial.

En estos escenarios presentados por empresas de seguridad informática de gran renombre mundial en combinación con autoridades estatales de los países líderes en investigación de riesgos y delitos informáticos, se han puesto en evidencia las continuos, y cada vez más efectivos, intentos de los atacantes por no dejar rastro al momento de acceder a un sistema informático que permita su identificación y posible ubicación.

> La amenaza: A medida que los cibercriminales se convierten en el foco de la investigación y el procesamiento en el sistema de justicia criminal, los hackers cuidadosos desarrollarán una nueva variante de malware que está diseñado para cumplir

> con su misión y luego borrar todas las huellas antes que las medidas de seguridad pueden detectar que un compromiso ha tomado lugar. (Manky, 2016) (Trad.)

Los rastros que normalmente quedan expuestos en un ataque informático (sin ser alterados) permiten realizar trazabilidad e identificar los delitos a las organizaciones cuando se realizan incluso desde adentro, es decir, por empleados de la misma empresa que no se sienten a gusto con políticas, personas o simplemente que han sido sobornadas a cambio de información.

Para el caso de las empresas en Colombia, es posible que no todos los administrativos o representantes legales ponen una gran atención a esas vulnerabilidades de la información, algunos podrían pensar que es muy costoso, otros porque no creen que podría pasarle a ellos u otros porque aseguran que sus sistemas son seguros, a lo que Corner comenta:

> No debe sorprendernos que los altos directivos se suelan mostrar desconcertados en cuanto a las medidas que deben adoptar para proteger sus sistemas informáticos. Tampoco resulta sorprendente que, debido a este desconcierto, las empresas permanezcan innecesariamente expuestas al peligro o protegidas en exceso contra riesgos inexistentes. (Corner, 2009, p.169)

Sin embargo, sin importar cuál sea el estado de la empresa en términos de seguridad informática, no está de más aplicar continuos estudios de seguridad y métodos actualizados que permitan identificar y tratar las vulnerabilidades de los sistemas de información y aún más en los casos que los ataques puedan ser internos. Es decir, a través de un estudio de seguridad debemos partir de la identificación de las posibles amenazas, de quien debemos protegernos de delitos informáticos en las empresas, luego identificar los riesgos y el impacto de la materialización de éstos, pero en los casos que la crisis sea inminente se permita realizar un adecuado análisis forense.

**Informática forense y los retos actuales.**

Como se nombró anteriormente, la importancia de un estudio de seguridad para la identificación de riesgos puede combinarse con la elaboración de un Plan del Manejo de Crisis para el tratamiento de las vulnerabilidades, pero también es preciso emplear técnicas que nos permitan tener importante información para realizar una investigación adecuada y obtener evidencias que puedan servir como elementos probatorios de tipo penal en caso de llevarse a cabo alguno de los delitos informáticos definidos.  Casey define la evidencia de digital como

“cualquier dato que puede establecer que un crimen se ha ejecutado… o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor” (Casey, 2001, p.8).

En esta definición que plantea Casey se menciona el objetivo principal en lo que los estados y las autoridades a nivel mundial centran su atención para definir leyes y normas, teniendo en cuenta que ante cualquier delito, sin importar su naturaleza, deben existir elementos o evidencias científicas que esclarezcan el delito, que prueben la intención y grado de participación de algún individuo, utilizando técnicas que demuestren veracidad de los elementos encontrados y sobretodo que sean contundentes al momento de que puedan ser acusatorios.

Este tipo de procedimientos de recolección de evidencias han llegado a ser muy especializados, además de ser requeridos para el normatividad legal al punto de ser un tipo de ciencia conocida como Informática Forense, definida como ciencia que busca revelar a través de los medios informáticos los hechos y la generar hipótesis que tienen relación directa con el evento.

Aun mas, este tipo de ciencia ha tomado gran interés teniendo en cuenta que nuestra naturaleza siempre está en la búsqueda de esclarecer cualquier tipo de acontecimiento, y  más en los casos donde nos han realizado una afectación a nivel de integridad humana o económica.

Ya siendo los computadores materia de alto interés general y especial énfasis como casos de estudio, un integrante de la Policía Nacional comenta:

> Sin embargo, la evidencia digital que explicaría el método y el medio utilizado por el atacante para hacer posible la infección podría estar muy lejos de allí. Un caso frecuente es un teléfono inteligente, previamente infectado y sincronizado con un equipo en la oficina de una gerencia o una memoria USB encontrada por un empleado en su hora de almuerzo y conectada sin seguridad a la red, facilitan la puerta de acceso al atacante. (Coronel Garcia, 2015, p.1)

Bajo este concepto, nuestros activos son aún más vulnerables por la incorporación de nuevas tecnologías digitales que están estrechamente ligadas al diario vivir en nuestras sociedades cibernéticas. En otras palabras, la misma tecnología que nos permite estar más conectados y ser más eficientes en muchas actividades, está siendo utilizada como medio o herramienta para llevar a cabo los delitos.

**Técnicas anti-forenses informáticas**

En estas nuevas integraciones de tecnología es sano reconocer que la tecnología está avanzando más rápidamente que los entes legales que pueden tener control a los delitos cometidos y peor aún, que la creación y modificación de las leyes es un proceso extremadamente lento en donde quedaran muchos crímenes impunes. Para terminar de completar, adicionalmente de legislar lentamente acerca de estas actividades ilegales, se deben realizar estudios y enseñanza en profundidad a todas las personas que intervienen en el proceso legal buscando tener competencias acorde con lo requerido por los cargos para los que son contratados por el estado.

> El reconocimiento de las vulnerabilidades en las herramientas utilizadas para adelantar procedimientos de informática forense, ha generado la aparición de las llamadas técnicas anti-forense que se definen como: "cualquier intento de comprometer la disponibilidad de la evidencia para un proceso forense". Estas técnicas buscan manipular el material más sensible de una investigación al destruir, ocultar, eliminar y falsificar la evidencia. (Paus, 2015, p1)

Existen muchos autores que coinciden con la definición anterior de las Técnicas Anti-Forenses donde un panorama de aceptación y claridad al concepto a nivel mundial, sin embargo, sobrepasando la definición es de vital importancia identificar y detallar cuáles son las técnicas utilizadas por los atacantes, a lo que contrariamente los autores muestran grandes diferencias en la forma en que están clasificadas y utilizadas como teoría para manipular las evidencias.

Por ejemplo Paus agrupa las técnicas anti-forenses en "Técnicas de Borrado o destrucción de la información (…), Técnicas de ocultación de la información (…), Técnicas de sobreescritura de metadatos (…), Técnicas de cifrado de la información (…), y Otras técnicas en comunicaciones" (Paus, 2015, p.1).

Por su parte, Garfinkel (2009) las clasifica en 4 categorías con subdivisiones de una forma más completa y detallada:

**Tabla No. 5.** *Clasificación Técnicas Anti-Forenses (Garfinkel)*

| **Tecnicas Anti-Forenses Tradicionales** |
|---|
| Sobreescribir datos y metadatos |
| Criptografia, esteganografia y otros métodos de ocultación de datos |
| **Tecnicas Anti-Forenses que minimizan huellas** |
| Inyeccion de la memoria y la funcion de proxy Syscall |
| Live Cds, tokens USB de arranque y máquinas virtuales |
| Identidades y almacenamiento anónimos |
| **Tecnicas Anti-Forenses que explotan errores Computer Forensic Tools** |
| Falta de validación de datos |
| Ataques de denegación de servicio |
| Heurística frágil |
| **Tecnicas Anti-Forenses que detectan los Computer Forensic Tools** |
| Contrarrestar el analisis forense con SMART |
| Deteccion de Analisis Forense de Redes |

**Fuente.** *Garfinkel, 2009, p.1-8.*

Bajo otras literaturas se encuentra Vasquez (2016) que muestra un enfoque más completo y además actualizado a las tendencias actuales en términos informáticos:

**Tabla No. 6.** *Clasificación Técnicas Anti-Forenses Informáticas (Vasquez)*

| TÉCNICAS ANTIFORENSES INFORMÁTICAS | | | |
|---|---|---|---|
| **TECNICA** | **DETALLE** | **TIPOS** | |
| **1. OCULTAMIENTO DE DATOS** | Estas técnicas apuntan principalmente a ocultar la evidencia digital. El perito forense informático puede encontrarla pero sin poder interpretarla; o peor aún no encontrarla por la manera que fue ocultada. | *Criptografia* | por Cifrado de Discos |
| | | | por Cifrado de Discos por Hardware |
| | | | por Cifrado de Discos Virtuales |
| | | | por Sistemas de Archivos Criptográficos |
| | | | por Sistemas de Archivos con Cifrado |
| | | | por Protocolos de Comunicación |
| | | *Esteganografía* | por Texto |
| | | | por Audio |
| | | | por Imagen |
| | | | por Video |
| | | | por Protocolos de Red |
| | | *Empaquetadores de Programas* | |
| | | *Otras Formas de Ocultamiento* | |
| **2. ELIMINACION DE DATOS** | El objetivo de estas técnicas es lograr la eliminación de la evidencia digital. Al perito forense informático se le dificulta mucho recuperar datos que fueron destruidos. | *Sanitización* | Taxonomía de los Datos |
| | | | Sanitizacion por Software |
| | | *Destrucción Física* | |
| **3. ANTICONCEPCIÓN DE DATOS** | A diferencia de la sobrescritura y borrado de datos, las técnicas de anticoncepción directamente previenen la creación de datos. Datos que nunca existieron obviamente no pueden ser recuperados utilizando ninguna herramienta forense. | *Syscall Proxying* | |
| | | *Inyección de Código en Memoria* | |
| | | *Live Distros* | |
| | | *Manipulación del Kernel* | |
| | | *Maquinas Virtuales* | |
| | | *Compiladores/Ensambladores en Memoria* | |
| **4. OFUSCACIÓN** | El propósito de las técnicas de ofuscación es confundir, desorientar y desviar la investigación forense. | *Sobreescritura de Metadatos* | en Atributos de Archivos |
| | | | Imágenes JPEG |
| | | *Emails* | por Sistema de Punto Muerto |
| | | | Spam combinado con esteganografia |
| | | | Falsificación de encabezados |
| **5. ATAQUES AL SOFTWARE FORENSE** | Entre las nuevas tendencias anti-forenses se destacan los ataques contra las herramientas forenses. | *Fallas en la Validacion de Datos* | |
| | | *Heurísticas Frágiles* | |
| | | *Contrarrestar el Analisis Forenses* | |
| | | *Denegacion de Servicio* | |
| | | *Integridad del Hash* | |
| | | *Detectar el Monitoreo de Red* | |
| **6. ATAQUES A PROCEDIMIENTOS FORENSES** | Otras de las nuevas tendencias anti-forenses son aquellas que atacan a las diferentes etapas de los procedimientos forenses. | | |

**Fuente.** *Vasquez, M. 2016. Técnicas Anti-Forenses Informáticas (Tesis de Especialización). p, 81.*

Es interesante como además se presenta un poco más de detalle a éste último método que a simple vista pone en riesgo cualquier tipo de investigación que se adelante por un delito, "Ataque a Procedimientos Forenses"; Vasquez (2016) plantea una tabla que muestra la forma en que son comparados los procedimientos forenses y los ataques que podrían recibir:

**Tabla No. 7.** *Técnicas de Ataques Anti-Forenses Informáticas (Vasquez)*

| Etapa | Descripción | Ataques |
|---|---|---|
| **Identificación** | Método por el cual el perito identifica que hay un incidente para investigar. | Oscurecer el incidente o esconder el nexo entre el dispositivo digital y el hecho bajo investigación. |
| **Preservación** | Pasos por los cuales se preserva la integridad de la evidencia. | Interrumpir la cadena de custodia o poner en duda la integridad de la evidencia misma. |
| **Recolección** | Proceso por el cual los datos son extraídos de la evidencia. | Evitar que se complete la recolección de datos o poner en duda el software, hardware, políticas y procedimientos utilizados para recolectar la evidencia. |
| **Examinación** | Proceso que se ocupa de cómo se revisa la evidencia. | Mostrar que las herramientas son inadecuadas, incompletas o que no están certificadas. |
| **Análisis** | Etapa en la cual el perito saca las conclusiones a partir de la evidencia. Se basa en las herramientas, la habilidad del perito y el resto de la evidencia no digital que fue encontrada. | Si el caso se basa solamente en la evidencia digital, la interpretación será la más propensa a ser atacada. |
| **Presentación** | Métodos por los cuales los resultados de la investigación digital son presentados al jurado u otros investigadores. | Si la evidencia es sólida, herramientas y métodos anti-forenses serán usados para atacar la fiabilidad y el rigor de los informes o el examinador. |

**Fuente**. *Vasquez, M. Técnicas Anti-Forenses. (2016)*

Toda la clasificación de técnicas anti-forenses mostrada por Vasquez nos permite tener una perspectiva más amplia del alcance al que están llegando los delincuentes, dado que la clasificación de las múltiples amenazas puede coincidir a un mismo objetivo. Aunque en muchas ocasiones podríamos estar realizando medidas de control sobre ataques externos a la información

de la empresa, y nos confiamos que tenemos los riesgos bajo control, pasamos por alto las amenazas que tienen más capacidad de materializar un riesgo, los empleados y los visitantes. Bajo la misma perspectiva se requiere cada vez más en las empresas gestar la cultura de seguridad en todo nivel y de forma transversal en todos los procesos que la componen. El cargo que tiene la obligación y la responsabilidad de buscar un cambio en la cultura organización basada en riesgos y en protección, es el Gerente, Jefe o Administrador de la seguridad. Desde esta óptica, el encargado de seguridad puede tener la facilidad de exponer los riesgos a los que continuamente puede verse expuesta la empresa en cualquier proceso, los cuales pueden ir desde la selección del personal que va a ser contratado, hasta la evaluación a Gerencias y Presidencias. Se debe tener en cuenta que este tipo de nueva identidad organizacional basada en riesgos para llegar a tener resultados visibles en la empresa, debe presentar excelente formulación de políticas y procedimientos, además de tener rigurosas repeticiones y continuas validaciones que demuestren que su aplicación no entorpecen el rendimiento y el cumplimiento del macro objetivo de la compañía.

También con las mismas Técnicas de Vasquez se puede tomar como punto de partida y un reto grande para los Administradores de Seguridad debido que surgen nuevas vulnerabilidades, más complejas y más difíciles de identificar en la aplicación de las técnicas de control y seguridad informática básicas, requiriendo de esta forma una continua actualización en temas de avances informáticos, métodos delictivos y herramientas utilizadas principalmente por agresores informáticos. En otras palabras, además de fomentar la cultura organizacional basada en riesgos, se hace necesario ir a la vanguardia en los estudios de seguridad y las nuevas tecnologías para el manejo de la información.

A pesar que el panorama de la seguridad informática en las empresas en Colombia no sea muy controlado y poco penalizado, no significa que la batalla contra los atacantes está perdida al momento de encontrar pruebas que nos ayuden como evidencia en delitos cometidos.

En el caso de las técnicas anti-forenses, Zuccardi, G y Gutierrez, J. plantean las siguientes recomendaciones:

> Sin embargo, este problema es mitigado con algunas características que posee la evidencia digital:
> • La evidencia de Digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. (…)

> • Actualmente, con las herramientas existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.
> • La evidencia de Digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
> • Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios. (Zuccardi, G y Gutierrez, 2011, p. 9)

Con estas recomendaciones propuestas como principio de la manipulación de la información, tenemos un referente que nos abre las puertas a múltiples planes de contingencia, manejo de crisis y planes de continuidad de negocio, brindándoles a las personas que intervienen con la compañía una percepción de seguridad de la información con sus características propias, Integridad, Confidencialidad y Disponibilidad.

**Ventajas de la prevención de técnicas anti-forenses**

Teniendo identificados los posibles atacantes de la tecnología e información y las técnicas que pueden utilizar como forma de evitar quedar en evidencia, es realmente importante encontrar las ventajas de la aplicación de técnicas que impidan o proporcionen control a este tipo de actividad ilícita.

Las ventajas vienen inherentes a cada una de las actividades que se realicen permanentemente en las compañías en pro de obtener una cultura organizacional basada en riesgos, en donde como se dijo anteriormente, la seguridad en todo nivel debe ser una percepción generalizada en los integrantes de la empresa y los posibles atacantes, en donde su primer objetivo viene apoyado sobre la estrategia como se menciona:

> La estrategia de gestión de riesgos para abordar la seguridad digital debe tener un enfoque flexible y ágil para abordar las incertidumbres digitales. Lo anterior, con el fin de alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales, y proteger a las personas frente a las amenazas de seguridad digital (OCDE, 2015).

Esta cultura a través de la estrategia debe tener los siguientes elementos que traducen en las ventajas de los métodos aplicados a prevenir los riesgos de ataques a la información:

1. Percepción de Seguridad: “Regla 10: Si la seguridad informática es sencilla, nadie creerá en ella” (Corner, 2009, p.423). Es claro que en las empresas que se tienen implementados niveles de control, además de auditorías permanentes y aleatorias a todos los procesos, se genera

hacia los posibles atacantes internos con “motivaciones personales” una disuasión que exige tener un plan de ataque más estructurado que evite ser descubierto fácilmente y para los atacantes con más conocimientos en la ejecución de delitos, se obliga a tomarse más tiempo en la identificación y análisis de los sistemas de seguridad instalados. En otras palabras, cuando hay percepción de seguridad en una compañía por parte de cualquier individuo, la idea de algunos posibles ataques pueden acabarse y en otras demuestra que no se es un blanco fácil para llevarse a cabo.

2. Políticas Claras y Eficaces: CONPES a través del Documento 3701 presenta un enfoque basado en “Lineamientos de política para ciberseguridad y ciberdefensa para contrarrestar las amenazas cibernéticas en el entorno digital. No obstante el éxito de la política de ciberseguridad y ciberdefensa, se hace necesario complementar sus esfuerzos teniendo en cuenta…, la gestión de riesgos” (Documento CONPES 3854, 2016 , p.9)

Aunque puede ser un incluyente en el punto anterior, las políticas de seguridad en la mayoría de situaciones no vienen pensadas únicamente como métodos de prevención de riesgos, sino que también ayuda a la optimización de procesos y recursos en la consecución del macro objetivo de la compañía. De esta forma se integra casi que automáticamente los niveles gerenciales y directivos en la generación y aplicación de las políticas, las cuales también deben ser fijadas con el fin de minimizar las motivaciones de daño por parte de los empleados.

3. Seguridad Compartida: “el seguro de riesgo por infidelidad es un sistema de emergencia que puede reducir la gravedad de la perdida” (Corner, 2009, p. 392). con el compromiso que se muestra en los puntos anteriores por parte de los directivos de las organizaciones, es una buena práctica la de transferir algunos riesgos a través de contratación de seguros o pólizas ante eventos de perdida de información, contratos de confidencialidad y tercerización en los procesos de selección y contratación del personal. Con esto minimizamos los impactos en caso de materializarse los riesgos de robo de información y además disminuimos la probabilidad de contratar personas que sean una permanente amenaza dentro de las instalaciones.

De igual forma se deben combinar los esfuerzos que realizan las compañías de forma independiente con las propuestas en seguridad que ofrece el estado y los organismos públicos especializados en estos temas, como por ejemplo se refleja en la publicación del Departamento Nacional de Planeación en el CONPES 3854:

> Objetivo 5.3.3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos: Este objetivo busca empoderar a los ciudadanos y al Estado en relación con los riesgos del entorno digital, y consolidar las capacidades del país para hacer frente al crimen, la delincuencia y otros fenómenos que afectan la seguridad nacional desde este entorno. (Documento CONPES 3854, 2016, p. 57).

4. Comunicación Proactiva: podría tenerse en cuenta que la comunicación en las empresas generan un riesgo por posible filtración de información clasificada, sin embargo en el caso de la buena comunicación entre la planeación y ejecución de los procesos, se pueden evidenciar fallas y eventos fuera de lo normal o que requieren ser tenidos en cuenta como posibles vulnerabilidades no identificadas y medidas de control que no están siendo efectivas y que son una gran oportunidad en las empresas como afirma Peters: "El fallo es la auténtica esencia del aprendizaje, del crecimiento y del éxito" (Peters, 2006, p.75). Esta comunicación reafirma el compromiso con las labores realizadas y el respeto por los actores asociados a los procesos.

5. Recursos: el tema que más atención tiene a nivel de gerencia en una compañía es uno de los factores fundamentales y decisivos en la cultura organizacional basada en riesgos, el factor económico. Si bien, el impacto de perdida financiera que se genera después de un ataque en las empresas y más en términos de información (que es lo que se busca evitar con la aplicación de políticas de control de riesgos) es alto, el costo de su implementación es directamente proporcional. Las motivaciones al personal operativo, los perfiles de los encargados de seguridad e informática, la inversión en tecnología, los costos asociados a procesos de control y demás defensas a la infraestructura y la información, aunque son altas financieramente hablando, son justificadas en dos grandes puntos, primero, la disminución del impacto de materializarse los riesgos identificados pueden garantizar la continuidad de la compañía, y segundo, cuando se implementa un adecuado esquema de seguridad, muchos de los procesos y recursos de la compañía son optimizados en costos, gastos y en tiempos, proporcionando un mayor margen de utilidad de la misma forma que un aceptable retorno de inversión.

6. Equipo de Trabajo de Seguridad Informática: "sólo una persona excepcional podría resolver por sí misma todos los problemas de seguridad informática" (Corner, 2009, p.431). No se puede dejar por fuera el conocimiento técnico especializado. Las competencias en términos de sistemas de información e informática es un obvio requerimiento de las personas

encargadas de la seguridad informática, sin embargo, ese tipo de conocimientos es tan sólo uno de los requisitos de este equipo de trabajo. Se requiere personal que en todos sus actos muestre evidencia de análisis, control y panorama de riesgos con una constante proyección hacia la seguridad y la optimización de recursos y procesos.

## Conclusión

Las ciencias forenses informáticas están empezando a ser acogidas y aplicadas en grandes proporciones en nuestro país como forma encontrar la responsabilidad y castigo (según lo requiera) a los delitos informáticos realizados por las diferentes amenazas a las que están expuestas.

Aunque el fraude en las empresas es inevitable en un 100%, no significa que no podamos aplicar métodos, herramientas y políticas para prevenir, controlar los riesgos identificados en la gestión de seguridad de la compañía y en el peor de los casos, encontrar los rastros de los atacantes que consiguen materializarlos.

Por encima de cualquier actividad que vincule la seguridad informática, es necesario tener presente este antecedente como el principio básico del ataque a las técnicas Anti-Forenses:

> La impresión que la empresa suscita en los observadores externos tiene una relación directa con su exposición al fraude. Si se considera que una forma mantiene niveles de control insatisfactorios y cuenta con un personal desmotivado, esta imagen está tentando a los demás a apoderarse de su patrimonio. (Corner, 2009, p. 361)

De esta forma podemos apreciar que además de los controles básicos a los procesos, las herramientas especializadas en seguridad informática, una efectiva comunicación y una cultura organizacional basada en riesgos, son la fuerte barrera que disminuye la probabilidad de ataques a uno de los bienes más importantes de las compañías, La Información.

# Referencias


Bank of America. (2015). CIO Reports – A Transforming World – Making Cents of CyberSecurity. Recuperado de http://www.pbig.ml.com/publish/content/application/pdf/GWMOL/PBIG_AR6LBDNM_2016-07.pdf

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Waltham, USA: Elsevier Inc.

Comer, M. (1993). *El Fraude en la Empresa* (Segunda Edición.). España: Deusto.

Congreso de la República. (05 de Enero de 2009). Ley 1273 de 2009. *Ley 1273 de 2009*. Bogotá, Bogotá, D.C., Colombia: Congreso de la República.

Congreso de la República. (2012). *Ley 1581 de 2012*. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Coronel Garcia, F. (2015, 29 de Junio). Convergencia Tecnología y Cibercrimen. *Revista Sistemas (ACIS)*. Recuperado de http://52.0.140.184/revsistemas1/index.php/component/k2/item/196-convergencia-tecnol%C3%B3gica-y-cibercrimen

Departamento Nacional de Planeación, 2016, Consejo Nacional de Política Económica y Social - Documento 3854, en adelantes CONPES.

Gaitan, A. & Uyabán, M. (2012) *El ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI, I edición*. Colombia: Esdegue - SIIA – CEESEDEN.

Garcia, Camilo. (2013. Mayo, 1) ¿En Colombia se investigan los delitos informáticos?. *Colombia Digital.* Recuperado Octubre 2016, de https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html

Garfinkel, S., (2009). *Anti-Forensics: Techniques, Detection and Countermeasures.* (Trabajo Investigativo). Naval Postgraduate School, CA, USA.

KPMG Advisory Services Ltda (2013), *Encuesta de Fraude en Colombia 2013*, Colombia.

Manky, D. (22 de Agosto de 2016). *Fortinet*. Obtenido de Fortinet Blog: https://blog.fortinet.com/2016/08/22/looking-back-at-our-2016-predictions?utm_source=web&utm_medium=home-cta1&utm_campaign=blog-post-fortiguard-threat-predictions

Organización para la Cooperación y el Desarrollo Económicos (2015) Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, en adelante ODCE, Francia: ODCE. Recuperado de http://www.OCDE.org/sti/ieconomy/digital-security-risk-management.pdf.

Paus, L. (2015). *Técnicas Antiforenses*. WeLiveSecurity-ESET. Recuperado de http://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses/

Peters, T. (2006). *Gestionar con Imaginación.* España: Deusto.

Policía Nacional de Colombia. (Mayo-Agosto 2016). Tablas Estadísticas de Delitos 2015. *Revista Criminalidad.* (58), p. 1-36.

POLICIA NACIONAL - Dirección de Investigación Criminal e INTERPOL, (2016). *Guía de Seguridad para los Actores de la Cadena de Suministro* (V Edición), Colombia.

Tecnosfera (2016. Abril, 25). Perdidas de empresas colombianas en fraudes electrónicos. *El Tiempo.* Recuperado Noviembre 2016, de http://www.eltiempo.com/tecnosfera/novedades-tecnologia/perdidas-de-empresas-colombianas-en-fraudes-electronicos/16573154.

Vasquez, M. (2016). *Técnicas Anti-Forenses Informáticas* (Tesis de Especialización). Universidad Nacional de Cordoba, Cordoba, Argentina.

Ventas de Seguridad. (01 de 2016). Amenazas en Ciberseguridad para 2016. *Ventas de Seguridad*, *20*(1), 66-68.

Zuccardi, G y Gutierrez, J (2006). Informática Forense. Recuperado de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

# Lista de ilustraciones

# Lista de Tablas