Mª Luisa Fanjul

CONCEPTUALIZACIÓN, EVOLUCIÓN Y CLASIFICACIÓN DEL CIBERDELITO EMPRESARIAL

DEFINICIÓN DEL PERFIL DEL CIBERDELINCUENTE. IMPLICACIONES ESTRATÉGICAS

AMEC
EDICIONES

María Luisa Fanjul Fernández

CONCEPTUALIZACIÓN, EVOLUCIÓN Y CLASIFICACIÓN DEL CIBERDELITO EMPRESARIAL.

DEFINICIÓN DEL CIBERDELINCUENTE. IMPLICACIONES ESTRATÉGICAS.

ESERP Business & Law School

Security FORUM

©Conceptualización, evolución y clasificación del ciberdelito empresarial. Definición del ciberdelincuente. Implicaciones estratégicas.
©María Luisa Fanjul Fernández
©2018 Editorial: AMEC Ediciones
C/ Marqués del Vasto 3. 28003. Madrid. España.
ISBN: 978-84-946590-5-8

Maquetación y diseño: Editorial RingoRango (www.ringorango.com)
Impreso en España.

Investigadora principal:
Dra. Mª Luisa Fanjul

Coordinadores:

Capítulo 1
Dr. Alejandro Barceló

Capítulo 4
Dr. Luis Aparicio Ordaz
Dr. Roberto Morales

Capítulo 5
Dr. Jose Ramón Sarmiento
Dr. José Rodríguez
Lda. Mª Jesús Cardete

Investigadores:
D. Pablo Molero
D. Ian Sánchez
D. Andrés Cartes
Dña. Miriam Caba
Dña. Raquel Sánchez
D. Julio César Úbeda
Dña. Heidi Diana Bravo

ÍNDICE GENERAL

0 MEMORIA DE INVESTIGACIÓN

1. JUSTIFICACIÓN DEL OBJETO DE ESTUDIO

La delincuencia informática se configura como uno de los grandes problemas en materia delictiva de los últimos años. La falta de información al respecto unida a la baja percepción de riesgo por parte de las empresas y al hecho de que la comisión del delito vaya, en muchas ocasiones, un paso por delate de los avances realizados en materia de prevención, convierten los ciberataques en una amenaza constante para el entorno empresarial.

En este contexto, el presente proyecto de investigación aborda el ciberdelito desde dos ámbitos claramente diferenciados.

Por un lado pretende unificar criterios para poder ofrecer una clasificación de las técnicas y herramientas utilizadas en este tipo de delito, con el objetivo final de cubrir el vacío de información existente en relación con la seguridad en el ciberespacio y, por otro lado, ofrece una caracterización del ciberdelincuente a través de diferentes variables tales como personalidad, nivel de conocimientos y especialización informática y en sistemas de red y lugar de comisión del acto delictivo.

Igualmente, se realiza una investigación cualitativa para determinar el conocimiento del empresario español de las diferentes amenazas en materia de ciberseguridad y su percepción de peligro ante la posibilidad de un ataque.

1.1. GRADO DE INNOVACIÓN

La existencia de un vacío en el conocimiento teórico-práctico especializado sobre el ciberdelito fija el principal objetivo de la investigación, puesto que la falta de información y de unicidad en los criterios para la evaluación de los ciberataques, condicionan de forma alarmante los protocolos de actuación tanto preventivos como en los casos en los que el ciberataque deja de ser una amenaza y se convierte en una realidad.

En este contexto la **innovación de las aportaciones** que se realizan a lo largo del estudio quedarían definidas de la siguiente forma:

— Tras comprobar que no existe consenso en el análisis de las herramientas y técnicas utilizadas en los ciberataques empresariales, se propone una **clasificación inédita** de las herramientas y las técnicas de comisión de los ciberataques contra la empresa, estableciéndose una relación directa entre ambas.

— De la misma manera, la no existencia de una caracterización claramente definida del perfil del ciberdelincuente, configura la **segunda aportación inédita** al análisis del cibercrimen, que se concreta en la presentación del primer perfil psicopatológico del ciberdelincuente empresarial, atendiendo a las cuatro ramas de estudio de la psicología criminal: psicosis, neurosis, psicopatías y trastorno de la personalidad antisocial. Completando este perfil con las siguientes variables: (1) nivel de conocimiento informático y (2) lugar de comisión del acto delictivo (dentro o fuera de la empresa).

— Por último, se desarrolla un **diseño de investigación cualitativo** con el fin de profundizar en la percepción de riesgo y nivel de conocimiento que tiene el empresario español de los ciberataques dirigidos contra las organizaciones.

La investigación se completa con un **análisis de la evolución de delito** hasta llegar a los ciberataques, con el objeto de situarlos en el tiempo y entender mejor cuál es el punto de partida.

1.2. UTILIDAD E IMPLICACIONES ESTRATÉGICAS

Las acciones preventivas y de actuación relacionadas con los ciberdelitos, como en cualquier actuación criminológica, están condicionadas por el conocimiento previo que se tenga tanto del delito (herramientas, técnicas o escenarios) como del delincuente personalidad, motivaciones y modus operandi).

En este sentido, los protocolos de actuación deben centrarse en un estudio profundo de las técnicas y herramientas para ciberdelinquir así como en el perfil de los posibles ciberdelincuentes.

En ambos casos, el objetivo es prevenir y detectar posibles vulnerabilidades y brechas en los sistemas informáticos y en red, así como identificar a los posibles perfiles susceptibles de cometer el delito con anterioridad a la comisión del mismo.

Por tanto, *la presente investigación pretende ser el punto de partida en la toma de decisiones en el momento de establecer medidas de prevención tanto en las empresas y organizaciones, como en el momento de establecer pautas para la creación de productos y servicios de seguridad que se adecuen a las necesidades del mercado.*

En este contexto, las premisas en las que se fundamenta el estudio quedan definidas de la siguiente forma:

— El estudio y clasificación de las herramientas y las técnicas para la comisión del ciberdelito tienen como consecuencia una mayor adecuación de los sistemas de prevención y actuación contra los ciberataques, así como una mayor rapidez en la adopción de medidas cuando el delito ya ha ocurrido.

— El análisis de las herramientas y técnicas utilizadas en los ataques en el ciberespacio permite detectar vulnerabilidades y brechas que de otra manera podrían pasar desapercibidas.

— Identificar comportamientos sospechosos dentro de la empresa implica la prevención de posibles ciberataques.

— Conocer el comportamiento del ciberdelincuente atendiendo a sus motivaciones supone la temprana detección del delito.

— La concienciación de los empresarios de que cualquier empresa es susceptible de ser atacada es el punto de inflexión entre empresas que no poseen ningún tipo de sistema de seguridad, y empresas que, conscientes de los peligros existentes en la red, no solo se protegen de posibles ataques exteriores, sino de ataques protagonizados por sus propios empleados.

En este sentido, como se verá más adelante, los resultados son concluyentes. Los empresarios españoles a pesar de reconocer la amenaza que actualmente suponen los ciberataques, no protegen adecuadamente sus equipos, mostrando, además, un desconocimiento sobre el tema, que va en perjuicio de su seguridad.

Este hecho debería alertar a las compañías que se dedican a la comercialización de productos y servicios de seguridad, quienes deberían, a su vez, realizar como paso previo al desarrollo y venta de sus productos y servicios una labor de información, concienciando de las consecuencias de mostrarse como una empresa vulnerable, no solo frente a las amenazas externas, sino ante los propios trabajadores.

2. ESTRUCTURA DE LA INVESTIGACIÓN

La investigación se estructura en torno a **cuatro bloques** fundamentales de análisis (véase Tabla 2.1.):

(1) El primer bloque coincide con los capítulos 1 y 2.

(2) El segundo bloque se corresponde con el capítulo 3.

(3) El tercer bloque coincide con el capítulo 4.

(4) Por último, el bloque 4 se corresponde con el capítulo 5.

TABLA 2.1. Estructura de la investigación

BLOQUE	CAPÍTULOS
BLOQUE 1: Conceptualización, caracterización y evolución del ciberdelito empresarial.	Capítulo 1: Evolución histórica del delito: de la Escuela Clásica al Ciberdelito. Capítulo 2: Concepto y clasificación del ciberdelito: el ciberdelito empresarial.
BLOQUE 2: Clasificación del ciberdelito empresarial.	Capítulo 3: Caracterización y clasificación del ciberlito empresarial.
BLOQUE 3: Perfil del ciberdelincuente.	Capítulo 4: El ciberdelincuente empresarial: perfil y mapas de comportamiento.
BLOQUE 4: Percepción del ciberdelito empresarial en España.	Capítulo 5: Análisis de la perspectiva empresarial sobre el ciberdelito en España: enfoque cualitativo.

FUENTE: Elaboración propia

A continuación se detalla el planteamiento de cada uno de los bloques identificados junto con las conclusiones alcanzadas.

BLOQUE 1
Conceptualización, caracterización y evolución del ciberdelito empresarial

Los contenidos del BLOQUE 1, como se puede observar en la Tabla 2.1., conforman los dos primeros capítulos de la investigación y responden al marco teórico de la misma.

El **capítulo 1** pretende ser un acercamiento a la evolución del delito que permita delimitar el concepto hasta llegar a la definición de ciberdelito.

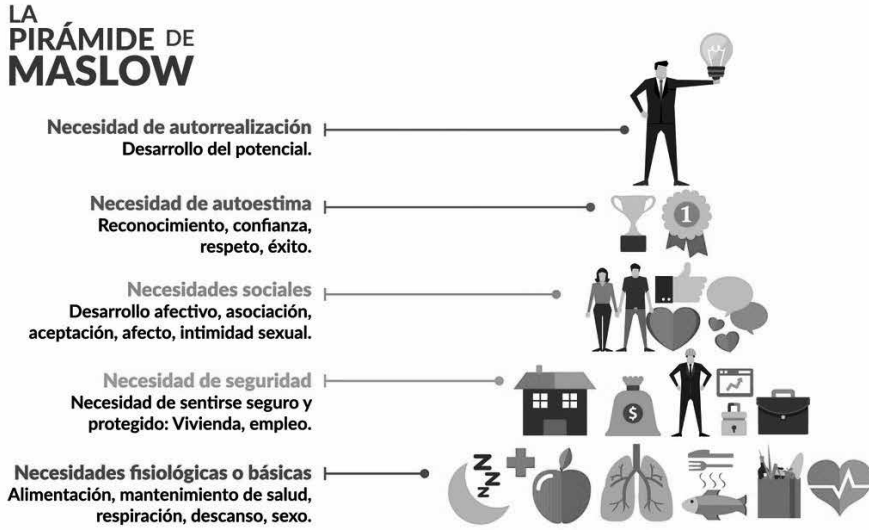
Para ello se realiza un breve análisis de la historia de la delincuencia y se propone un estudio de las diferentes teorías que han surgido a

lo largo de los dos últimos siglos, con el objeto de determinar cómo el entorno social y los factores de situación son concluyentes, tanto en la concepción como en el desarrollo de los actos delictivos.

Concretamente se asocia **el nacimiento del ciberdelito con la aparición y posterior desarrollo de las nuevas tecnologías (TIC)**, si bien, se observa como las motivaciones para cometer cualquier acto delictivo son siempre las mismas, independientemente del tipo de delito que se cometa, fundamentándose en estados de carencia que se satisfacen a través del propio acto criminal y que culminan con el cumplimiento de deseos orientados a cubrir necesidades, tales como la estima.

En este contexto, se determina que el ciberdelincuente asocia la comisión del delito a la necesidad de crecimiento personal a través de recompensas económicas, unida a la necesidad de pertenencia a grupo, reconocimiento y autorrealización. (Este punto se desarrollará con detenimiento en el Capítulo 4, a través del estudio del perfil psicológico del ciberdelincuente) (Véase Imagen 2.1.).

IMAGEN 2.1. Clasificación de las necesidades de crecimiento



FUENTE: http://static3.depsicologia.com/

En lo referente al **capítulo 2** se aborda la evolución del ciberdelito y se realiza una primera clasificación a partir de la tipología de ciberdelitos analizados por Quimbo (2004) según el sujeto pasivo o víctima del mismo.

Como consecuencia del análisis realizado se conceptúa el ciberdelito en la empresa como una clase de delito específico y se concluye que el ciberdelito se ha convertido en una de las principales amenazas para el entramado empresarial español, pudiendo afirmarse que no sólo crece el número de actos delictivos sino que los delincuentes van perfeccionando sus ataques, adelantándose, en muchas ocasiones, a los propios desarrollos tecnológicos de prevención. Esto supone la existencia de una serie de brechas en materia de seguridad informática complicadas de parchear.

Adicionalmente, se detecta, hoy en día, las empresas se enfrentan a un total desconocimiento de lo que puede suponer un ataque de este tipo para su organización, ya que, por un lado, apenas existe información fiable al respecto, siendo las principales fuentes aquellas compañías cuya actividad se orienta a la comercialización de productos y servicios que combaten este tipo de acciones y, por otro, la percepción de que un ciberataque nunca se dirigirá hacia su estructura.

Igualmente, se concluye que uno de los grandes problemas del ciberdelito en general y contra las empresas en particular es la empatía que despiertan en la sociedad los ataques en el ciberespacio. Considerando al delincuente como un héroe cuando es capaz de invadir espacios privados, robando información y poniendo a prueba a las autoridades, tal es el caso, de la admiración que llegan a despertar todos aquellos que han conseguido acceder a los archivos clasificados de la CÍA o del FBI.

Por último, se observa la necesidad de poner en práctica toda una serie de protocolos de actuación encaminados a proteger a la organizaciones y a concienciar a los empresarios de la amenaza que

supone para su compañía no adoptar determinadas medidas de seguridad.

BLOQUE 2
Clasificación del ciberdelito empresarial

El **capítulo 3** analiza las diferentes herramientas de las que se dispone actualmente para la comisión del ciberdelito. De la misma manera se relacionan estas herramientas con las diferentes técnicas de ciberataques.

Los resultados obtenidos se muestran en las Tablas 1 y 2 recogidas en los ANEXOS 1 y 2, respectivamente, de la presente memoria de investigación y que suponen el primer intento por unificar toda la literatura existente, hasta el momento, acerca de la clasificación y conceptualización del ciberdelito.

En la **Tabla 1** se definen las herramientas utilizadas en los ciberataques. Para su identificación y clasificación se ha procedido a su caracterización, a la descripción de sus síntomas, a la evaluación de sus riesgos así como a la explicación de los posibles protocolos de prevención. Se han enumerado un total de 11 herramientas.

En la **Tabla 2** se contemplan las técnicas de ciberataque. Igualmente se procede a su identificación y clasificación, a la descripción de sus síntomas, la evaluación de los riesgos, la explicación de los protocolos de prevención junto con la especificación de cuál es la herramienta que suele utilizarse en cada una de las técnicas definidas.

BLOQUE 3
Perfil del ciberdelincuente

El **capítulo 4** de la investigación tiene como punto de partida el crimen y la agresión como una constante en la historia de la humanidad situando la ciberdelincuencia como cualquier otra forma conocida de acto criminal, que difiere de la desviación social tradicional en lo que se ha venido a conceptuar como desviación *online,* donde el delincuente utiliza la tecnología para la comisión del delito utilizando un ordenador, un teléfono inteligente o una PDA.

En este contexto se insiste en que aunque se asiste a la aparición de nueva forma de delinquir en lo que al medio y herramientas ser refiere, así como a la aparición de nuevos escenarios del crimen, las motivaciones para la comisión del ciberdelito son las mismas que empujan al crimen a los delincuentes que actúan en otros ámbitos que nada tienen que ver con las nuevas tecnologías.

Aun así la reciente incorporación del ciberdelito al entorno empresarial justifica el estudio del perfil del ciberdelincuente atendiendo tanto a la capacidad de control del medio donde se comete el delito (conocimiento tecnológico) como a su perfil psicológico.

Como consecuencia el BLOQUE 4 desarrolla un análisis con el objetivo de identificar **el perfil del ciberdelincuente** teniendo en cuenta que su comportamiento puedo estar condicionado por las siguientes variables:

1. Conocimientos Informáticos y nivel de especialización.
2. Variables psicográficas.
3. Situación en la estructura empresarial.

1. Conocimientos informáticos y nivel de especialización

En líneas generales puede afirmarse que para la comisión de un delito informático si bien se requieren de unos conocimientos mínimos relacionados con el medio informático, los sujetos activos de los mismos no precisan conocimientos técnicos cualificados, bastando con un coeficiente intelectual medio y la oportunidad de realizar el hecho. Por tanto, en primera instancia podríamos clasificar a los ciberdelincuentes en dos categorías diferenciadas:

1. aquellos que manejan con facilidad los ordenadores y son expertos conocedores de los sistemas en red y
2. aquellos cuyos conocimientos y habilidades no podrían ser categorizados en el nivel de expertos.

En el primer caso, los ciberdelincuentes se especializan en delitos informáticos mientras que en el segundo la tecnología simplemente es un medio para cometer el delito. De ahí que el perfil de ambos sea normalmente diametralmente opuesto, puesto que mientras para el primero el acto en sí supone un reto y contribuye a su crecimiento personal a través de la adquisición de conocimientos específicos y el reconocimiento, para el segundo el móvil suele relacionado con la venganza personal o con la posibilidad de obtener algún beneficio económico, si bien un grupo reducido de estos aspira a perfeccionar su técnica en la búsqueda constante de autorrealización o pertenencia a grupo.

En este sentido, se propone una segmentación del ciberdelincuente que coincidiría con los siguientes grupos:

1. Maestro o experto.
2. Intruso.

En el caso del **maestro o experto** los perfiles identificados se enmarcan dentro del concepto de *hacker,* término que hace referencia a todas aquellas **personas o comunidades con un nivel de especialización alto en el manejo de las nuevas tecnologías**.

Concretamente los **maestros o expertos** coincidirían con la figura de los *black hat hackers* (Véase Tabla 2.2.) y englobarían a todos aquellos ***hackers* cuya finalidad es vulnerar los sistemas informáticos de la empresa con la único objetivo de obtener beneficios económicos o reconocimiento.**

TABLA 2.2. Clasificación de los Hackers

HACKER		
Persona o comunidad experta en el área informática y entorno digital, que domina el lenguaje de programación, la manipulación de hardware y software y las telecomunicaciones, dedicando sus conocimientos y esfuerzos a intervenir o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o servicio.		
White Hat Hacker	***Grey Hat Hacker***	***Black Hat Hacker***
Son los *Hackers* Éticos o Tradicionales. Utilizan sus conocimientos técnicos para descubrir vulnerabilidades o brechas en los sistemas informáticos, y ponerlas en conocimiento del administrador del sistema con el fin de solventarlas.	Sujetos cuya ética es ambigua. Poseen conocimientos comparables a los de un *Black Hat Hacker* que utilizan para encontrar vulnerabilidades o fallos de seguridad, ofreciéndose, posteriormente a solventarlos bajo un acuerdo económico.	Los sombreros negros se dedican a realizar actividades orientadas a vulnerar la seguridad de sistemas, ingresar de forma violenta e ilegal a sistemas privados y extraer información restringida con fines económicos o personales.

FUENTE: Elaboración propia

Los **intrusos,** por su parte, son aquellos ciberdelincuentes cuyos conocimientos informáticos son escasos, limitándose, incluso, a ser meros ejecutores del ataque, al haber adquirido previamente el *software* malicioso (malware) en mercados negros, relacionados, en muchas ocasiones, con la venta ilegal en la *Deep Web* o Internet Profunda (véase Tabla 2.3.) (véase Infografía Anexo 3):

TABLA 2.3. Clasificación del ciberdelincuente en función de sus conocimientos tecnológicos

MAESTROS O EXPERTOS	INTRUSOS
Máximos exponentes de la ciberdelincuencia especializada. Si bien según su filosofía pueden actuar de buena fe poniendo sus conocimientos al servicio social y de la empresa.	Delincuentes informáticos con un nivel de conocimientos tecnológicos bajos. Su móvil puede estar relacionado con la venganza personal, la pertenencia a grupo y el reconocimiento social. En algunos casos sus fines pueden ser económicos.

FUENTE: Elaboración propia

2. Variables psicográficas

Para el estudio de las variables psicográficas del ciberdelincuente empresarial se ha profundizado en el análisis de la personalidad de los ciberdelincuentes atendiendo a su personalidad, el modus operandi y la motivación.

Para abordar la investigación, en primera instancia, se ha revisado la literatura existente sobre el comportamiento delictivo condicionado por la posibilidad de padecer uno de los cuatro trastornos de la personalidad tipificados en la psicopatología: **psicopatía, neurosis, psicosis y trastorno de la personalidad antisocial.**

Igualmente se ha analizado el comportamiento de aquellos sujetos que no padeciendo ningún trastorno de la personalidad inician una carrera criminal en el ciberespacio.

Los resultados obtenidos caracterizan dos tipos de ciberdelincuentes diferenciados, los psico-ciberdelincuentes y los normo-ciberdelincuentes (véase Tabla 2.4.):

TABLA 2.4. Tipos de ciberdelincuentes (Perfil Psicológico)

PSICO-CIBERDELINCUENTE	NORMO-CIBERDELINCUENTE
Es aquel sujeto que adopta un comportamiento delictivo en la red, valiéndose, en muchas ocasiones, de sus conocimientos tecnológicos y del anonimato que le confiere el entorno digital, adoptando un comportamiento caracterizado por la hostilidad, un bajo ajuste emocional y falto de empatía. Dirigido, a su vez, por una desviación psicopatológica (psicosis, neurosis, trastorno de la personalidad antisocial o psicopatía). La motivación del delito suele atender a la búsqueda de reconocimiento, seguridad y pertenencia a grupo. Identificando un grupo muy reducido de psico-ciberdelincuentes cuya motivación sea puramente económica.	Se identifica el normo-ciberdelincuente como aquel delincuente en la red que comete actos delictivos sin sufrir ninguna de las psicopatologías propias del perfil del psico-ciberdelincuente. Las características del delito suelen ser las mismas que el en caso de los cometidos por los psico-delincuentes, sin embargo, la motivación es diferente, ya que rige el beneficio económico por encima de cualquier otro.

Fuente: Elaboración propia

Posteriormente, la investigación define diferentes perfiles en función de la clasificación anterior. En total se caracterizan un total de 11 perfiles, 7 psico-ciberdelincuentes distribuidos en 4 grupos diferenciados (véase Tabla 2.5.) y 5 normo-delincuentes distribuidos en 3 grupos (Véase Tabla 2.6., Tabla 2.7. y Tabla 2.8.):

TABLA 2.5. Grupos diferenciados de psico-ciberdelincuentes

CIBER-PSICÓPATA	Se caracterizarán por la falta de ética, remordimientos y empatía hacia la víctima. Pueden incluso llegar a justificar el delito pensando que la culpa es del propio sistema por no estar correctamente protegido. Cuando el ciberdelito es cometido por un *insider* (desde dentro de la organización) no desarrollan ningún tipo de lealtad hacia la empresa de la que forman parte.
CIBER-NEURÓTICO	Son introvertidos y muy sensibles a presiones externas. Normalmente sus habilidades sociales no son muy sofisticadas. Tienden a cometer ciberataques de la mano de un *outsider* que les manipula.
CIBER-PSICÓTICO	Sujetos que sienten que tienen derecho a realizar este tipo de ataques. Sienten que las organizaciones son merecedoras de las consecuencias del delito pudiendo fundamentar este tipo de justificación en delirios o incluso en alucinaciones.
CIBER-SOCIÓPATA	Apenas tienen tolerancia a la frustración y generan actitudes negativas a todo lo que les venga impuesto. Tienen un historial de problemas en los primeros años de vida asociados a los grupos de socialización primarios (familia y escuela). Prefieren el carácter predecible de los ordenadores a las relaciones personales. De tal manera que muchos de ellos reemplazan sus interacciones profesionales o sociales directas y «crean» su propia personalidad *online*.

FUENTE: Elaboración propia

TABLA 2.6. Clasificación de los ciberdelincuentes

PSICO-CIBERDELINCUENTE		NORMO-CIBERDELINCUENTE	
CIBER-PSICÓPATA	**INTEGRADO** Ciberdelincuente-exitoso **NO INTEGRADO** Ciberdelincuente-ejecutor	**CIBER–OPORTUNISTA**	Ciberdelincuente-ventajista
CIBER-NEURÓTICO	Ciberdelincuente-manipulable	**CIBER–COMÚN**	Ciberdelincuente - pandillero Ciberdelincuente – rebelde
CIBER-PSICÓTICO	Ciberdelincuente-enajenado Ciberdelincuente-salvador	**CIBER-HABITUAL**	Ciberdelincuente neo-profesionales Ciberdelicuente-profesional Ciberdelicuentes- a sueldo
CIBER-SOCIOPÁTA	Ciberdelicuente-inadaptado		

Fuente: Elaboración propia

TABLA 2.7. Clasificación de los psico-ciberdelincuentes

PSICO-CIBERDELINCUENTE
CIBER-PSICÓPATA
Ciberdelincuente-exitoso: Sujeto de clase media, media-alta, mayoritariamente varón y cuyo comportamiento estaría condicionado por la búsqueda de nuevas sensaciones a través de la comisión del delito, así como por la obtención de un beneficio de tipo económico. Son profesionales de éxito y su vida personal es aparentemente perfecta. Son narcisistas, tienen una gran capacidad para mentir y manipular, así como una total ausencia de remordimiento.
Ciberdelincuente-ejecutor: El ciberdelincuente-ejecutor responde al perfil de un sujeto que ha crecido en un ambiente marginal, lo que le ha propiciado un estilo de vida antisocial. Son egocéntricos y violentos. No tienen ninguna vinculación real con nadie. Sólo buscan el placer más inmediato e intenso. Disfrutan humillando, por lo que no dudarán en difamar todo aquello que no coincida con su forma de ver las cosas.
CIBER-NEURÓTICO
Ciberdelincuente-manipulable: Los ciberdelincuentes manipulables son personas inseguras de sí mismas como consecuencia de la angustia que padecen. Viven constantemente una situación de miedo que les impide delinquir de motu propio, si bien podrían hacerlo en nombre de otros.
CIBER-PSICÓTICO
Ciberdelincuente-enajenado: Sujeto condicionado por un trastorno delirante que le sume en una serie de creencias falsas cuya consecuencia más directa es la pérdida del contacto con la realidad, como consecuencia, sus acciones son incontroladas y si sitúan fuera de todo sentido común. Se caracterizan por su aspecto descuidado por el desorden en su vida tanto afectiva como social. Suelen ser solitarios y ofrecen una apariencia extraña a los demás. El sujeto enajenado tiene sospechas infundadas y piensa que otros están complotando en contra de él/ella. La imagen de sí mismo es generalmente despreciada.
Ciberdelincuente-salvador: Sujeto que cree haber sido elegido para desarrollar una misión muy importante o para «salvar al mundo» de algún peligro indefinido. Este individuo sufrirá delirios de grandeza que le llevarán a cometer delitos de carácter muy específicos.
CIBER-SOCIÓPATA
Ciberdelincuente-inadaptado: Este tipo de ciberdelincuente no tiene una predisposición a la actividad delictiva, siendo las circunstancias vividas en su grupo de socialización primaria las que en la mayoría de las ocasiones les lleva a iniciarse en la delincuencia.El ciber-inadaptado busca satisfacer necesidades de pertenencia a grupo, autoestima y autorrealización. Tiene problemas de identidad y el reconocimiento público le ayuda a sentirse seguro.

FUENTE: Elaboración propia

TABLA 2.8. Clasificación del normo-ciberdelincuente

NORMO-CIBERDELINCUENTE
CIBER-OPORTUNISTA
Ciberdelincuente-ventajista: El ciber-ventajista responde a una persona ambiciosa y sin escrúpulos. Normalmente encuentra en el delito una forma de enriquecerse. Son personas que llevan una vida normal pero en un momento determinado llevados por su afán de hacer dinero fácil ven en el delito una forma de aumentar sus ingresos. Este tipo de delincuentes medirán muy bien las consecuencias de su delito, analizarán pros y contras y, posteriormente, ejecutarán el ataque.
CIBER-COMÚN
Ciberdelincuente-pandillero: Buscan un beneficio económico a corto plazo a través de un medio que les resulta muy familiar. Pueden actuar en solitario o en grupo, sin embargo, aunque a veces no actúen de forma individual, en ningún caso se puede hablar de crimen organizado. Los ciberpandilleros podrán abandonar la ciberdelincuencia, siendo su carrera delictiva el resultado de la suma de actos vandálicos en la red de forma aislada, o, en su defecto, consolidarán esta carrera convirtiéndose en delincuentes habituales.
CIBER-HABITUAL
Ciberdelincuente-neoprofesional: Este ciberdelincuente supone un paso adelante desde la ciberdelincuencia común para llegar a la ciberdelincuencia profesional, convirtiendo el delito en una forma de vida. Normalmente el ciberdelincuente-neoprofesional responderá al siguiente perfil: — Conocimientos de programación limitados. — Confía en los kits de herramientas para llevar a cabo sus ataques. — Pueden causar daños a los sistemas, ya que no entienden cómo funciona el ataque. — Buscan atención de los medios.
Ciberdelincuente-profesional y Ciberdelincuente a sueldo: La diferencia fundamental entre ambas categorías de ciberdelincuentes es que el primero comete el delito en beneficio propio, mientras que el segundo es contratado por un segundo cobrando por sus servicios.En ambos casos hablamos de dos perfiles de sujetos que han convertido el ciberdelito en su modo de vida, especializándose en esta categoría e iniciando una carrera criminal.

FUENTE: Elaboración propia

3. Situación en la estructura empresarial

El análisis de la variable situacional permite identificar dos tipos de ciberdelincuentes en el ámbito empresarial, aquellos que atentan

desde dentro de la organización y aquellos que atentan desde fuera, pudiendo encontrarse una combinación de ambos.

En el primer caso se hará referencia al **ciberdelincuente *insider*** y en el segundo al **ciberdelincuente *outsider*** *(véase Infografía Anexo 4)*.

El **ciberdelincuente *insider*** es aquel sujeto que actúa desde dentro de la empresa formando parte de la estructura de la misma.

En este sentido, es importante que las empresas comiencen a ser conscientes de que los ciberataques pueden provenir de dentro de la organización, es decir, que los propios empleados pueden ser aquellos que agredan a la compañía.

Igualmente, es importante que se den cuenta que para que un empleado se convierta en un *insider* son muchas las ocasiones en las que no hacen falta unos conocimientos avanzados en materia informática o sistemas de red, puesto que solo necesitan saber diferenciar entre los archivos que les interesen o que puedan usar y el método que van a emplear para la sustracción de datos ya sea por USB, email u otras técnicas.

El **ciberdelincuente *outsider***, por su parte, se define como aquel sujeto que actúa desde fuera de la empresa, pudiendo responder a un nivel alto de especialización o no y a un perfil psicopatológico o a un perfil normalizado (véase Tabla 2.9.):

TABLA 2.9. El ciberdelincuente con respecto a su situación contractual con la empresa

OUTSIDER	INSIDER
Sujeto que actúa desde fuera de la empresa, pudiendo responder a un nivel alto de especialización o no y a un perfil psicopatológico o normalizado.	Sujeto que actúa desde dentro de la empresa formando parte de la estructura de las mismas.

FUENTE: Elaboración propia

BLOQUE 4
Percepción del ciberdelito empresarial

El BLOQUE 4 analiza la percepción que las empresas españolas tienen acerca del ciberdelito y de la posibilidad de ser sujetos pasivos del mismo. Para la realización de esta parte del estudio se optó por un diseño cualitativo, incluyendo 20 entrevistas personales y estableciéndose un único perfil básico de entrevistado que se define como *«directivos y mandos intermedios de empresas, gerentes y propietarios que son susceptibles de sufrir un ciberataque dado el volumen de datos que manejan»,* tomándose en consideración las siguientes variables:

(1) número de empleados de la empresa y

(2) categoría profesional del entrevistado.

Los entrevistados respondieron a un total de 8 preguntas (véase Anexo 5) teniendo plena libertad para manifestar sus respuestas, si bien el hecho de plantear las mismas preguntas en el mismo orden a todos los participantes introduce un fuerte elemento de rigidez en la dinámica de la entrevista.

Los ámbitos de análisis se describen a continuación:

1. Conocimiento de la evolución del ciberdelito empresarial en España.
2. Conocimiento de los tipos de ciberdelitos más frecuentes.
3. Conocimiento de softwares específicos contra el ciberdelito
4. Comportamiento y protocolos de actuación ante el ciberdelito: prevención.

Las conclusiones obtenidas son las siguientes:

1. Conocimiento de la evolución del ciberdelito empresarial en España

Las conclusiones alcanzadas en esta área son las siguientes:

— Las empresas tienen constancia del ciberdelito y del aumento de la actividad delictiva en la empresa.

— Aun así no se informan acerca de los peligros a los que están expuestos, aunque les parezca un tema preocupante y, en muchos casos, manifiesten sentir curiosidad.

2. Conocimiento de los tipos de ciberdelitos más frecuentes

Los ciberdelitos más conocidos son el *phishing*, el robo de identidad y la privacidad y, por último, el *hacking*.

La respuesta obtenida es sorprendente, puesto que el *hacking* es la acción de *hackear* pero no siempre es considerado un delito, tal y como, se expuso en el capítulo 4 sobre el perfil del ciberdelincuente y su nivel de conocimiento informático.

Por otro lado, esta respuesta confirma el desconocimiento en materia de ciberataques, puesto que en la mayoría de los casos ningún empresario contrataría un *hacker*, dado que identifican esta figura con la de un ciberdelincuente.

3. Conocimiento de softwares específicos de contra el ciberdelito

Tras el análisis de las respuestas obtenidas al respecto de la protección de los equipos informáticos, las conclusiones alcanzadas son las siguientes:

— Los virus se reconocen como las principales amenazas en el ciberespacio, por lo que la prevención en la empresa pasa

principalmente por la instalación de un antivirus profesional, en el mejor de los casos, y, en el peor, por la descarga de un antivirus gratuito de Internet.

— La percepción de Apple como invulnerable ante los ciberataques conlleva la no protección de estos equipos.

— En ningún caso se contempla la posibilidad de proteger otros dispositivos como las impresoras o las cámaras de seguridad (Internet de las Cosas).

4. Comportamiento y protocolos de actuación ante el ciberdelito: prevención

En lo que respecta a la adopción de medidas, las respuestas obtenidas permiten concluir que:

— Actualmente las empresas no adoptan medidas de seguridad específicas en materia de ciberdelito.

— Las medidas más populares son el *firewall* y los antivirus.

— El tamaño de la empresa está relacionado con las medidas adoptadas, siendo las PYMES las que menos percepción de peligro tienen.

— Igualmente, son los mandos intermedios de la empresa los que sienten con más frecuencia la desprotección.

Esta respuesta está relacionada con la confianza que los empresarios manifiestan tener hacia sus empleados, a pesar de ser conscientes de que pueden ser atacados por uno de ellos en cualquier momento.

En este sentido, los entrevistados confirman que en relación a sus trabajadores las únicas de medidas de seguridad que adoptan en materia de seguridad es la restricción de navegación por redes sociales y los registros del historial de dicha navegación.

3. CONCLUSIONES

1. A pesar de la evolución del ciberdelito contra la empresa se asiste a una falta de información que siga criterios unificados. En este sentido es importante destacar tres puntos:
   — La no existencia de una definición de ciberataque universal.
   — La no existencia de una clasificación del ciberdelito atendiendo a las técnicas y las herramientas.
   — La no existencia de un perfil del ciberdelincuente.
2. Por otro lado, se asiste a un total desconocimiento por parte del empresario de lo que puede suponer un ciberataque. Su percepción de vulnerabilidad es muy baja, no realizando ningún tipo de acción específica en esta materia, puesto que:
   — No identifica al empleado como una amenaza.
   — Sus protocolos de prevención se reducen a las restricciones de navegación entre sus empleados y a la instalación de antivirus y *firewall*.
   — No contempla la posibilidad de que el resto de sus equipos conectados en red puedan ser amenazados.

Adicionalmente, se concluye que:

1. Existe una confusión conceptual entre herramienta y técnica. Muchas herramientas son utilizadas en diferentes ataques.
2. Las vulnerabilidades son descubiertas con posterioridad al ataque, lo que impide la capacidad de reacción de las empresas.
3. Es necesario avanzar con mayor rapidez que los ciberdelincuentes para poder subsanar cuanto antes las brechas en los sistemas en red. En esta línea, se hace necesario invertir en I+D+I.
4. La delincuencia en el medio *offline* solo difiere de la delincuencia *online* en el medio en el que comete el delito, pudiendo variar,

por tanto, el modus operandi y la escena del crimen, sin embargo sus motivaciones son exactamente las mismas.

5. Conocer a tu adversario siempre es una ventaja. En este sentido, analizar el comportamiento del ciberdelincuente nos permite adelantarnos a sus movimientos al poder detectar hábitos sospechosos.

Por último, la investigación determina que mientras no se produzca un cambio conductual en los empresarios españoles, es muy difícil parar el ciberdelito. Puesto que la no percepción de inseguridad unida al hecho de que ninguna compañía piensa que es susceptible de ser atacada, limita las posibilidades de prevención a través de la comercialización de sistemas de seguridad.

1 EVOLUCIÓN HISTÓRICA DEL DELITO: DE LA ESCUELA CLÁSICA AL CIBERDELITO

RESUMEN

El crimen y el delito han sido abordados históricamente desde diversas disciplinas, en un intento por explicar cuáles son las razones fundamentales por las que el hombre delinque. En este sentido, a lo largo de los años se han analizado la influencia de aspectos como la personalidad, la actitud, la inclusión social o la marginalidad, la cultura o los procesos de socialización, entre otros, como determinantes del comportamiento humano.

En el presente capítulo se propone un recorrido por las diferentes teorías criminológicas que han surgido en últimos siglos, con el objetivo de señalar determinadas variables tales como el entorno social y los factores de situación como concluyentes tanto en la concepción como en el posterior desarrollo de las formas de delinquir. Concretamente en el último epígrafe se concluye que el ciberdelito es consecuencia no solo de los avances tecnológicos, si no que se encuadra dentro la propia evolución de las relaciones humanas.

PALABRAS CLAVES: evolución del delito, positivismo, escuela clásica, sociología, psicología, tendencias, ciberdelito.

ABSTRACT

Since the beginning of mankind, criminal activities have been studied through several disciplines. In an attempt to explain the main reasons of why man commit crimes or performs aggresive acts, psycology, biology or sociology have analyzed the influence of aspects such as the personality, attitude, so-

cial integration or culture as determinants of human behavior. In this chapter, a study about the historical evolution of delinquency is carried out and an analysis of the many theories that have emerged during the last two centuries is proposed, in order to figure out how social environment determines the conception and development of the different forms of crimes contemplated in the subsequent chapters, until the cybercrime.
KEYWORDS: evolution of crime, positivism, classical School, sociology, psychology, trends, cybercrime.

1.1. EL SIGLO XIX

La concepción de delito en el siglo XIX está profundamente marcada por los acontecimientos históricos que tienen lugar en esta época. Numerosos juristas, psicólogos y sociólogos profundizan tanto en el perfil del delincuente como en las razones que llevan al ser humano a cometer actos criminales.

Se asiste al nacimiento de concepciones que nada tienen que ver con teorías anteriores, comenzando a entender el delito como un hecho que no puede desvincularse del entorno en el que se comete.

1.1.1. La Escuela Clásica

El siglo XIX marca el inicio de una nueva definición del delito que supone una ruptura con respecto al siglo XVIII. Los hijos de la Revolución Francesa comienzan a reivindicar los derechos del hombre bajo la tutela del Estado Liberal no intervencionista, que rechazaba todo lo que estuviera relacionado con el Absolutismo. Nace de esta forma la Escuela Clásica.

Los clásicos entenderán el delito como un ente jurídico abstracto aislado de cualquier fenómeno natural y social, desvinculando al

delincuente del medio donde realiza el acto y caracterizándolo como un ser racional dotado de libre albedrío, que obra sin sujeción a influencias extrañas.

Entre los méritos de la Escuela Clásica se pueden mencionar los siguientes:

— El hecho de haber realizado un estudio sistemático sobre el delito como ente jurídico.

— El haber logrado la abolición de las penas infamantes o deshonrosas.

— El haber rodeado al imputado de garantías tales como el principio de legalidad frente al poder sancionador del Estado.

No obstante y a pesar de los avances realizados por los clásicos en lo que al delito y su concepción se refiere, se debe tener en cuenta que esta corriente ofrece una visión muy limitada al considerar el delito únicamente como un ente jurídico, restando importancia al estudio del delincuente e ignorando que el delito, por el hecho de ser consecuencia de una acción humana, tiene como protagonista a una persona.

Aun así, la evolución del concepto de delincuencia hacia un concepto más amplio donde los delincuentes pasan a formar parte de la configuración de la sociedad, convirtiéndose en una variable más en las relaciones que se establecen en ésta, como consecuencia de toda una serie de factores internos y externos, tales como el clima, la cultura, la actitud, la percepción o el aprendizaje, no se producirá hasta mediados de este siglo con los positivistas (Gómez, 2016).

1.1.2. El positivismo: Lombroso, Garófalo y Ferri

Los positivistas suponen el primer intento de dar una explicación a los comportamientos delictivos asociándolos directamente con el estudio del perfil psicológico de las personas susceptibles de cometer un delito.

De esta forma, autores como Lombroso, Ferri y Garófalo, máximos exponentes del positivismo, clasifican al delincuente y determinan que su comportamiento está claramente definido por toda una serie de taras genéticas.

Concretamente, Lombroso identifica un conjunto de rasgos físicos comunes a todos aquellos que delinquen de una forma continuada en el tiempo y establece siete grupos de delincuentes (Auladerecho, 2013):

1. El Criminal Nato o Atávico: criminal que presenta signos de inferioridad orgánica y psíquica, tales como menor capacidad craneal, gran capacidad orbitaria, impulsividad o falta de remordimientos.
2. El Delincuente Moral: sujeto cuyo estado psicopatológico le impide o le perturba la normal valoración de la conducta desde el punto de vista moral, pero no anula su capacidad cognoscitiva y volitiva. En este caso, Lombroso hace referencia a sujetos que no son capaces de convivir en sociedad y que desarrollan sentimientos de odio con o sin motivos. En líneas generales establece que son personas que odian con o sin motivos, crueles y/o indisciplinados.
3. El Delincuente Epiléptico: individuo que sufre de epilepsia y comete a causa de esta enfermedad un delito. Generalmente son muy violentos.
4. El Delincuente Loco: en esta clase de delincuentes el autor considera al alcohólico y al histérico. Además, Lombroso establece diferencias entre los delincuentes locos y los locos delincuentes, siendo los locos delincuentes los enfermos dementes, sin capacidad de entender o de querer, que cometen algún crimen sin saber lo que hacen, mientras que el delincuente loco es el sujeto que ha cometido un delito y después enloquece en prisión.

5. El Delincuente Ocasional: a los delincuentes ocasionales Lombroso los divide en pseudo-criminales y criminaloides. Los primeros son los que cometen delitos involuntarios, pero no por eso son menos punibles. Son los autores de delitos en los cuales no existe ninguna perversidad, y que no causan ningún daño social, pero que son considerables ante la ley. Los segundos son sujetos con cierta predisposición al delito, pero que en ningún caso lo hubieran cometido de no haberse presentado la oportunidad.
6. El Delincuente Pasional: Lombroso define al delincuente pasional como un delincuente hombre, de entre 20 y 30 años, con una afectividad exagerada y una tendencia clara al suicido inmediatamente después de cometer el delito.
7. La Delincuente Femenina: en este caso, el autor no llega a conclusiones definitivas sobre el perfil de la mujer delincuente, si bien las cataloga como verdaderos monstruos dado que las consecuencias del delito para ellas son dobles al sufrir un mayor ostracismo legal y social.

Actualmente, la clasificación propuesta por Lombroso podría servir para identificar y clasificar determinados actos delictivos, si bien esta caracterización debe hacerse siempre atendiendo a la evolución que la criminología ha experimentado a lo largo del siglo XX de la mano de la Psicología, la Sociología y el Derecho.

Por ejemplo, en el caso Frizl, el electricista que, con antecedentes por violación, encerró a su hija durante 25 años en su sótano y mantuvo relaciones con ella, teniendo 7 hijos, se observa un comportamiento marcado por la frialdad, la falta de empatía y la intencionalidad, lo que invita a pensar que se está ante un Criminal Nato, (Garcigalupo, 2014).

Por su parte, Ferri determina que el delito no es producto exclusivo de ninguna patología individual, sino que es un fenómeno social y que, además, es el resultado de la acción de factores individuales, físicos y sociales. Estos factores se describen a continuación:

1. Factores antropológicos o individuales: constitución orgánica del individuo, constitución psíquica y caracteres personales como raza, edad, sexo o estado civil.
2. Factores físicos o telúricos: clima, estaciones y temperatura.
3. Factores sociales: densidad de población, opinión pública, familia, moral, religión, educación o alcoholismo.

A día de hoy, muchos de los factores analizados por Ferri siguen teniendo vigencia en el análisis del delito. De hecho, uno de los aspectos más estudiados en relación con el comportamiento humano es la influencia de la climatología en el estado de ánimo. En este contexto, Martínez (2011) señala que existe una íntima relación entre las sensaciones de tristeza y cansancio y las condiciones meteorológicas, aumentando la agresividad durante las estaciones más lluviosas.

Por otro lado, para Garófalo, el hombre delincuente responde a un modelo de deficiencia psíquica o moral, de carácter hereditario, con una falta de sentimientos altruistas e incapacidad para vivir en sociedad. Además, defiende el bien de la sociedad por encima de todo, aunque para ello hubiese que eliminar a los individuos causantes del mal común.

Hoy por hoy, la visión del delito que ofrece Garófalo está muy superada. Autores como Jara y Ferrer (2005) apuntan a que la genética no está relacionada con la delincuencia, al entender que un gen no puede contener la predisposición al crimen sino que tendría que ser la totalidad de los genes, algo prácticamente imposible por la división de genes parental.

CUADRO 2.1.

Evolución del concepto de delito: de la Escuela Clásica al Positivismo

	Escuela Clásica	Escuela Positiva
Concepto de delito	Es un ente jurídico.	Es un ente de hecho natural y social, y no solamente un ente jurídico.
Responsabilidad	El libre albedrío. Su origen es producto de causas antropológicas, físicas y sociales.	Fundamenta la responsabilidad penal en Social. Su origen es producto de la inteligencia, voluntad y libertad.
Delincuente	Parte del supuesto de la normalidad del delincuente no exige que la pena se adapte a él. No estudia al delincuente.	Ser anormal. Estudia al delincuente.

Adaptado de http://cienciasjuridicasuesfmo.blogspot.com.es

1.2. EL SIGLO XX

La llegada del siglo XX supone un avance en el concepto de delincuencia, abordando el estudio de los actos criminales atendiendo a cuestiones como la evolución social y los procesos de adaptación del ser humano a su entorno.

1.2.1. Maxwell y Ernest Belling: la crítica social

A principios del siglo XX, las concepciones positivistas son adoptadas por Maxwell con el objeto de conocer mejor los delitos más habituales de la época: los robos y los hurtos como consecuencia de las necesidades biológicas del individuo. De esta forma, el autor realiza una primera aproximación al delito como una forma adaptativa del ser humano a las condiciones sociales en las que vive y las une al concepto de supervivencia.

> *"Los que se hallan en esta imposibilidad de procurarse las cosas necesarias para la existencia pueden, con una apariencia de razón, negarse a cumplir deberes que les son impuestos sin compensación equitativa. Pueden decir que la ruptura del lazo social no procede de ellos, sino del grupo que les deja morir de miseria"* (Maxwell, 1914).

Maxwell justifica así el delito y añade que es la propia sociedad la que provoca la delincuencia, al forzar una situación precaria que lleva al hombre a romper los límites de la legalidad, con el fin de satisfacer sus necesidades o las de sus familiares.

> Las teorías de Maxwell sobre el comportamiento social respecto a la delincuencia estarían más aceptadas actualmente que las de Lombroso. El delito asociado a la satisfacción de estados de carencia ligados a necesidades básicas continúa siendo una razón para generar actitudes empáticas hacia el delito y el delincuente.

Por su parte, autores como Ernest Belling comienzan a defender la idea de que los hechos delictivos evolucionan al mismo tiempo que

la sociedad y señalan que el avance de las tecnologías propicia la aparición de nuevos métodos para la consecución de fines ilícitos.

1.2.2. Friedlander: los grupos de socialización primarios

Durante la primera mitad del siglo XX se asiste a una tendencia decreciente en la delincuencia de las sociedades occidentales, incrementándose a partir de la II Guerra Mundial. Las causas de este incremento no fueron aleatorias, ya que diversos estudios demuestran que una exposición a la violencia como puede ser una guerra, provoca en las personas situaciones de estrés, lo que produce un mayor grado agresividad en el comportamiento de los individuos.

Igualmente, en esta época, la figura de la madre no estaba tan consolidada como figura de poder en la casa y, como consecuencia, los niños ya no tenían un referente que les impidiera realizar cualquier acto delictivo.

En este contexto, Friedlander (1951) afirma que existe un estado de delincuencia presente de forma latente que se fundamenta en un carácter antisocial que se adquiere en las primeras relaciones que se desarrollan en el seno del primer grupo de socialización. Si bien para que estas conductas afloren tendrán que darse toda una serie factores que sirvan de activadores tales como las malas compañías, el trabajo inadecuado o una situación familiar permisiva cuya consecuencia directa pueda relacionarse con la falta de valores o normas sociales.

A medida que los niveles de precariedad provocados por la II Guerra Mundial eran casi inexistentes y el control social comenzaba a estabilizarse, los niveles de delito se estabilizan; si bien entre 1970 y 1990 se asiste a un nuevo repunte que alcanzará las cifras más altas a partir del año 2000.

Este hecho es debido, entre otros, a la movilidad geográfica, ya que en muchas ocasiones a las personas que abandonan sus países de

origen no se les da facilidades para su integración en la sociedad, siendo un causante de la creciente globalización de las actividades delictivas (Avilés, 2002).

1.2.3. Los primeros avances tecnológicos: el delito informático

El Departamento de Justicia de Estados Unidos define el delito informático como *«cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución».*

Otros autores, como Parker (2006), definen los abusos informáticos como *«cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio».*

1.2.3.1. Nacimiento y evolución del ciberdelito

Durante la segunda mitad del siglo XX se asiste al nacimiento de los primeros ataques informáticos, estando este hecho relacionado con el desarrollo de las nuevas tecnologías. Concretamente en los años 60, este tipo de delito se caracterizaba por la destrucción de dispositivos electrónicos.

Ya en los años 70, los avances tecnológicos propician la aparición de otro tipo de actos delictivos relacionados con la utilización ilícita de sistemas operativos y la falsificación de datos informáticos. El fraude informático causó un gran número de pérdidas durante esta década en países como Estados Unidos.

En este sentido, Hernández (2009) señala que la difusión de los ordenadores en el mundo empresarial supuso que la mayoría de las manifestaciones de la delincuencia informática tuviesen relación con la delincuencia económica, siendo las más comunes el fraude informático, la manipulación de datos, los sabotajes informáticos, o

los espionajes empresariales. Hasta el punto de que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático o, al menos, éstas eran las principales manifestaciones del mismo.

Posteriormente, en los años 80, con la popularización de los ordenadores personales aumenta el número de ataques informáticos. En esta década prolifera el deseo de posesión de la figura del *software* y con éste la intención de piratearlo.

El primer ordenador personal «asequible», llamado Altair 8800, se vendió en los años 70. Este modelo fue seguido del Comodore 64, el TRS-80, y en 1980 el PC de IBM, que acerca la informática a todos los que estaban deseando encontrar nuevas formas de aprovechar las capacidades del sistema, siendo las redes del PC las que abren definitivamente las puertas al delito informático.

En este contexto, aparecen en 1986 los primeros virus conocidos. *«(c) Brain»*, *«Bouncing Ball»* y *«Marihuana»* fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los *diskettes*.

Aun así, no será hasta los años 90, con la aparición de la interfaz gráfica (WWW), cuando se produce el cambio más drástico en materia de delincuencia informática, siendo la desgeolocalización de los contenidos una de las grandes amenazas en un nuevo entorno digital que permitía compartir información desde cualquier lugar y ser recogida, igualmente, desde cualquier punto geográfico.

1.3. EL SIGLO XXI

La llegada del siglo XXI supone la consolidación del entorno digital como parte fundamental de la vida cotidiana de las personas. La

nueva era digital propicia el nacimiento de nuevas formas de delito: el ciberdelito.

1.3.1. De los delitos informáticos al ciberdelito

Casabona (2006) define el delito informático como aquel que se vale de elementos informáticos para la perpetración de los mismos y, se refiere al ciberdelito como un conjunto de delitos relacionados con una generación delictiva vinculada a las TIC, en el que interviene la comunicación telemática abierta, cerrada o de uso restringido.

Por tanto, y siguiendo a Rayón y Gómez (2014: 209), se entiende por ciberdelito *«cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito».*

Según Felson (2012: 13), "para llegar a comprender el ciberdelito, para prevenirlo, es muy importante entender la forma en que las personas interactúan con el ciberespacio cada día e incluso cada hora, dónde lo hacen y el modo en que trabajan. Debemos pensar en la relación que guarda el uso del ciberespacio con los extensos patrones de la vida diaria. De hecho, una persona que trabaje en horario nocturno podría intentar hacerse con contraseñas o utilizar los ordenadores de empresas que no estén bajo vigilancia".

En este sentido y partiendo de la afirmación realizada por Quintero (2001: 369), *«internet no es una simple progresión en la evolución tecnológica, sino un cambio revolucionario en los modelos de las relaciones sociales que sirve a la fluidez de los intercambios comerciales y de todo tipo»*, por lo que habría que entender el medio *online* no sólo como innovación y avance social, sino también como un hecho transformador y modificador de la vida en sociedad, que ha permitido al delincuente disponer de nuevas

formas de actuación e incluso crear tipos delictivos ausentes años atrás (Aguilar, 2015).

A día de hoy, puede afirmarse que la ciberdelincuencia ya ha sido aceptada por la sociedad moderna como una forma de delito, sin embargo, los mecanismos preventivos todavía no son adoptados por la mayor parte de los equipos informáticos.

De esta forma, las oportunidades y las vulnerabilidades llevan a que el número de delitos informáticos haya aumentado de forma exponencial en los últimos años.

1.4. CONCLUSIONES

El entorno social, entendiendo por éste el tipo de interacción que establece un sujeto social con otro u otros respecto a ciertas propiedades, características o procesos del entorno y a los efectos percibidos sobre el mismo, según roles y actividades desarrolladas por los sujetos (Granada, 2001), condiciona el comportamiento humano, desarrollando determinadas actitudes de carácter individual y grupal.

Así, a lo largo de la historia, el surgimiento o consolidación de factores sociales relacionados con la cultura, la religión o la tecnología han propiciado la aparición de nuevas formas de delito como consecuencia de un proceso adaptativo a una nueva realidad.

La aparición de estas nuevas formas de delito ha dado lugar a la elaboración de numerosas teorías en aras de explicar el hecho delictivo en sí mismo. Estas teorías han ido evolucionando desde un concepto meramente jurídico como es el caso de la Escuela Clásica, hasta un concepto que se ajusta más a la realidad que viven los individuos.

En este sentido, Moreno *et. al.* (2006) hacen referencia a toda una serie de elementos que son fundamentales para entender el desarrollo de determinados comportamientos que se relacionan con el comportamiento delictivo y justifican la aparición de nuevos delitos. Estos elementos se describen a continuación:

1. El espacio social: la cultura y el espacio geográfico en el que se encuentran durante su infancia y/o adolescencia las personas contribuyen a la creación de costumbres, creencias y patrones sociales que afectan a la personalidad del individuo. Existiendo, por ejemplo, una gran diferencia entre las zonas rurales y las grandes ciudades, entre otras razones, por la exposición a los distintos tipos de delitos que se cometen, condicionando el efecto imitación.
2. El barrio: se considera el barrio al entorno en el que se mueve cada persona a diario, aunque no se relacione dentro de ese mismo territorio con su grupo social. Éste influye en la cantidad, el tipo y la gravedad de los delitos cometidos. Dentro de este factor se encuentran las normas sociales inculcadas por el grupo o por la comunidad.
3. La educación: la educación como extensión de la familia y la escuela complementa la enseñanza de los individuos. Esta educación tiene una relación directa con la peligrosidad de cada individuo, de manera que si un individuo recibe una educación en un entorno familiar y escolar en el que la criminalidad está normalizada, el individuo también acogerá esta cultura delincuencial.
4. Religiosidad: se justifican los actos por religión, como una misión, incluyéndose dentro de éstos los actos impulsados por sectas.
5. Economía: las condiciones económicas son uno de los factores más importantes a la hora de provocar situaciones delictivas.

Actualmente, los avances en el campo de las telecomunicaciones se han convertido en un factor social clave en la aparición de nuevas formas de delito que, adecuándose al medio, han conseguido evolucionar de una forma alarmante en los últimos años. Estas nuevas formas de delito están relacionadas con otros factores sociales tales como la cultura, la economía o la religión.

En este sentido, la adaptación de los individuos a nuevas situaciones producidas por cambios en los mecanismos de comunicación con otros individuos está íntimamente ligada a la evolución de los delitos. Las tecnologías de comunicación provocan que los individuos se relacionen de forma diferente, lo que propicia la aparición de nuevos escenarios para cometer delitos cuya intencionalidad sigue siendo la misma.

Por tanto, se puede afirmar que el ciberdelito es una forma de delito consecuencia de la evolución tecnológica, si bien las motivaciones para cometer un acto delictivo continúan siendo las mismas, fundamentándose en toda una serie de estados de carencia que se satisfacen a través del propio acto criminal y culminan con el cumplimiento de deseos encaminados a cubrir necesidades tales como la estima, la pertenencia a grupo o crecimiento.

En el caso concreto del ciberdelito, la necesidad de crecimiento a través de recompensas económicas unida a la necesidad de pertenencia a grupo, reconocimiento y autorrealización, suele ser una constante en el perfil del ciberdelincuente.

1.5. BIBLIOGRAFÍA

AULADERECHO (2013):
http://auladerecho.blogspot.com.es/2013/05/clasificacion-de-los-delincuentes-desde.html
(CONSULTADO EL 11 DE FEBRERO DE 2017)

Aguilar, M. (2015): Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. Revista Criminalidad, 57 (1): 121-135.

Avilés Farré, J. (2002): La delincuencia en España: una aproximación histórica. UNED. Murcia

Beling Ernest (1903): "Die Rechtswissenschaft dé Gegenwart in Selbstdarstellungen" *(La prohibición de las pruebas como límite de la verdad en la instrucción criminal)*. Alemania.

Casabona, C. (2006). "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal" en *El cibercrimen nuevos retos jurídico-penales,* Editorial Comares. Granada 2006, pp. 1-42.

Felson M. (1979): "Social Change and Crime rate trends: A routine activity approach." *American Sociological Review*, vol. 44, no. 4, 1979, pp. 588–608.

Friedlander y Roshier. (1951): Internal migration in England and Wales, 1851 to 1951. Centre for Urban Studies, University College. London.

Garcigalupo E. (2014):
http://www.elimparcial.es/noticia/12775/opinion/el-caso-fritzl:-tenia-razon-lombroso-1.html
(CONSULTADO EL 24 DE FEBRERO DE 2017)

Granada, H. (2001): "El ambiente social" Investigación y desarrollo. Universidad Norte. Colombia. Enero 2001.

Hernández Díaz, L. (2009): "El delito informático" Eguzkilore, Nº 23, San Sebastián, Diciembre 2009.

Jara M., Ferrer S. (2005): *"Genética de la Violencia"*. Revista Chilena de Neuro-psiquiatría. (188-191)

Kremer W., Hammond C. (2013): *"Hikikomori": por qué tantos japoneses no quieren salir de sus cuartos*. BBC Mundo.

Martínez L. (2011):
http://www.actitudfem.com/entorno/trabajo/el-clima-determina-tu-estado-de-animo (CONSULTADO EL 24 DE FEBRERO DE 2017).

Maxwell, J. (1914): *El crimen y la sociedad*, Trad. GONZÁLEZ, J. M., Madrid.

Moreno, T. (2006):
http://www.monografias.com/trabajos98/delincuencia-como-fenomeno-social-y-su-prevencion/delincuencia-como-fenomeno-social-y-su-prevencion.shtml
(CONSULTADO EL 15 DE FEBRERO DE 2017).

Parker, (2006) *Crime by computer* citado en HERNÁNDEZ DÍAZ, L. (2009): "El delito informático" Eguzkilore, Nº 23, San Sebastián, Diciembre 2009, pp. 207.

Parsons Talcott (1990): "Igualdad y desigualdad en la sociedad moderna, o una revisión de la estratificación social", *Sociológica*, núm. 12. Universidad Autónoma Metropolitana.

Quintero, G. (2001): “Internet y propiedad intelectual”, en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Madrid, 2001, págs. 369 y 370

Rayón Ballesteros, M. y Gómez Hernández, J.A. (2014): *Cibercrimen: particularidades en su investigación y enjuiciamiento, Anuario Jurídico y Económico Escurialense*, XLVII (2014) 209-234.

2 CONCEPTO, EVOLUCIÓN Y CLASIFICACIÓN DEL CIBERDELITO: EL CIBERDELITO EMPRESARIAL

RESUMEN

La nuevas tecnologías y la sociedad de la información se han posicionado como uno de los elementos clave en la toma de decisiones tanto en el ámbito empresarial como profesional. El dato y la analítica de datos han dado lugar a nuevas formas de comportamiento fundamentadas en la capacidad de gestionar información. En este contexto, ha surgido conductas antisociales asociados a formas de delito caracterizadas por escenarios y modus operandi desconocidos hasta el momento. En este contexto, el medio digital se configura como un medio donde proliferan nuevas y complejas oportunidades para infringir la ley (Garavilla, 2010; Rayón y Gómez, 2014; Aguilar, 2015).

De esta forma, el ciberdelito ha estado presente desde que se inicia el uso generalizado de Internet y se integra en la sociedad como parte de la cotidianidad. Concretamente, el ciberdelito se generaliza con la irrupción del comercio electrónico, asistiendo a un incremento de la tasa de delitos informáticos en los últimos años.

En este capítulo se aborda la evolución del ciberdelito y se realiza una primera clasificación fundamentada en la tipología de ciberdelitos analizados por Quimbo (2004) según el sujeto pasivo o víctima del mismo. El objetivo es delimitar el ciberdelito en la empresa como una clase de delito específico.

PALABRAS CLAVE: ciberdelito, ciberdelito empresarial, malware, *adware*, tipos de ciberdelito

ABSTRACT

Much has been shown about the benefits that technological media and the use of computing technology contributes to the present society, however the development of computer technologies provides a negative aspect too, becoming the gateway to asocial and criminal behaviour.

The digital media provides new and extremely complex opportunities to break the law, creating the possibility of perpetrating traditional crimes in non-traditional ways (Rayón and Gómez, 2014, Aguilar, 2015).

This way, cybercrime has been present since the beginning of the widespread use of the Internet and has integrated into society as part of everyday life. In particular, cybercrime, as seen in the previous chapter, is generalized with the eruption of e-commerce, witnessing an increase in the cybercrime rate in recent years.

This chapter approaches the evolution of cybercrime as well as a first labelling based on the classification of the cybercrimes analyzed by Quimbo (2004) according to its passive subject or victim. The purpose is to define cybercrime in the company as a specific kind of crime.

KEYWORDS: cybercrime, corporate cybercrime, malware, adware, types of cybercrime.

2.1. CONCEPTO Y CARACTERIZACIÓN DEL CIBERDELITO

El término ciberdelito contempla muchos tipos de delincuencia, siendo algunos de los más conocidos: la intercepción ilegal de datos informáticos, la interferencia de datos, el fraude y la falsificación (Sieber*,* 2008).

En este sentido, Téllez (1997: 103-104) conceptualiza el ciberdelito y lo define como *«la forma típica y atípica, entendiendo por éstas las conductas típicas, antijurídicas y culpables, en que se tienen a las computadoras como instrumento o fin para actividades con fines ilícitos, así tan solo filtre información privada y no ocasione una con-*

ducta dolosa o culposa». Como cualquier clase de delito, tiene sus características, pero éstas lo hacen único en el género:

1. Sólo una determinada persona o grupo de personas con conocimientos técnicos por encima de lo normal pueden llegar a cometerlos.
2. Son conductas criminales del tipo «cuello blanco», porque es de acuerdo al sujeto que los comete, es decir, este tipo de sujeto tiene un status socioeconómico y la comisión del delito no puede explicarse por pobreza, baja educación, poca inteligencia, ni por inestabilidad emocional.
3. Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado, se encuentran trabajando.
4. Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante. Provocan pérdidas económicas.
5. Ofrecen posibilidades de tiempo y espacio.
6. Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
7. Presentan grandes dificultades para su comprobación, por su carácter técnico».

Por su parte, Sarzana (1999:53) reduce estas conductas a *«cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material u objeto de la acción delictiva o como mero símbolo»* y Callegari (1985:115) señala que *«hay que puntualizar el delito informático como aquel que se da con la ayuda de la informática o de técnicas».*

En la presente investigación y siguiendo a Cárdenas (2008: 2-3) se entenderá como ciberdelito a *«aquellos delitos que para su comisión requieren necesariamente de una red de computadores (Internet). Esto abarca un ámbito delictivo bastante amplio, pues Internet se presta como medio para cometer delitos que importan emisión,*

transferencia o intercambio de información, atentados contra datos protegidos y otros».

2.2. EVOLUCIÓN DEL CIBERDELITO

Atendiendo a la definición de ciberdelito propuesta por Cárdenas (2008) y dados los antecedentes expuestos en el capítulo 2 de la presente investigación, el estudio de la evolución del ciberdelito se centra en el comienzo del siglo XX, tras la alarma generada en la población con el llamado **«Efecto 2.000»**.

2.2.1. La primera década del siglo XX

a) 2000–2003: el uso del correo electrónico y los gusanos informáticos

El «Efecto 2.000» marcó un antes y un después en el ciberdelito, asistiéndose a la aparición de toda una serie de ciberataques motivados principalmente por:

— El desafío que suponían para el ciberdelincuente los avances en las nuevas tecnologías.

— Un afán de notoriedad creciente.

En estos años se populariza el envío de *softwares* maliciosos a través de mensajes de correo electrónico no deseado. Normalmente, estos emails se acompañan de un vínculo o archivo adjunto.

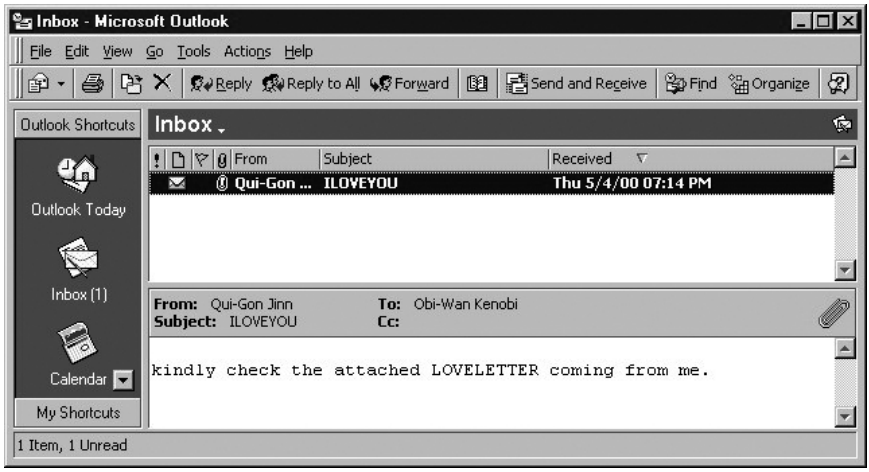
Tal es el caso del **gusano**[1] **«*I love you*»,** mensaje de correo electrónico no deseado con «*I love you*» en el asunto y un archivo adjunto

1 Los gusanos informáticos son un tipo de software pernicioso, semejantes a los virus informáticos. Estos gusanos, son programas informáticos que se ejecutan de forma automática y que empiezan varios procesos de intercambios de datos con la finalidad de dañar la red.

que pretendía ser una «carta de amor», que provocó el colapso en los equipos informáticos de decenas de millones de usuarios de Windows.

Algunas de las víctimas del virus del amor fueron: el Pentágono, el Parlamento Británico, la Reserva Federal, Ford, AT&T, Iberia, el Grupo Prisa, Vodafone, Dell o Telecinco. Los daños causados se estiman entre 4,9 y 7,7 millones de euros (véase Imagen 2.1.).

IMAGEN 2.1. El gusano «*I Love You*»



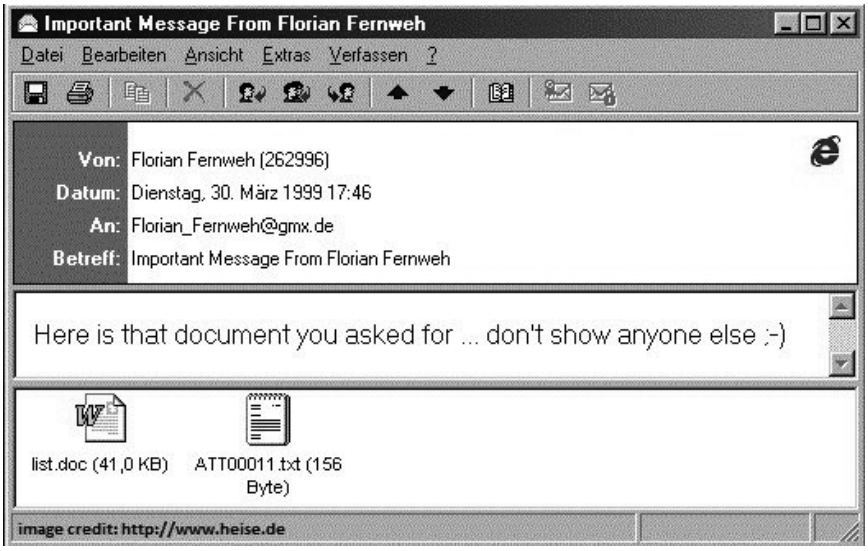
FUENTE: https://www.elandroidelibre.com

El predecesor del gusano «*I Love you*» fue «*Melissa*», un macro virus[2] que utilizaba técnicas de ingeniería social y que a través del mensaje «Aquí está el documento que me pediste, no se lo enseñes a nadie», en apenas unos días, protagonizó uno de los casos de infección masiva más importantes de la historia, causando daños de más de 80 millones de dólares a empresas norteamericanas y

2 Un virus de macro es un virus informático que altera o reemplaza una macro, que es un conjunto de comandos utilizados por los programas para realizar acciones habituales. Por ejemplo, la acción "abrir documento" en muchos programas de procesamiento de textos se basa en una macro para funcionar, debido a que existen distintos pasos en el proceso. Los virus de macro cambian este conjunto de comandos, lo cual les permite ejecutarse cada vez que se ejecuta la macro (Kaspersky, 2016).

compañías tales como Microsoft, Intel o Lucent Technologies, que tuvieron que bloquear sus conexiones a Internet (véase Imagen 2.2.).

IMAGEN 2.2. Macro Virus «*Melissa*»



FUENTE: http://www.pandasecurity.com

Estos ataques proporcionaron a los ciberdelincuentes la atención que buscaban, a la vez que los puntos de acceso WiFi comenzaban a ganar impulso suponiendo una nueva oportunidad para la ciberdelincuencia al facilitar el robo de información de los usuarios en redes inalámbricas no protegidas.

b) 2004–2005: los ordenadores zombies

En estos años la aparición del ***adware***[3] **o *software* compatible con la publicidad**, que muestran los *pop ups* de forma automática o anuncios de descarga en el equipo del usuario para hacer que éste

3 El *adware* es un *software* gratuito patrocinado mediante publicidad que aparece en ventanas emergentes o en una barra de herramientas en el equipo informático o navegador. El *adware*, en líneas generales es seguro, si bien puede ser utilizado para recopilar información personal y realizar un seguimiento de los sitios web visitados.

compre productos o servicios, es determinante en la evolución del ciberdelito.

Los proveedores de programas publicitarios vieron cómo aumentaban sus ingresos y los ciberdelincuentes aprovecharon la oportunidad para instalar diferentes paquetes de *adware* en millones de sistemas a cambio de cuantiosas cantidades económicas (véase Imagen 2.3.)

IMAGEN 2.3. Ordenador infectado por *adware* malicioso

FUENTE: http://www.tecnologiadetuatu.elcorteingles.es

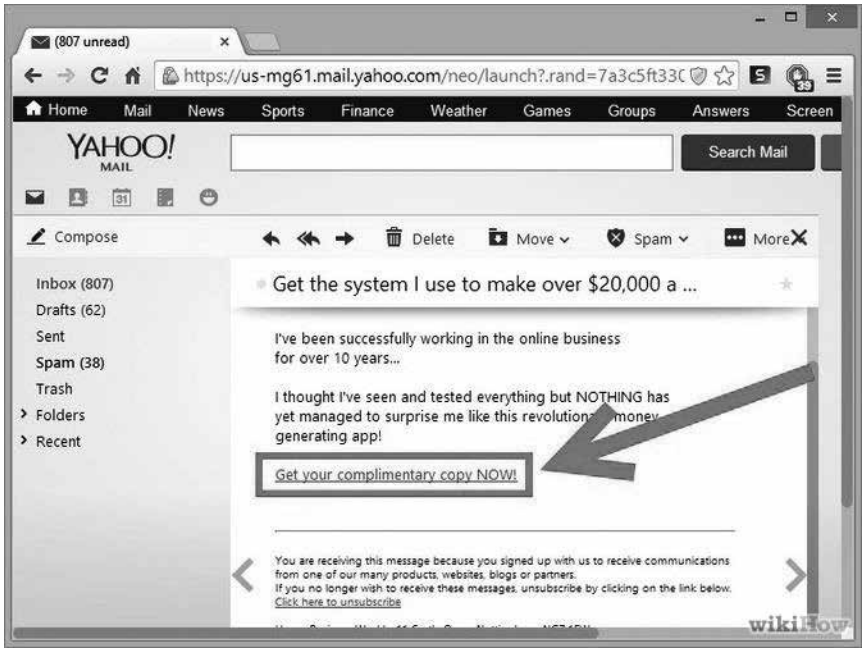
Los ***rootkits*** también jugaron un papel importante en esta época. Definido como un *software* espía, llegaba a los ordenados de las víctimas aprovechando cualquier deficiencia, modificando el funcionamiento del sistema operativo y eventualmente su núcleo.

Los *rootkits* son invisibles, lo que los hace difíciles de desinfectar, sin embargo, y a diferencia de los gusanos y virus, no tienen capacidad para duplicarse.

Por otro lado, se asiste al nacimiento de los **ordenadores zombies**. Los ciberdelincuentes podían infectar miles de máquinas al mismo tiempo, controlándolas de forma remota y sin el conocimiento de los usuarios, de tal manera que un ejército de ordenadores zombies siguiera ciegamente sus órdenes.

En cualquier caso, el objetivo principal de la delincuencia en este momento era ganar dinero, bien amenazando a las empresas con que atacarían sus ordenadores y sitios *web* a través del chantaje, o bien por las ventas generadas gracias al *spam*[4], (véase Imagen 2.4.).

IMAGEN 2.4. *Spam*



FUENTE: http://lopezdoriga.com

4 Mensajes no solicitados, no deseados o de remitente desconocido que pueden contener malware o software malicioso.

c) 2006–2008: las bandas organizadas

El dinero favoreció la organización de los ciberdelincuentes en bandas. Algunos poseían incluso una estructura similar a la de la mafia. Para proteger sus crecientes imperios comerciales, los ciberdelincuentes se hicieron más discretos a la hora de utilizar sus métodos, a la vez que mostraban todas sus habilidades tecnológicas.

En este contexto, muchos de los ciberdelincuentes simplemente se unieron a organizaciones que ya operaban fuera del medio digital, de tal manera que mientras éstas últimas aportaban su experiencia, los ciberdelincuentes aportaban sus conocimientos de expertos.

En este sentido, los primeros escenarios de la delincuencia organizada se focalizan en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios.

Finalmente, las bandas organizadas pierden su razón de ser. El crimen organizado y el ciberdelincuente comienzan un proceso paulatino donde se desvinculan a nivel operativo, de tal forma que la colaboración entre ambos se centra en la compra de los servicios de los primeros a los segundos.

El ciberdelincuente, de esta forma, se desvincula del hecho delictivo concreto y sólo ofrece el instrumento.

El más claro ejemplo de esto es la venta de «**kits de phishing**» en la que un usuario cualquiera, sin conocimientos avanzados de informática puede adquirir en el mercado del malware, un kit que sólo ha de configurar y poner en funcionamiento, para empezar a infectar equipos y obtener información de sus usuarios. Incluso en los acuerdos de servicio por el kit, informan que el desarrollador no se hace responsable del mal uso del programa.

d) 2009–2010: redes sociales y la importancia de los datos

A finales de la primera década del siglo XX las redes sociales consolidan su papel como agentes de socialización. Los ciberdelincuentes encuentran en estos medios de comunicación social una fuente de datos para cometer actos delictivos de toda índole.

2.2.2. El ciberdelito en la actualidad: ingeniería social y «Deep Web» o Internet Profunda

a) Estado de la cuestión: cifras y datos

Habiendo realizado un repaso de la evolución de los ciberdelitos, el verdadero motivo de su estudio no podría justificarse de otro modo sino es a través del análisis de cifras reales.

El ciberdelito ha experimentado un crecimiento exponencial en los últimos años, y así queda de manifiesto en el mapa mundial a tiempo real de la empresa rusa Kaspersky[5], donde se puede observar que diariamente la cifra de ciberataques asciende a más de 300.000 ataques diarios.

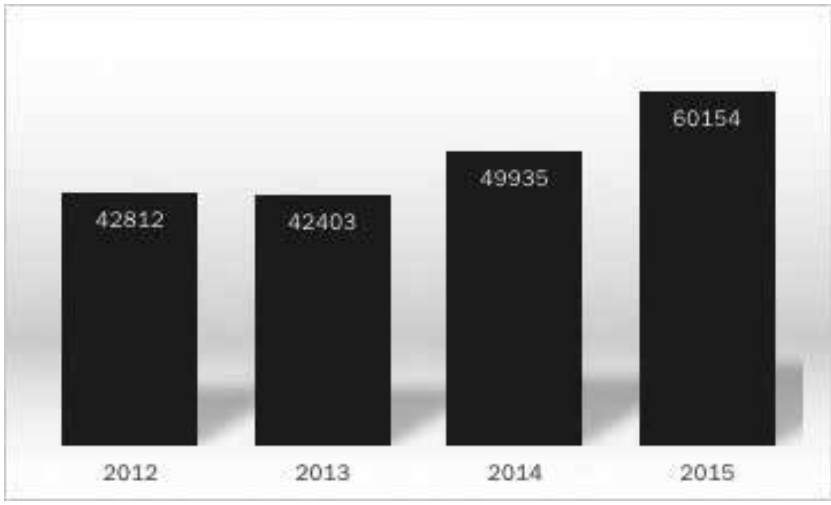
Según Brett Kelsey, vicepresidente y director de tecnología de Intel Security en Latinoamérica, el ciberdelito significa un 0,8% del PIB mundial, o lo que es lo mismo, 6,100 millones de dólares, cifra que va en aumento año tras año.

Concretamente en el caso español, y según un informe del Ministerio del Interior (2015), la evolución del ciberdelito en España ha supuesto en cifras reales un incremento de 17.342 ciberdelitos desde el año

5 http://cybermap.kaspersky.com

2012 hasta el año 2015, tal y como puede observarse en el Gráfico 2.5. que se muestra a continuación.

GRÁFICO 2.5. Evolución del número de ciberdelitos en España (2012 – 2015)



Adaptado de Ministerio del Interior (2015)

En cuanto a la evolución de la ciberdelincuencia, teniendo en cuenta las categorías delictivas, el Ministerio del Interior identifica siete categorías diferenciadas, siendo el fraude informático el que cobra mayor relevancia en los últimos años. En segunda posición, se encuentran las amenazas y coacciones, seguidas del acceso e interpretación ilícita, la falsificación informática, los ataques contra el honor, la interferencia en los datos y los delitos contra la propiedad intelectual, tal y como queda reflejado en el Gráfico 2.6.

GRÁFICO 2.6. Evolución de la ciberdelincuencia por categorías delictivas en España (2012 -2015)

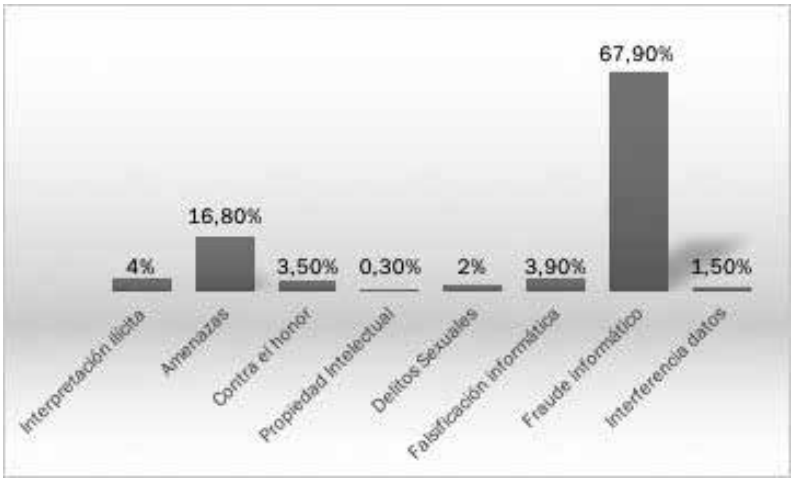
	Acceso ilícito	Amenazas	Ataques contra el honor	Propiedad intelectual	Delitos sexuales	Falsificación informática	Fraude informático	Interfer. de datos
2012	1701	9207	1891	144	715	1625	27231	298
2013	1805	9064	1963	172	768	1608	26664	359
2014	1851	9559	2212	183	974	1874	32842	440
2015	2386	10112	2131	167	1233	2361	40864	900

2012 2013 2014 2015

Adaptada de Ministerio del Interior (2015)

En porcentajes, tal y como se muestra en el Gráfico 2.7., el fraude informático constituye el 67,90% de los ciberdelitos cometidos en España, mientras que las amenazas y coacciones suponen un 16,80% y el acceso e interpretación ilícita un 4%.

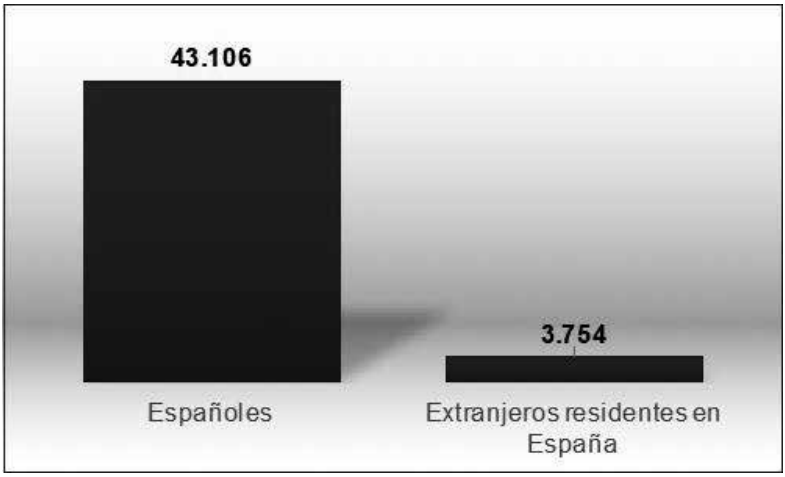
GRÁFICO 2.7. El ciberdelito en España (Porcentajes)



Adaptado de Ministerio del Interior (2015)

Por otro lado y atendiendo al perfil de las cibervícitimas en territorio español, los españoles son más atacados que el resto de nacionalidades, un 92% de las víctimas son españolas frente a un 8% de extranjeros residentes en España (véase Gráfico 2.8.).

GRÁFICO 2.8. Número de cibervíctimas según nacionalidad en territorio español



Adaptado de Ministerio del Interior (2015)

b) Ingeniería social: redes sociales

La ingeniería social podría definirse como un elemento no técnico de bajo coste, utilizado por los ciberdelincuentes, que manipula a los individuos utilizando la conducción psicológica, para inferir en los sistemas de seguridad, influyendo en sus actitudes, acciones y relaciones.

El objetivo del ciberdelincuente es obtener información, realizar fraudes u obtener acceso ilegítimo de los usuarios bien sea por vía telefónica, por contacto directo o por correo, tanto electrónico como tradicional.

La ingeniería social se utiliza cada vez con más frecuencia en el ataque a las medianas y pequeñas empresas así como a las grandes corporaciones.

Normalmente la ingeniería social se aprovecha de la inexperiencia del usuario, conociendo bien a su víctima, haciéndose pasar por alguien de su entorno o agente superior, utilizando la persuasión.

En general, los métodos de la ingeniería social están organizados de la siguiente manera:

1. **Acercamiento:** el ciberdelincuente trata de ganarse la confianza del usuario adoptando un rol cercano al usuario: una empresa cliente, un posible proveedor de servicios, etc.
2. **Alerta:** el ciberdelincuente utiliza un pretexto de seguridad o situación de emergencia para que el usuario colabore.
3. **Distracción:** el ciberdelincuente comunica al usuario que su colaboración ha sido de ayuda y que todo ha vuelto a la normalidad, evitando que este pueda avisar a alguien de su empresa o entorno.

Los medios más utilizados se describen a continuación:

1. Teléfono (*vishing*): llamadas telefónicas de personas que se hacen pasar por una organización con una buena imagen de marca y alta notoriedad.
2. Correo electrónico (*phishing*).
3. Correo tradicional.
4. USB (*baiting*): el atacante carga unidades de USB con *malware* y espera que el usuario las conecte a su dispositivo.
5. Mensajería instantánea.
6. Páginas web.
7. Redes sociales.

El problema en este tipo de ataques es que no hay un signo inmediato que advierta de un ataque, y por ello se recomienda seguir las siguientes indicaciones:

1. Antes de ofrecer información tanto personal como empresarial, averiguar la identidad de la persona que solicita la información.
2. En caso de que se acceda a facilitar la información solicitada, verificar qué información se está dando.

3. Y con respecto a lo anterior, preguntarse la importancia de la información que se está pidiendo.

De forma más específica y con respecto a las redes sociales, su virtualización ha permitido la comunicación global y dinámica dando un carácter tangible a muchos de los aspectos intangibles de las redes sociales del mundo real, al apoyarse en complejos sistemas de información y en el uso de dispositivos (*Coz et. al.,* 2012).

Una red social virtual es una serie de servicios prestados a través de Internet que permite a los usuarios generar un perfil: el hacer públicos datos e información personal y proporcionar herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles (Coz et. al., 2012).

La ingeniería social aplicada a las redes sociales es una de las técnicas más sencillas y efectivas para aproximarse a la víctima, ya que, en líneas generales, los usuarios suelen aceptar invitaciones de otros sin contrastar o verificar el perfil. A esto se le une el hecho de la facilidad con la que se obtiene información a través de estos medios puesto que, hoy por hoy, muy pocos usuarios limitan la privacidad de sus perfiles, accediendo, además, desde cualquier ubicación.

Según afirma Emanuel Abraham, hacker ético de «Security Solution & Education», «*la persona que efectúa este método, trata de engañar a la víctima, buscando entrar en confianza o haciéndose pasar por alguien más para obtener lo que necesita. Teniendo en cuenta que somos muy vulnerables y nos movemos a través de una serie de impulsos irracionales, el que ejecute esta técnica usará comúnmente el teléfono, internet, el disfraz u otros métodos para engañar fingiendo ser alguien más. En muchos de los casos la persona suplanta a un trabajador de la empresa o a alguien de servicio técnico*».

c) Deep Web o Internet Profunda

La *Deep Web* es la parte de la red que no está indexada en los motores de búsqueda o directorios, dando forma a lo que se ha llamado la Internet Profunda. Hoy en día se estima que cerca de un 85% de todo el contenido que hay en Internet se encuentra en la *Deep Web.*

Con respecto a la clasificación de los contenidos presentes en esta parte «invisible» de Internet, cabe mencionar la dificultad de dicha tarea, debido, entre otras cosas, a la enorme heterogeneidad de los mismos. Aguillo (2001) propone una clasificación basada en criterios documentales y reconoce los siguientes grupos:

— **Bases de datos bibliográficas:** incluidos los catálogos de bibliotecas, las bases de datos de referencias bibliográficas, gratuitas o de pago, etc.

— **Bases de datos alfanuméricas y a texto completo:** también se incluyen en esta categoría las obras de referencia, tipo enciclopedia o diccionarios.

— **Revistas electrónicas y archivos de documentos:** tanto las de acceso gratuito, que normalmente exigen registro previo, como las de pago (acceso a través de IP o palabra clave), son invisibles a los motores de búsqueda.

— **Documentos en formatos no indexables,** esto es, ficheros no HTML o textuales desarrollados con formatos más elaborados (pdf; ppt; doc; etc.).

Actualmente se estima que existen aproximadamente 550 billones de documentos en la *Deep web* frente a 1 billón de documentos en la red superficial, siendo las redes virtuales privadas (*virtual private networks* o VPN) tecnologías que corresponden a esta clasificación de red invisible y sus principales representantes. Estas redes corresponden a infraestructura y contenidos a los que se puede acceder únicamente a través de un *software* específico, siendo uno de los ejemplos más representativos TOR.

Según la propia página web de TOR, «*la red TOR es un grupo de servidores operados por voluntarios que permite a la gente mejorar su privacidad y la seguridad en Internet. Usuarios de TOR emplean esta red mediante la conexión a través de una serie de túneles virtuales, en lugar de hacer una conexión directa, lo que permite a ambas organizaciones e individuos compartir información a través de redes públicas sin comprometer su privacidad. En la misma línea, TOR es una efectiva herramienta de elusión de la censura, permitiendo a sus usuarios llegar a destinos o contenidos que de otra manera estarían bloqueados*».

Concretamente, TOR es un proyecto diseñado e implementado por la Marina de los Estados Unidos. Puede definirse como una red de túneles virtuales que permite a los usuarios navegar con privacidad en Internet, y a los desarrolladores crear aplicaciones para el intercambio de información sobre redes públicas sin tener que comprometer su identidad. Igualmente, ayuda a reducir o evitar el seguimiento que hacen los sitios web de los hábitos de navegación de las personas y a publicar sitios web y otros servicios sin la necesidad de revelar su localización.

Si bien, el objetivo de TOR es proteger a los usuarios de la vigilancia en Internet (por ejemplo, del análisis de tráfico). También se ha utilizado para mantener ocultos diferentes servicios de dudosa legalidad.

Así, en la Internet Profunda se pueden encontrar contenidos ilegales de entidades anónimas que buscan realizar diferentes transacciones bajo privacidad. La venta de bienes y servicios de origen ilícito se puede clasificar en 6 grandes grupos definidos a continuación (Iter Criminis, 2016):

1. **Tráfico de drogas:** supone un 62% de los bienes que se trafican en la Deep web. Dentro de esta categoría se pueden encontrar los productos químicos para su fabricación, productos derivados, así como el conjunto de actos que conlleva el consumo de droga.

2. **Tráfico de información (16%):** engloba desde la venta de listados de direcciones de páginas web «.onion», a información robada de compañías.

   También se pueden encontrar cuentas sustraídas a usuarios legítimos de servicios en Internet que son vendidas en subasta al que más puje por obtenerlas, siendo sus precios menores a los oficiales.

3. **Venta de aplicaciones maliciosas (15%):** se pueden encontrar principalmente las siguientes aplicaciones o programas maliciosos:

   — ***Keyloggers***: son programas informáticos que ayudan al ciberdelincuente a rastrear las pulsaciones que son realizadas por el trabajador de una empresa en su teclado, cuya finalidad es el conocer qué información mete el usuario en el ordenador, así como contraseñas.

   — ***Exploits:*** son programas que se usan para aprovechar la inseguridad de un sistema para conseguir fines, como puede ser el acceso no autorizado. Se venden desde exploits por 1 euro ya parcheados anteriormente por las empresas, hasta exploits 0 Day (exploits no registrados por la empresa y que aún no existe forma de neutralizarlos) de hasta cientos de miles de euros.

   — ***Botnet:*** es una red de ordenadores que son afectados para que mediante un ataque DDOS se quede sin funcionamiento un servidor o página web, mediante el colapso provocado por miles de peticiones de acceso a un ordenador. El contratar este tipo de ataque puede valer tan sólo 1€, aunque depende del tiempo de operación.

   — ***Ransomwares:*** es un tipo de troyano, el cual cifra los archivos de la víctima, y le muestra que si quiere recuperar

su información personal, tendrá que pagar una cantidad de dinero (dinero virtual o bitcoins[6]

4. **Venta de armas (2%):** en el ranking mundial de venta ilegal, la de armas ocupa el tercer lugar; por delante de la misma encontramos la venta de drogas y tráfico de personas. Sin embargo, en la Deep Web abarca el 2% del mercado ilegal.

   Algunas de estas armas provienen de países de Europa del este, cuyo rastro se perdió por la disgregación de la Unión Soviética o durante la Guerra de los Balcanes, y pertenecen al mercado negro.

5. **Asesinatos/agresiones por encargo (1%):** dentro de esta red existen personas que se ofrecen para realizar delitos anónimos por mandato de otros a cambio de una cantidad de dinero. Este tipo de delitos comprende palizas o incluso el matar directamente a alguien.

---

6 ¿Qué son las Bitcoins? Las bitcoins o también conocidas como "monedas virtuales" fueron concebidas en el año 2009 bajo el seudónimo de Satoshi Nakamoto. El principal objetivo de su creación es la realización de compras a través de internet; aunque el Banco de España amplía dicho objetivo, afirmando que: "Las bitcoins nacen con ambiciones elevadas: proporcionar a los ciudadanos un medio de pago que posibilite la ejecución de transferencias de valor rápidas, a bajo coste y que, además, no pueda ser controlado ni manipulado por gobiernos, bancos centrales o entidades financieras".

Se caracterizan por:

- Estar descentralizadas: Ninguna institución, entidad bancaria o Estado puede controlar su emisión. La minería de la propia red gestiona el flujo de bitcoins en función de la demanda existente de manera descentralizada. A diferencia de las monedas físicas de cada país, no es posible que se genere inflación al crear más bitcoins.
- Imposibilidad de su falsificación: Como ya hemos mencionado, son monedas criptográficas con un sistema que protege a los usuarios, haciendo más fáciles las transacciones entre partes, garantizando que los poseedores de este tipo de moneda puedan controlar las operaciones que realicen.
- No existir intermediarios: Las operaciones se hacen directamente entre dos partes: emisor – receptor. Tiene un funcionamiento P2P (Peer-to-peer), es decir, entre iguales, haciendo que las operaciones tengan un bajo coste en el procesamiento y dichas transacciones sean prácticamente inmediatas.
- Irreversibilidad de las transacciones: Una vez que se paga, la operación no puede ser anulada. Según la características anterior (no existen intermediarios), la devolución depende de un acuerdo entre ambas partes de manera directa.
- Poder realizar cambio de divisa: como cualquier otra moneda. Puedes transformar, por ejemplo bitcoins a euros.
- Mantener la privacidad del usuario.
- El dinero te pertenece al 100%: al no existir terceros, no puede interceder nadie ni tu cuenta puede ser bloqueada.

Además de los seis bloques citados anteriormente, dentro del mercado ilegal en la *Deep Web*, se encuentra ***WikiLeaks***, organización internacional de medios de comunicación y sin ánimo de lucro, la cual sube a su sitio web, bajo el anonimato de sus fuentes, informes y documentos filtrados con información sensible para el interés público, como pueden ser el espionaje, la corrupción o las guerras.

2.3. CLASIFICACIÓN DEL CIBERDELITO

Según Gordon *et. al. (*2006), los delitos reconocidos tienen una gran diversidad de infracciones, lo cual hace más difícil su clasificación o tipología. Uno de los sistemas de clasificación es el definido por el Convenio sobre la Ciberdelincuencia, en el que se distinguen cuatro tipos diferentes de infracciones:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
2. Delitos Informáticos.
3. Delitos relacionados con el contenido.
4. Delitos relacionados con el derecho de autor.

Esta clasificación no es del todo coherente porque no se fundamenta en un criterio único para distinguir las categorías. De estas categorías, tres hacen referencia al objeto de la protección jurídica: ‘’delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos relacionados con el contenido; y delitos relacionados con el derecho de autor’’. La cuarta categoría, delitos informáticos, no se identifica con el objetivo de la protección jurídica sino con el método. Esta incongruencia hace que haya un poco de coincidencia entre las categorías según explica Gercke, M. (2014).

Por su parte, otros autores como Quimbo (2004) clasifican los delitos informáticos en 3 tipos diferentes según la víctima:

1. Ciberdelitos contra las personas: trasmisión de pornografía infantil o ciberacoso.
2. Ciberdelitos contra la propiedad privada: acceso informático no autorizado, vandalismo informático, trasmisión de malware, posesión no autorizada de información digital, cracking, creación de virus o pirateo de software.
3. Ciberdelitos contra la autoridad: ataques a webs del gobierno.

En esta línea, se propone una segunda tipología de delitos informáticos que establece diferencias entre aquellos que atentan directamente contra la intimidad, el honor o la propiedad privada de las personas físicas y aquellos que atentan contra las empresas, teniendo en cuenta que en ambos casos los métodos y objetivos pueden ser similares.

2.3.1. Ciberdelito contra las personas físicas

Se entiende por ciberdelinciencia contra las personas aquella que delinque contra los principios básicos del individuo, teniendo un conjunto de características comunes, descritas a continuación:

1. Es una manera rápida de infringir mediante procedimientos fáciles de ejecutar a un coste reducido.
2. Puede aportar elevadas cantidades de dinero bajo el anonimato como consecuencia de que la investigación de fraude habitualmente es tardía, existiendo un bajo porcentaje de éxito en su detección. Además, por lo general, no se denuncia de manera frecuente y las sentencias son leves.

Algunos delitos contra las personas físicas son descritos a continuación:

1. Acoso a menores o *grooming*: un adulto se hace pasar por un menor, ganándose la confianza del otro, coaccionándole para conseguir mediante chats, redes sociales o mensajería instantánea: imágenes o contenidos sexuales.

2. *Carding*: consiste en adquirir algún producto o servicio mediante el uso de tarjetas de crédito pertenecientes a algún titular o producidos por algún programa informático. Por el contrario, está la venta de productos a través del comercio electrónico; el usuario realizará la compra y pago de un producto, pero este no recibirá nada, pues ha sido estafado.
3. *Phising*: se trata de adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información de tarjetas de crédito.
4. *Pharming*: es la explotación de una vulnerabilidad en el software de los servidores DNS o en el equipo de los usuarios.
5. Ataques XSS o estafas en la venta de productos: explotan la confianza del individuo que deposita en cierta página web.

2.3.2. Ciberdelito contra las empresas

La ciberdelincuencia contra las empresas se entiende como el conjunto de conductas relacionadas con el acceso, la apropiación o el intercambio de información en las redes, llevados a cabo sin el consentimiento o autorización requeridas, o haciendo un uso ilícito de la misma, que van en contra de una institución, organización o cualquier otra clase de sociedad o persona jurídica.

En 2015 la empresa hotelera Hyatt detectó un software malicioso en los ordenadores de la compañía. El malware analizaba y procesaba los datos de pago de los clientes con el objetivo de sustraer el dinero de las cuentas bancarias de los mismos. Se comunicó que el problema se solucionó, aun así, se advirtió a los clientes de que revisaran sus cuentas para comprobar cualquier actividad inusual (Hosteltur, 2016).

En su mayoría, los ciberdelincuentes que atentan contra la empresa se aprovechan de la escasa formación del factor humano y de los mecanismos insuficientes de autenticación de muchas organizaciones, que van desde la gestión de salarios hasta la gestión de clientes; eligiendo de manera efectiva sus objetivos dentro de las organizaciones.

La motivación económica es uno de los principales móviles por lo que uno de los objetivos más valorados es el robo de documentación e información susceptible de ser comercializada.

No obstante, no se trata de ataques casuales que van dirigidos a todos los miembros de la organización, sino que es un proceso complejo. El proceso puede durar varios meses. El ciberdelincuente analiza el sistema que la corporación utiliza y decide el perfil del empleado a través del cual va a tener acceso a los datos, el puesto que ocupa dentro de la organización, la forma de comunicación, para posteriormente preparar su estrategia.

2.3.2.1. El ciberdelito en las PYMES

Las PYMES desempeñan un papel fundamental en las economías nacionales. Cuando se les confía datos de sus clientes, las PYMES también tienen la responsabilidad de proteger esta información contra atacantes online. Sin embargo, como se detalla en el estudio comparativo sobre capacidades de seguridad de Cisco (2015), las PYMES muestran signos de que sus defensas contra atacantes son más débiles de lo que les exigen sus retos.

A su vez, estos puntos débiles pueden poner en riesgo a los clientes empresariales de las PYMES. Los atacantes que pueden vulnerar la red de una PYME, también podrían encontrar una puerta de entrada en una red empresarial.

Según los resultados del estudio comparativo sobre capacidades de seguridad de Cisco (2014), las PYMES utilizan menos procesos para

analizar riesgos y menos herramientas de defensa contra amenazas de las que utilizaban el año anterior.

Por ejemplo, el 48% de las PYMES afirmaron en 2015 que usaban seguridad web; el 59% afirmó que lo hacía en 2014. Sólo el 29% ha dicho que usaban parches y configuración en 2015, en comparación con el 39% en 2014.

Además, de los encuestados de PYMES que no tienen un responsable ejecutivo de seguridad, aproximadamente una cuarta parte no cree que sus empresas sean objetivos de gran valor para los ciberdelincuentes. Esta opinión indica un exceso de confianza en la capacidad de su empresa para evitar los sofisticados ataques online actuales o bien que los ataques nunca ocurrirán en su empresa.

2.4. CONCLUSIONES

El ciberdelito se ha convertido en una de las principales amenazas para el entramado empresarial español. En este sentido, puede afirmarse que no sólo crece el número de actos delictivos, sino que los delincuentes van perfeccionando sus ataques, adelantándose, en muchas ocasiones, a los propios desarrollos tecnológicos de prevención, lo que supone la existencia de una serie de brechas en materia de seguridad informática complicadas de parchear.

Actualmente, además, la empresa se enfrenta a un total desconocimiento de lo que puede suponer un ataque de este tipo para su organización, ya que, por un lado, apenas existe información fiable al respecto, siendo las principales fuentes aquellas compañías cuya actividad se orienta a la comercialización de productos y servicios que combaten este tipo de acciones y, por otro, la percepción de que un ciberataque nunca se dirigirá hacia su estructura.

Otro de los problemas que se ha detectado es la empatía que despiertan en la sociedad los ataques en el ciberespacio, considerando al delincuente como un héroe cuando es capaz de invadir espacios

privados, robando información y poniendo a prueba a las autoridades, como es el caso de la admiración que llegan a despertar todos aquellos que han conseguido acceder a los archivos clasificados de la CIA o del FBI.

Estos hechos, unidos a la digitalización de los procesos de la empresa a través del Internet de las Cosas o la Ingeniería Social, justifican y hacen necesarios la redacción y puesta en práctica de toda una serie de protocolos de actuación encaminados a proteger, entre otros, la propiedad intelectual, posibles ataques al honor o el robo de datos e información, lo que se ha venido a llamar BIG DATA.

2.5. BIBLIOGRAFÍA

Aguilar, M. (2015): Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. Revista Criminalidad, 57 (1): 121-135.

Aguillo, I. (2001): Internet invisible o infranet: definición, clasificación y evaluación. En: Maldonado Martínez A, coordinadora. La información especializada en Internet: directorio de recursos de interés académico y profesional. Madrid: Consejo Superior de Investigaciones Científicas, Centro de Información y Documentación Científica; p. 161-177.

Callegaril, N. (1985). «Delitos informáticos y legislación». En: Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana, No. 70, Medellín.

Cárdenas, C. (2008): «El lugar de comisión de los denominados ciberdelitos». Polít. crim., N° 6, A2-6, pp. 1-14.

CCM (2017):
http://es.ccm.net/contents/25-ingenieria-social)
(Consultado el 21 de febrero de 2017)

Cisco (2014): Informe anual de seguridad. Publicado en https://hackingetico.com//wp-content/uploads/2014/03/cisco2014_infosec_report.pdf (Consultado el 25 de marzo de 2017)

Cisco (2015): Informe anual de seguridad.
Publicado en: http://www.cisco.com/c/dam/global/es_es/assets/pdf/asr_final_os_ah_es.pdf (Consultado el 25 de marzo de 2017)

Coz F., Fojón E., Heradio, R. y, Cerrada, J. (2012): Evaluación de la privacidad de una red social virtual. RISTI, Edición Nº 9.

Hosteltur (2016):
https://www.hosteltur.com/115313_ataques-internet-hoteles-van-apuntan-mejor.html (Consultado el 22 de febrero de 2017)

ITER CRIMINIS (2016):
http://itercriminis.com/analisis-sobre-los-negocios-ilegales-en-la-deep-web/
(Consultado el día 17 de febrero de 2017)

Quimbo (2004): Clasificación de los ciberdelitos según la víctima. Publicado en
http://e-legales.net/category/articulos/
(Consultado el 15 de febrero de 2017)

Ministerio del Interior (2015):
http://www.interior.gob.es/documents/10180/3066430/Informe+Cibercriminalidad+2015.pdf/c10f398a-8552-430c-9b7f-81d9cc8e751b

Rayón Ballesteros, M. C., y Gómez Hernández, J. A. (2014): Cibercrimen: particularidades en su investigación y enjuiciamiento/ Cybercrime: particularities in investigation and prosecution. Anuario Jurídico y Económico Escurialense (47), pp.209-234.

Sarzana, C. (1979): Criminalitá e tecnología en computers crime». En: Rassegna penitenziaria e criminologica, Nos 1-2. , Roma: Ministero della Giustizia.

Sieber, U. (2008): Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law. In: Delmas-Marty, M. / Pieth, M. / Sieber, U. (ed(s).): Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008, 127 – 202

Tellez, J. (1997): Derecho informático. México: McGraw-Hill Book Company.

TOR (2017):
https://www.torproject.org/about/overview.html.en
(Consultado el 17 de febrero de 2017)

We Live Security (2016):
http://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/
(Consultado el 21 de febrero de 2017)

3 LOS CIBERDELITOS CONTRA LA EMPRESA: HERRAMIENTAS Y TÉCNICAS DEL CIBERATAQUE

RESUMEN

El ciberdelito contra la empresa puede adoptar diversas formas, dependiendo no sólo del objetivo del mismo sino también del perfil del ciberdelincuente o de la seguridad del sistema informático de la organización.

En la actualidad no existe una clasificación universal de los ciberdelitos lo que supone un impedimento para su estudio. Por ello en este capítulo se propone una clasificación propia de los ciberataques contra la empresa atendiendo a tanto a su naturaleza y objetivos como a las herramientas utilizadas para su comisión.

PALABRAS CLAVE: tipos de ciberdelito, motivación del ciberdelito, amenazas contra la seguridad informática de la empresa, malware, denegación de servicios, internet de las cosas, ingeniería social, Zero Day.

ABSTRACT

Cybercrime against a company can adopt various forms, depending not only on its objective but also on the profile of the cybercriminal or the computer system security of the company.

At the momento there is no universal classification system for the cybercriminals which impedes their study. Therefore, in this chapter, there is proposed a classification of the cyber attacks against the company, taking into account both its nature and objectives but also, the tools used for the attack.

KEYWORDS: Types of cybercrime, motivation of cybercrime, threats against the IT-security of the company, malware, denial of service, internet of things, social engineering, Zero day.

3.1 HERRAMIENTAS Y TÉCNICAS DEL CIBERATAQUE EMPRESARIAL

A continuación y teniendo en cuenta la actividad delictiva en el ciberespacio se definen y caracterizan las herramientas utilizadas con más frecuencia en el ciberataque empresarial. Igualmente, estas herramientas están recogidas en la Tabla 1 adjuntada en la memoria de la investigación.

1. Troyano

Descripción. Tipo de virus que aparenta ser un software de ayuda o divertido para pasar inadvertido pero que en realidad está provocando daños o el robo de datos.

Síntomas. Aquellos terminales que se encuentren infectados por troyanos mostrarán algunas señales como que aparezcan o desparezcan archivos, que se ejecuten o se cierren programas sin razón aparente o que algunos periféricos dejen de funcionar. Estos son algunos de los muchos síntomas de un sistema infectado.

Riesgos. Su propósito principal es dar acceso remoto al ciberdelincuente a un sistema para que pueda usar otro tipo de software como un keylogger para registrar las teclas pulsadas y obtener información.

Métodos de prevención. Además de tener todos los software de tu ordenador actualizado, existen otras formas de protegerse de este tipo de ataques como no conectarse a una red Wifi abierta o diferenciar las cuentas de usuario de las cuentas de administrado, en caso de que se infecte la cuenta de usuario, el atacante no tendrá permisos de administrador y no tendrá un acceso completo.

2. Troyano bancario

Descripción. Una variedad del troyano que está orientado al robo de datos bancarios.

Síntomas. En general, al igual que el troyano clásico, la existencia de un troyano bancario en un sistema suele reducir la velocidad de este hasta el punto de que puede provocar errores entre los periféricos o algún software.

Riesgos. Tienen como principal objetivo robar datos privados de las cuentas bancarias de los usuarios. Utilizan diferentes técnicas para obtener los datos de acceso a todo tipo de entidades financieras.

Métodos de prevención. Este tipo de ataques se aprovechan de la ingenuidad de las personas, es por ello que sería primordial la concienciación de los trabajadores y evitar descargarse archivos de páginas web poco fiables.

3. Rootkit

Descripción. Están diseñados para proporcionar a los hackers un acceso administrativo a la computadora sin el conocimiento del usuario.

Síntomas. La evidencia de un sistema infectado por un rootkit es más compleja de detectar, es por ello que debería ser un programa antivirus el que detectara archivos ocultos, inicios de sesión ocultas al usuario o datos que se están enviando fuera de la terminal.

Riesgos. Da el control total de la terminal al ciberdelincuente desde el momento en el que se enciende el ordenador y dificulta la detección de otros archivos dañinos que haya en el sistema.

Métodos de prevención. Es necesario un programa que no solo analice los archivos del ordenador, sino que también debe controlarse lo que se hace al ejecutar cada programa.

4. Keylogger

Descripción. Un tipo de software usado para registrar todo lo que se escribe en el teclado, de esta forma los ladrones pueden leer cualquier información que se escriba, como contraseñas, tarjetas de crédito, correos electrónicos, etc.

Síntomas. Suelen presentar los comportamientos que comparten la mayoría de los virus informáticos, estos son: un uso excesivo del disco duro o de la red, un enlentecimiento del sistema o algún tipo de retraso en el comportamiento y uso del ordenador.

Riesgos. Quien controla este software puede ver que teclas está pulsando su víctima, de manera que junto a otro tipo de malware puede obtener contraseñas o incluso lograr tener acceso a los datos bancarios del infectado.

Métodos de prevención. Se debe utilizar un antivirus actualizado, evitar acceder a redes Wifi abiertas y no manipular información personal en ordenadores públicos.

5. Gusanos

Descripción. Se divide de manera similar a las células del cuerpo humano y se propaga a través de las redes de los terminales. Este tipo de malware es capaz de reproducirse a través de algún medio de comunicación como, por ejemplo, el correo electrónico. Todo esto con la finalidad de infectar el mayor número de terminales posibles.

Síntomas. Para poder infectar una terminal con un gusano, primero ha de penetrar el sistema. Para ello se suelen enviar archivos por correo y, cuando se tratan de gusanos informáticos suelen tener una doble extensión pero para poder observar esto, el ordenador debería tener desactivada la función de «ocultar las extensiones del archivo para tipos de archivos conocidos». Una vez infectado, un claro

síntoma sería que la disquetera se abra y se cierre continuamente y sin razón aparente.

Riesgos. Se podría decir que el mayor riesgo de un gusano informático es su velocidad de propagación. Infecta un gran número de terminales y, combinado con otras herramientas, puede recabar información o llevar a cabo actividades perjudiciales para la empresa.

Métodos de prevención. Para evitar ser infectado por un gusano es recomendable mantener actualizado el sistema operativo en todo momento al igual que otros softwares que se tengan instalados. También se debe realizar una navegación segura y prudente, tratando de evitar páginas con dudosa reputación y evitar ejecutar archivos sospechosos, esto incluye los archivos adjuntos que recibamos por email.

6. Botnets

Descripción. Es el nombre con el que se denomina a un grupo de PC que estén infectados y sean controlados por un atacante de forma remota. Los ordenadores que forman la botnet son los llamados bots o zombies.

Síntomas. El ordenador vaya más lento de lo normal o que algunas aplicaciones dejen de funcionar son unos de los principales indicadores de que nuestro ordenador puede haber sido infectado y estar siendo usado como lo que se conoce como un ordenador «zombie».

Riesgos. Alguien puede estar usando la terminal de forma remota y puede conseguir datos personales que se guarden en el ordenador, puede ser utilizado para reenviar spam o infectar a otros terminales o incluso puede cometer otro tipo de delitos desde tu ordenador suplantando tu identidad.

Métodos de prevención. Mantener actualizado el sistema operativo y un antivirus y tener unos buenos hábitos de uso son unas de las maneras de evitar ser infectado y convertir tu ordenador en parte de

una botnet. También se debe evitar instalar nada que no se haya elegido, pulsar enlaces de emails cuyo remitente desconoces o desconfiar de los chollos que te anuncian por Internet.

7. Backdoor

Descripción. Son accesos, desconocidos por el usuario, dejados por el ciberdelincuente para poder acceder al sistema de su víctima en cualquier momento.

Síntomas. No tienen unos síntomas claros, puesto que existen backdoors que han sido instalados a propósito para poder llevar a cabo tareas de mantenimiento o administración de forma remota.

Riesgos. Da un acceso, que normalmente pasa inadvertido, al sistema que el ciberdelicuente puede usar para obtener información sensible de la empresa o llevar a cabo otras acciones perjudiciales entre otras muchas otras actividades que podría llevar a cabo.

Métodos de prevención. Es muy importante eliminar un backdoor por completo para eliminar cualquier posibilidad de fallar al intentar removerlo del sistema. Es recomendable disponer de un programa que realice esta limpieza de forma automática puesto que es muy difícil e improbable lograr eliminar un backdoor por completo de forma manual.

8. Adware

Descripción. Es un tipo de software gratuito patrocinado mediante publicidad que suele aparecer en ventanas emergentes, o pop-ups. La mayoría de veces el adware es molesto pero seguro, aunque a veces se suele usar para recopilar información personal sin autorización.

Síntomas. Señales de que estamos infectados por un adware serían que nos saltan pop-ups de publicidad continuamente, que nos

instalen barras de herramientas o añadan páginas como favoritos en nuestros navegadores.

Riesgos. Aunque no suele representar una gran amenaza, el adware pone la información personal de los usuarios a disposición de quien distribuya o publique el software, además de resultar muy molesto para la persona afectada.

Métodos de prevención. Se pueden eliminar manualmente pero dependiendo del adware, puede resultar demasiado complejo. Por ello, existen programas que automatizan la eliminación de este tipo de software.

9. Sniffing

Descripción. En términos generales, el sniffing consiste en la detección o retención de toda la información que circula por una red. Una vez que se obtiene la información, se almacena y se interpreta para poder conseguir datos sensibles como contraseñas, información bancaria o cualquier otra información que pueda ser usada en beneficio del ciberdelincuente. Este método es uno de los principales que se realizan cuando se intenta robar información.

Síntomas. El sniffer entra al pc a través de su instalación y para ello el usuario debe aceptar la instalación. En el caso de que se solicitara la instalación de un archivo sospechoso y se aceptara, existen programas que detectan el sniffer en el sistema o a través de la red.

Riesgos. El atacante obtiene acceso a la información almacenada en el sistema atacado, dejando información personal en manos del ciberdelincuente y podrá usarla de la forma que le plazca.

Métodos de prevención. Es recomendable no hacer uso de una red wifi pública puesto que tal vez se trate de una red fraudulenta que esté esperando a que un usuario se conecte para poder capturar la información. También se debe evitar enviar información sensible a través de la red para no dar la oportunidad de un robo de datos.

10. Rogueware

Descripción. El rogueware es una aplicación que intenta parecerse a otra, por apariencia o nombre, para engañar y timar a los usuarios.

Síntomas. Al tratarse de un programa que se hace pasar por otro, simplemente haría falta comprobar si el programa en cuestión está llevando a cabo con su función o que el programa sospechoso está usando más memoria de lo que debería.

Riesgos. Generalmente se utiliza para conseguir dinero pero mediante esta estafa también se puede obtener información.

Métodos de prevención. Este tipo de programas intentan suplantar la identidad de otros softwares, por ello el principal método de prevención sería evitar descargar programas desde páginas no oficiales.

11. Spear phising

Descripción. Un ataque a una organización específica en la que el phisher simplemente obtiene detalles de un empleado y los utiliza para obtener un acceso más amplio al resto de la red a través de un envío de un email fraudulento u otras medidas.

Síntomas. Un empleado consciente de las amenazas que existen en la red, no tendrá problemas en identificar una acción de *spear phishing*. Esto gira alrededor de la ingeniería social y generalmente suele llevar a cabo sus ataques a través de correos electrónicos. Estos correos llegan a un empleado en concreto con la intención de que se descarguen el archivo adjunto y les permita entrar en el sistema. Es por esto que resulta de suma relevancia el instruir y concienciar a los empleados sobre los riesgos existentes.

Riesgos. El atacante obtiene acceso a la red a la que esté conectado la terminal infectada, pudiendo acceder a toda la información de esa red.

Métodos de prevención. Para prevenir ser atacados de esta manera, los empleados deben ser conscientes de que pueden recibir emails falsos que les pidan información. Algunos especialistas también recomiendan usar un buen gestor de contraseñas.

3.2. TÉCNICAS DE CIBERATAQUE CONTRA LA EMPRESA

1. Ataque DoS (Denial of Service)

Descripción. Aquel ataque que consigue que se pierda la conectividad a la red de la víctima, sobrecargando y obligando a una computadora, una red o un servidor a dejar de estar disponibles para sus usuarios.

Síntomas. El servidor de una empresa, al ser atacado con miles de solicitudes de comunicación, se sobrecarga y no puede dar respuesta a todas las peticiones dejando el servicio indisponible, de tal manera que por falta de capacidad o ancho de banda no se consigue dar respuesta a los usuarios que visiten la página y no puedan hacer uso de ella.

Riesgos. Puede sufrir grandes pérdidas económicas a causa de la interrupción de los procesos de negocio y los costes de la recuperación, sin tener en cuenta el daño a su reputación, el tiempo y recursos que se necesita para restablecer la confianza de los clientes. En negocios de tipo e-commerce, la banca y los servicios de juegos on-line un ataque de éxito puede tener consecuencias muy negativas.

Métodos de prevención. Es complicado impedir un ataque Dos o DDoS si no se tienen las herramientas o el conocimiento adecuado, por ello la mayoría de empresas subcontratan un servicio que les proteja de este tipo de amenazas.

Principales herramientas utilizadas. Dado que este tipo de ataque trata de sobrecargar un sistema o una red, la herramienta fundamen-

tal sería la botnet, cuanto más ordenadores zombies sobrecarguen el sistema que está siendo atacado, mayor será la efectividad del ataque.

2. Advanced Persistent Threat (APT)

Descripción. Se trata de un conjunto de procesos informáticos sigilosos y continuos que involucra complejas técnicas que utilizan softwares maliciosos para explotar vulnerabilidades en los sistemas., dirigidos a traspasar la seguridad de una empresa en concreto. Una APT, suele fijar sus objetivos en organizaciones o naciones por motivos de negocios o políticos.

Síntomas. Una APT es un ataque a gran escala que, dado a su elevado coste, se suele llevar a cabo contra empresas o incluso gobiernos. No tiene unos síntomas predefinidos puesto que cada APT es diferente y trata de pasar desapercibido.

Riesgos. Los riesgos a los que se somete una víctima de APT varían según el ataque dada la caracterización única de cada ataque. En general, cualquier víctima de APT está expuesta a grandes riesgos ya sean de tipo financiero o social.

Métodos de prevención. Es un ataque muy complejo y hará falta un equipo especialista en seguridad para intentar detenerlo.

Principales herramientas utilizadas. En cada APT se emplean herramientas distintas dado que cada ataque es único en su género pero todos comparten una característica, y es que no se trata de un simple ataque sino de un conjunto de procesos que dependiendo del atacante, puede emplear unas herramientas u otras.

3. Stealth Virus

Descripción. Virus que se adjuntan por sí solos a ciertos archivos del ordenador, para atacar y esparcirse rápidamente por todo el

equipo. Tienen una gran habilidad para camuflarse y no ser descubiertos.

Síntomas. No se suelen detectar síntomas evidentes puesto que la función principal de esta técnica es el sigilo. Por ello es importante realizar análisis en la terminal cada cierto tiempo.

Riesgos. El riesgo principal de esta técnica sería que un tercero tuviera algún tipo de control sobre el sistema y pasara de forma inadvertida de manera que no se tomarían medidas y el ciberdelincuente gozaría de total libertad.

Métodos de prevención. Un antivirus actualizado que realice análisis continuamente sería, en un principio, una forma de protegerse contra un virus furtivo.

Principales herramientas utilizadas. Es un virus informático que suele emplear un troyano u otra herramienta que le permita instalarse en el sistema sin ser detectado.

4. Zero Day Attack

Descripción. Es un tipo de exploit, un tipo de ataque que aprovecha y explota las vulnerabilidades de un sistema, las cuales son desconocidas por la empresa atacada y el público en general.

Síntomas. El Zero Day Attack no muestra unos síntomas claros, es por ello que es tan importante contar con buenas medidas de seguridad dado que, por lo general, cuando una empresa se da cuenta de que ha sido atacada, ya es demasiado tarde.

Riesgos. Los riesgos dependen de la gravedad de la vulnerabilidad existente en el sistema.

Métodos de prevención. Depende principalmente de la habilidad para detectar y neutralizar exploits zero-day y así evitar cualquier tipo de ataque de este tipo. En general, la defensa ante este tipo

de ataque consiste en las medidas de seguridad empleadas y los programas dedicados a ello.

Principales herramientas utilizadas. Se suelen emplear principalmente un virus informático, un troyano, un gusano o una backdoor aprovechando la reciente vulnerabilidad del sistema y asegurarse un acceso en el futuro.

5. HOAX

Descripción. Es como se conoce a los fraudes que se llevan a cabo a través de los bulos en internet.

Síntomas. El ciberdelincuente intenta que facilites dinero o información para lo que parecer ser una causa con fines sociales y sin ánimo de lucro pero que en realidad es mentira y solo quiere obtener información personal.

Riesgos. Se cometen estafas en las que se obtiene tanto dinero como información del usuario que posteriormente utilizará para llevar a cabo otro tipo de ataques.

Métodos de prevención. Ser consciente de la posibilidad de que existen fraudes que se cometen a través del correo electrónico o las redes sociales e ir con cuidado en relación a cualquier petición de información que no hayas solicitado previamente.

Principales herramientas utilizadas. El HOAX se llevaba tradicionalmente a través de correos electrónicos masivos pero con la aparición de las redes sociales, se ha facilitado su distribución y aumentado su alcance potencial por lo que cada vez más, se pueden observar este tipo de ciberdelitos en las redes sociales.

6. Control IoT

Descripción. Este ataque se aprovecha y toma control del IoT, esto es, tomar el control de la interconexión digital de objetos cotidianos a través de internet.

Síntomas. Aquellos dispositivos u objetos que estén interconectados a través de internet, actuarán de manera sospechosa o realizarán acciones que no se le ha ordenado. Esto significaría que está siendo controlado por otra persona.

Riesgos. Dependiendo del nivel de interconexión que haya en la empresa, el riesgo puede ser distinto pero aquella persona que tome el control del IoT sin autorización podrá controlar todo aquello que esté conectado a la red y hacer un uso ilimitado de ello. No solo representan un riesgo de seguridad sino que son una amenaza a nuestra privacidad.

Métodos de prevención. Existen herramientas que escanean todos los dispositivos que se encuentran conectados a una red para comprobar si existen vulnerabilidades que puedan ser explotadas para acceder a ellos y tomar el control.

Principales herramientas utilizadas. El control del Iot se basaría principalmente en el uso de exploits, aprovechando vulnerabilidades de la red para introducirse en ella. Aunque previamente se empleará un sniffer para conseguir información como la dirección ip de la red u otros datos que puedan ser de utilidad en el ataque.

7. Phishing

Descripción. Son aquellas estafas en las que se suplanta la imagen de una empresa o entidad pública y se engaña a la víctima solicitando datos como si fueran la empresa en la que está interesada la víctima.

Síntomas. La recepción de una solicitud que aparenta pertenecer a una empresa, normalmente reconocida, que pida que se faciliten

unos datos personales para alguna promoción de algún tipo u otras razones que resulten sospechosas.

Riesgos. Los riesgos a los que está expuesta una persona víctima de phishing son incontables. Dado que el phishing permite hacerse con los datos de su víctima para acceder a cuentas personales, pero el phishing también puede ser utilizado para instalar algún tipo de malware en ordenador que recibe la acción de phishing.

Métodos de prevención. La forma más segura para no resultar víctima de phishing es nunca responder a ninguna solicitud de información personal, ya sea a través de correo electrónico, llamada telefónica o SMS.

Principales herramientas utilizadas. El phishing puede llevarse a cabo de diversas maneras, desde un simple mensaje a un teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente o la recepción de un correo electrónico.

8. Spyware

Descripción. El spyware o programas espías son programas que, sin conocimiento o consentimiento para ello, recopilan la información de la que disponga el terminal afectado.

Síntomas. Los síntomas de infección son, entre otros, que habría un cambio en la página de inicio del navegador y que no se podría cambiar, se abrirían varios pop-ups, barras que se añaden en el navegador que no podemos eliminar o que la navegación se hace más lenta.

Riesgos. A través del spyware se puede tener acceso por ejemplo, al correo electrónico, a contraseñas, a la dirección IP, se puede obtener otra información como las páginas webs que visita, que software tienen instalados, cuales se descargan, que compras se hace por internet y datos más importantes como la tarjeta de crédito y las cuentas de banco. Quien se haga con esta información la podrá

usar con la misma libertad que su propietario original.

Métodos de prevención. Suelen entrar en los sistemas a través de páginas web que descarguen el malware u ocultos en programas gratuitos. Por ello, con un programa anti-spyware y una navegación prudente, se reducirían las probabilidades de infección.

Principales herramientas utilizadas. Existen distintos tipos de spyware y cada uno se dedica a una acción distinta pero en general, los spyware suelen utilizar keyloggers, troyanos, backdoor, gusanos y otros métodos que les permite tanto infectar al usuario como ampliar las posibilidades del delincuente.

9. Crimeware

Descripción. Cualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un crimen financiero en la red.

Síntomas. El crimeware es bastante difícil de detectar, sin embargo, suele presentar algunos síntomas como la ralentización general del sistema o la recepción no solicitada de correo electrónico, que pueden incluir archivos adjuntos. Incluso que el proveedor de servicios de Internet le avise de que el equipo está enviando spam, esto significaría que está siendo utilizado por un tercero.

Riesgos. Existen dos riesgos diferentes en el crimeware. Por un lado estaría la víctima contra la que se lleva a cabo el delito financiero en donde se le roba parte de su capital. Por otro, se encontrarían aquellas personas infectadas, pertenecientes a la botnet a través la cual se ha atacado y se ha llevado a cabo el ciberdelito financiero pudiendo ser confundidos con el ciberdelincuente.

Métodos de prevención. Disponer de programas antivirus y mantener actualizados los softwares instalados en el ordenador es la manera más básica de evitar cualquier infección. También puede consultar con su proveedor de servicios de Internet el nivel de protección que ofrece contra el crimeware.

Principales herramientas utilizadas. Virus informáticos, troyanos bancarios, gusanos o botnets son unas de las herramientas más utilizadas por los ciberdelincuentes que realizan acciones de crimeware.

10. Ransomware

Descripción. La finalidad de este ciberataque es bloquear o restringir el acceso del usuario al sistema hasta que se realice un pago al ciberdelincuente.

Síntomas. Que el usuario no pueda usar el sistema como habitualmente hace, que el sistema no deje instalar ni desinstalar software o que aparezcan programas que te piden, de la forma que sea, dinero son indicadores de que la terminal ha sido infectada.

Riesgos. Se pueden perder todos los datos que han sido retenidos por el ransomware y la tramitación del pago del rescate no garantiza la recuperación de dichos datos. Las perdidas pueden variar según el valor de la información que se tenga almacenado en el sistema.

Métodos de prevención. Es necesario estar protegidos con programas antivirus especializados y que estén actualizados de forma que no baje su efectividad. También se pueden realizar copias de seguridad en dispositivos que no estén conectados al sistema.

Principales herramientas utilizadas. Un método de llevar a cabo este tipo de ataque es emplear el correo electrónico para propagar un troyano que llevará a cabo la función de restringir el acceso a los archivos afectados.

3.3. CONCLUSIONES

El estudio de los tipos de ciberdelitos contra la empresa a través de numerosas fuentes secundarias pone de manifiesto la no existencia de una clasificación universal de los mismos. Igualmente se detecta cierta confusión terminológica entre herramientas para el ciberata-

que y técnicas de ciberataque, como consecuencia se elabora una clasificación propia, descrita en los epígrafes anteriores y detallada en los anexos 1 y 2 de la investigación.

3.4. BIBLIOGRAFÍA

Elaboración propia a partir de las siguientes fuentes secundarias:

ALONSO, C. (Maligno Alonso), YouTube,(2016)
https://www.youtube.com/watch?v=Q47uhvDby8U,
(Consultado por última vez el 10/02/2017)

Código Penal sobre propiedad intelectual: Ministerio de Educación, Cultura y Deporte, (2015) http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedadintelectual/la-propiedad-intelectual/preguntas-mas-frecuentes/registro/tex_codpenal.pdf,
(Consultado por última vez el 07/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/ddos-distributed-denial-of-service-attack/
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/zero-day-exploit/
(consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/exploit/
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/alternative-classifications/#spyw
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/hoax/
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/phishing/
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/dns-cache-poisoning-pharming/
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/stealth-virus/
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2015)
https://securelist.com/threats/strategies-for-mitigating-advanced-persistent-threats-apts/ (Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/alternative-classifications/#spyw,
(Consultado por última vez el 11/02/2017)

KASPERSKY LAB, Securelist, (2013)
https://securelist.com/threats/alternative-classifications/#crim
(Consultado por última vez el 11/02/2017

ASHTON, K (2009), «That «Internet of Things» Thing». RFID Journal
(Link de la nota de prensa)
http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

GUBBI, J. et al (2013): Future Generation Computer Systems (páginas 1645-1660). Editor Peter Sloot, Amterdam, (2013)
(Links del libro):
http://ac.els-cdn.com/S0167739X13000241/1-s2.0-S0167739X13000241-main.pdf?_tid=c9444e8a-f004-11e6-b8c2-00000aab0f27&acdnat=1486781582_dfa22c93347575dba62e74364b715683
https://www.journals.elsevier.com/future-generation-computer-systems/editorial-board

Bibliografía específica para IoT, Zero Day, Phishing y HOAX

VÁSQUEZ, E., (2016), La vulnerabilidad del IoT, un riesgo para las empresas https://securingtomorrow.mcafee.com/languages/espanol/la-vulnerabilidad-del-iot-un-riesgo-para-las-empresas/, (Consultado por última vez el 18/02/2017)

AGUILAR, Q., (2015), IoT podría ser una puerta hacia las vulnerabilidades https://revistaitnow.com/iot-podria-ser-una-puerta-hacia-una-vulnerabilidad/ (Consultado por última vez el 18/02/2017)

Cyber Aware Blog, (2014), HM Government, Five things small businesses get wrong about security http://www.cyberaware.gov.uk/blog/five-things-small-businesses-get-wrong-about-security, (Consultado por última vez el 18/02/2017)

Grupo de Delitos Telemáticos de la Guardia Civil (Unidad Central Operativa), (2015) https://www.gdt.guardiacivil.es/webgdt/alertas_gdt.php?id=230 (Consultado por última vez el 18/02/2017)

HENRYRAUL, (2016), Ataques de Día Cero. ¿Qué son y cómo combatirlos? https://henryraul.wordpress.com/2016/07/19/como-combatir-los-ataque-de-dia-cero/ (Consultado por última vez el 18/02/2017)

AVAST, (2015) https://www.avast.com/es-es/c-zero-day (Consultado por última vez el 18/02/2017)

Arizmendi Alonso, L. J. 2014 ‘’Ataques DoS y DDoS, prevención detección y mitigación’’ [en línea] disponible en <http://luisarizmendi.blogspot.com.es/2014/03/ataques-dos-y-ddos-prevencion-deteccion.html> Consultado: 22de febrero de 2017)

Cognitiva, (2016), IBM
http://cognitiva.la/que-es-ibm-watson/
(Consultado por última vez el 18/02/2017)

IBM, (2016)
http://www-03.ibm.com/security/es-es/solutions/risk-management-data-protection/
(Consultado por última vez el 18/02/2017)

SOPHOS, (2016), Amenazas de día cero,
https://www.sophos.com/es-es/security-news-trends/security-trends/zeroday-threats.aspx
(Consultado por última vez el 18/02/2017)

DDoS

http://aprenderinternet.about.com/od/Glosario/g/Que-es-Denegacion-de-Servicio.htm (Castro, L. 2017)

https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/ (Esau, A. 2015)

Ransomware

https://hipertextual.com/2016/12/que-es-el-ransomware-y-como-combatirlo (Lopez, J. M. 2016)

http://www.neoteo.com/los-mejores-programas-anti-ransomware/ por (Pardo, L. 2016)

Instituto Internacional Español de Marketing Digital, (2016), ‘’Qué es Ransomware’’ [en línea] disponible en <https://iiemd.com/que-es-ransomware-2/>
(Consultado: 23 de febrero de 2017)

ABC, (2016), ‘’Definición de Ransomware’’ [en línea] disponible en <http://www.definicionabc.com/tecnologia/ransomware.php>
(Consultado: 24 de febrero de 2017)

Stealth Virus

Enciclopedia de Características. (2017). 10 Características de los Virus Informáticos. Recuperado de: http://www.caracteristicas.co/virus-informaticos/
Fuente: http://www.caracteristicas.co/virus-informaticos/#ixzz4YyxD415b

Bonsembienate, F. (2016) http://hecate.com.ar/vr/vr13/anali.htm

4 EL CIBERDELINCUENTE EMPRESARIAL: PERFIL Y MAPAS DE COMPORTAMIENTO

RESUMEN

Actualmente la delincuencia informática se configura como uno de los grandes problemas de seguridad a nivel internacional. La falta de información al respecto, unida a la baja percepción de riesgo por parte de las empresas, organizaciones y usuarios y al hecho de que la comisión del delito vaya, en muchas ocasiones, un paso por delante de los avances realizados en materia de prevención, convierten los ciberataques en una amenaza constante en un entorno cada vez más tecnológico.

En este contexto, las actuaciones en materia de ciberdelincuencia, deben orientarse, cada vez más, hacia el conocimiento tanto del delito en sí mismo (herramientas, técnicas o escenarios) como del perfil del ciberdelincuente.

En este sentido, es importante señalar que la ciberdelincuencia es considerada por muchos autores como cualquier otra forma conocida de delito, aun cuando su aparición supone el nacimiento de una nueva forma de delinquir. Una de las razones reside en que las motivaciones del delincuente informático para cometer un acto delictivo son las mismas que las observadas en cualquier otro tipo de delincuente. A pesar de ello, es preciso apuntar que la concreción del perfil del ciberdelincuente ha evolucionado a lo largo de los últimos años[1], asistiéndose a un cambio de planteamiento fundamen-

1 Tradicionalmente se ha considerado que la delincuencia informática era propia de jóvenes de clase media, obsesionados por el medio en busca de poder, conocimientos y una mejor consideración entre sus amigos o compañeros de trabajo, que actuaban sin fines lucrativos inmediatos y con ánimo de venganza.

tado en la personalidad de los autores de las infracciones, que nos acerca a una clase de sujetos que intensifican sus objetivos, destacando, entre otros, los fines económicos.
Como consecuencia, en el presente artículo de investigación se propone un estudio de las variables psicográficas que determinan el comportamiento de los ciberdelincuentes a través del análisis de su personalidad, el modus operandi y la motivación para la comisión del delito.
Por otro lado, la propia naturaleza del ciberdelito hace necesario el estudio del perfil del ciberdelincuente atendiendo a la capacidad de control del medio donde comete el delito. Por ello, adicionalmente, se propone un estudio del comportamiento del delincuente informático teniendo en cuenta sus conocimientos y su dominio del entorno digital.
Por último, se establece la distinción entre el ciberdelincuente *insider* y el ciberdelincuente *outsider.* En el primer caso se hace referencia al ciberataque cometido por un sujeto que pertenece a la estructura empresarial y, por tanto, actúa desde el interior de la empresa y en el segundo caso, se hace referencia al ciberataque cometido por un sujeto que no pertenece a dicha estructura.
PALABRAS CLAVES: psicología, perfil del delincuente, *hacker*, *outsider*, *insider*, ciberdelito empresarial.

ABSTRACT
Crime and aggression is a constant in the history of mankind (Espinosa and Anzures, 1999). In the specific case of cybercrime, several studies conclude that this type of criminal activity can be considered as any other known form of criminal act, although in this type of social deviance reference is made to what has been conceptualized as online deviation where the criminal uses technology for the commission of crime used a computer, a smart phone or a PDA.
In this context, it could be said that while there is a new form of crime and the emergence of new crime scenes, the

motivations remain the same as pushing criminals to commit crimes in any other type of crime. The study of the profile of the cybercrime must be adjusted to the previous studies of the criminal act, the starting point of which, is the analysis of the criminal profile of the criminal.

Furthermore, the very nature of cybercrime makes it necessary to study the profile of the cybercriminals, taking into account the ability to control the environment where the crime is committed. Consequently, it is proposed a study of the behavior of the computer delinquent taking into account their knowledge and mastery of the digital environment.

Surprisingly, the conclusions reached permits to establish a direct relationship between this level of specialization and the psychological profile, since depending on the type of crime to which the objectives are referenced, the cybercrime can be from observed that acts for purely economic issues to the one that realizes it by revenge or by recognition.

KEYWORDS: psychology, criminal's profile, hacker, outsider, insider, business cybercrime.

4.1. EL PERFIL TECNOLÓGICO DEL CIBERDELINCUENTE

Para la comisión de un delito informático si bien se requieren de unos conocimientos mínimos relacionados con el medio informático, en general, los sujetos activos de los mismos no precisan conocimientos técnicos cualificados, bastando con un coeficiente intelectual medio y la oportunidad para delinquir.

De esta forma y en primera instancia, podríamos clasificar a los ciberdelincuentes en dos categorías diferenciadas:

(1) aquellos que manejan con facilidad los ordenadores y son expertos conocedores de los sistemas en red y

(2) aquellos cuyos conocimientos y habilidades no podrían ser categorizados en el nivel de expertos.

En el primer caso, normalmente, los ciberdelincuentes se especializan en delitos informáticos, mientras que en el segundo la tecnología, simplemente, es un medio para cometer el delito. De ahí que el perfil de ambos sea diametralmente opuesto, puesto que mientras para el primero el acto en sí supone un reto y contribuye a su crecimiento personal a través de la adquisición de conocimientos específicos, para el segundo el móvil únicamente está relacionado con la venganza personal o con la posibilidad de obtener algún beneficio económico.

4.1.1. Ciberdelincuentes especializados: la figura de los hackers

El término ***hacker*** hace referencia a un sujeto o comunidad experta en el área informática y Web, que domina aspectos como el lenguaje de programación, la manipulación de *hardware* y *software* o las telecomunicaciones y que dedica sus conocimientos y esfuerzos a intervenir o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o servicio.

4.1.1.1. Tipos de hacker según su filosofía

1. «White Hat Hackers»

Este tipo de *hackers* son los encargados de la seguridad de los sistemas informáticos. Los ***White Hat Hackers*** también ejercen el control a la hora de vulnerar sistemas, sin embargo, lo hacen para estudiar y fortalecer los fallos encontrados.

Se dedican a encontrar «*bugs*» (errores del sistema informático), con el fin de darlos a conocer a las compañías desarrolladoras y/o ayudar a mejorar el sistema de seguridad. Suelen intercambiar ideas, datos y herramientas en comunidades *online*.

2. *«Gray Hat Hackers»*

Este tipo de *hackers* usan sus habilidades para traspasar los niveles de seguridad y posteriormente ofrecer sus servicios como administradores de seguridad informática para corregir dichos errores.

Cabe destacar que pese a que puedan violar los principios éticos, lo hacen sin intención de delinquir. Realizan una labor de concienciación poniendo de manifiesto que la vulnerabilidad en los sistemas informáticos existe, si bien, en la mayoría de las ocasiones cobran por subsanar la brecha informática y solucionar el problema.

3. *«Black Hat Hackers»*

Conocidos como «sombreros negros» se dedican a realizar actividades para vulnerar la seguridad de sistemas, ingresar de forma violenta e ilegal a sistemas privados y extraer información restringida con intenciones malignas (robar, destruir datos), cuyo fin es económico o personal.

4.1.1.1.1. Tipos de Black Hat Hackers

Los *Cracker*

Los *crackers* son *hackers* que realizan actividades de *hacking* con fines maliciosos, destructivos o criminales. Son expertos programadores que utilizan sus conocimientos para modificar el comportamientos de sistemas y redes.

Su motivación suele ser económica, si bien detrás de cada uno de sus ataques se esconde una búsqueda de fama y reconocimiento muy ligada a una personalidad ególatra. Son obsesivos y se mueven por una afán destructivo e insaciable.

Normalmente los *crackers* se relacionan en grupos pequeños de difícil acceso.

Se distinguen diferentes tipos de *crackers* que se describen a continuación:

— ***Crackers* de sistemas.** Programadores y *decoders* que alteran el contenido de un programa.

— ***Crackers* de criptografía.** *Crackers* que se dedican a la ruptura de criptografía (*crackear* códigos).

— ***Phreakers.*** Son *crackers* especializados en los sistemas de telefonía, incluyendo la telefonía móvil y de voz. Inicialmente les movía el conocimiento, actualmente su motivación es fundamentalmente económica con tintes activistas.
Sus delitos están dirigidos hacia las empresas de telefonía y las grandes multinacionales, organizaciones que, bajo su punto de vista, estafan a sus clientes con facturas desmesuradas y servicios insuficientes.

— ***Cyberpunks.*** *Crackers* en línea definidos como vándalos de páginas web o sistemas informatizados.

Los *Viruckers*

Los *viruckers* son creadores de virus. Su principal objetivo es introducir un virus informático en un sistema para destruirlo, alterarlo o inutilizarlo.

Les gusta actuar de forma individual, por lo que no existe un sentimiento de comunidad. Son un grupo altamente peligroso y con una gran difusión. No disponen de ningún tipo de código ético.

Traficante de armas

Hackers que desarrollan y venden *malware* y otras herramientas de *hackeo* a otros ciberdelincuentes. En esta categoría se incluyen los *hackers* que utilizan los *ransomwares*.

Los traficantes de armas orientan su actividad hacia la consecución de beneficios económicos. Normalmente se mueven en mercados «subterráneos» (*Deepweb*). Sus ataques pueden dirigirse tanto a empresas como a personas físicas.

Banquero

Es el *Hacker* que se dedica únicamente al robo de información financiera. La información es utilizada en su propio beneficios, bien para ser vendida, bien para traficar con ella.

Sus principales armas son el *phishing* para robar las credenciales de los usuarios, las páginas falsas o el malware más avanzado para hurtar datos valiosos de la red de una organización.

Contratista

Son los denominados *hackers* por contrato («*hackers for hire*»). Sus objetivos son fundamentalmente económicos, prestando sus servicios en solitario o en grupo. No tienen ningún tipo de ética, por lo que les es indiferente atacar a una empresa que a una persona física.

Agente especial

Como su nombre indica, son personas con un nivel de especialización muy alto, pudiendo considerarse las «fuerzas especiales» de los *hackers* de sombrero negro. Normalmente llevan a cabo APT (amenazas persistentes avanzadas) y espionaje cibernético.

Suelen ser contratados por gobiernos extranjeros u organizaciones poderosas, aunque puede ser alguien del propio país o empresa y jugar un papel de agente doble, para atacar objetivos de gran valor, como son las grandes corporaciones del sector financiero, de tecnología de la información e incluso de defensa y energía, Los ataques

que llevan a cabo requieren mucho tiempo y son muy costosos y complejos. Pertenecen a grandes organizaciones criminales.

Ninja peso pesado

Estos cíberdelincuentes actúan con mucho sigilo para obtener información confidencial de empresas y corporaciones e intercambiarla por grandes cantidades de dinero, sin preocuparse por su uso final.

Normalmente actúan desde una organización perfectamente estructurada donde los líderes se convierten en agentes profesionales que operan como las compañías legítimas que esperan atacar.

Ciber-soldados

Su tarea principal es la de penetrar en los sistemas o redes de otro país con la intención de provocar daños, interrupciones o explotaciones con el objetivo final de inutilizar la capacidad militar de un oponente.

Aunque su cometido es principalmente militar y el Pentágono lo ha clasificado como una fuerza más a tener en cuenta junto a los soldados de tierra, mar y aire, los cíber-soldados también pueden realizar APT o trabajar como espías corporativos, a pesar de que su aprendizaje se orienta a un objetivo militar específico.

Spammer

Hacker que hace *Spam*. Difusión de mensajes no deseados, en su mayoría publicitarios. Frecuentemente se hace de manera automática y en masa, con el objetivo de poder llegar al mayor volumen de usuarios posible.

Los *Spam* pueden tener diferentes objetivos, desde molestar al receptor hasta generar polémica o publicitar un producto o servicio.

La ilegalidad normalmente tiene su origen en la forma en la que los *spammers* crean sus bases de datos.

Domainer

Es la persona que compra y registra dominios con el fin de monetizarlos. Se caracterizan por registrar dominios después de eventos de gran relevancia con el objeto de una posterior reventa.

Según expone Hernández, (2008) ‘*’una variante, bastante peligrosa, se dedica a montar empresas que ofrecen un servicio de comprobación de disponibilidad de dominios, que cuando es utilizado, lo compra para una futura reventa”*.

Espías Informáticos

Son aquellos que utilizan las técnicas más comunes de infiltración, sabotaje y chantaje. El espía informático accede a sistemas informáticos gubernamentales, a correos electrónicos de secreto privado, etc.

En el ámbito industrial tienen como objeto conseguir fórmulas, derechos de producción, etc. dañando en gran medida a las compañías.

Sniffer

Un *sniffer*, en realidad, es un programa de ordenador usado para controlar y analizar el tráfico red transmitido de una localización de red a otra. Estos programas son softwares muy especializados y con características no estandarizadas. El objetivo de este tipo de hackers es el robo de información con fines económicos mayoritariamente.

Terrorista informático

Ciberdelincuente que hace uso de los canales tecnológicos de información electrónica para llegar a la población e infundir terror y

miedo. Generalmente los motivos suelen estar relacionados con la religión, la economía o la política.

Phisher

El *phiser* es un *hacker* que suplanta la identidad de un usuario tras la obtención de sus datos. Su principal motivación es el dinero. Normalmente utilizan el envío de correos masivos para incitar al receptor del mensaje a hacer *clic* en un enlace incrustado.

El principal daño a la empresa es el posible deterioro en su imagen de marca derivado en primera instancia de la inseguridad que el cliente siente al utilizar de nuevo sistemas telemáticos para la realización de determinadas gestiones. Sus objetivos suelen ser las entidades bancarias.

Hoaxer

Son los *Hackers* que difunden bulos o correos en cadena. Su único objetivo es molestar y engañar, no teniendo ningún tipo de aspiración económica.

A través del reenvío de estos mensajes pretenden llegar al máximo número de personas posibles, pudiendo causar un deterioro importante en la imagen de una empresa, cuando se trata de un ataque directo a su posicionamiento de marca.

Hacktivista o anarquista

Hacker que ataca principalmente a aquellas organizaciones que considera que atentan contra los intereses sociales. Su objetivo es, por tanto, político o social. Al *hacktivismo* también se le conoce como «desobediencia civil electrónica». Se consideran Hackers de sombrero blanco. Si bien, en muchas ocasiones, sus acciones quedan desvirtualizadas al esconder fines con ánimo de lucro.

Uno de los grupos *hacktivistas* más conocidos en la actualidad es «Anonymous».

Una variante de este tipo de acciones son las protagonizadas por los **Netstrikes,** en este caso, sí que puede hablarse de protestas pacíficas en la red.

4.1.2. El ciberdelincuente no especializado

Emugger

Los *emuggers* son el grupo más numeroso de ciberdelincuentes. No poseen grandes habilidades o conocimientos técnicos. Desarrollan códigos maliciosos, *adwares* o *spams* y, una vez que perfeccionan la técnica, lo repiten una y otra vez con el fin de obtener ganancias económicas de manera muy rápida.

Wannabe

Aficionados que desean integrarse en un conjunto de especialistas de dicha actividad. Es un usuario que sabe más que el promedio, aunque es consciente de que no posee el mismo nivel del grupo y que debe adquirir más conocimiento. Etimológicamente proviene del inglés *«want to be»'* que quiere decir: quiero ser (Hernández, 2008).

Poseur

Parecido al *wannabe*, pero este usuario sólo tiene interés por intentar ser participante del grupo, sin que le importe en verdad los ideales, el conocimiento o cualquier otra cosa del mismo.

Sin embargo, se diferencia del anterior en que el *poseur* se aplica con mayor frecuencia en el ámbito fuera de internet, es decir, las personas que utilizan algunos estilos musicales o modas y aparien-

cias con la finalidad de autoconvencerse ser miembro de la misma. (Hernández, 2008).

Newbie

Es el considerado novato, que siente curiosidad por el mundo del *hacking*, busca información sobre el tema y descarga todas las utilidades y programas que puede en su ordenador para ver qué hacen. Pocas veces son capaces de penetrar en un sistema vulnerable, pero cuando lo hacen, se pierden debido a sus escasos conocimientos y no saben qué hacer.

Muchas veces se les confunde con los *lammers*, ya que suelen presumir de las habilidades que han aprendido. Su carrera delictiva suele encaminarse a:

1. Se convierten en *lammers*.
2. Maduran, aprenden y saben lo que hacen y se convierten en *hackers*.

Lammer

Es el usuario que alardea de poseer algunos conocimientos que en verdad no tiene. Con frecuencia, son aficionados con poca madurez, falta de sociabilidad o habilidades que intentar una manera falsa de destacar sobre los demás.

Script kiddie

Un *script kiddie* es un usuario con poca experiencia en los sistemas informáticos que, utilizando herramientas y mecanismos automáticos que han sido pre-empaquetados y definidos por otros, interrumpen en los sistemas informáticos.

Su principal motivación no es el dinero, sino alardear. Intentan demostrar que poseen las capacidades o *hackean* por pura emoción de hacer algo ilegal, tratando de ampliar su curriculum en su carrera hacia el cíber-crimen. Sin embargo, al no ser expertos, cometen errores como no ocultar la IP, quedando así expuestos.

4.2. EL PERFIL PSICOLÓGICO DEL CIBERDELINCUENTE

Tal y como se veía en apartados anteriores, la concreción del perfil del ciberdelincuente ha evolucionado a lo largo de los últimos años. Si bien tradicionalmente se ha considerado que la delincuencia informática era propia de jóvenes de clase media, obsesionados por el medio en busca de poder, conocimientos y una mejor consideración entre sus compañeros, que actuaban sin fines lucrativos inmediatos y con ánimo de venganza, en la actualidad, se asiste a un cambio de planteamiento fundamentado en la personalidad de los autores de las infracciones, acercándose a una clase de sujetos que intensifican sus objetivos, destacando los propósitos lucrativos.

Igualmente la peculiaridad de los medios empleados permite identificar un tipo de delincuente que no coincide con el delincuente marginal, sino con sujetos que tienen conocimientos del medio informático. De tal manera que mientras la criminología clásica señalaba los aspectos sociales, económicos y culturales como determinantes para la compresión de una específica delincuencia fundamentada en la exclusión social, la complejidad del ciberdelito rompe con esta forma de entender y de explicar el fenómeno criminal.

4.2.1. El psico-ciberdelincuente y el normo-ciberdelincuente

El **perfil psicológico** de una persona podría definirse como el conjunto de características que reúne un sujeto y que responde a su carácter, actitudes, aptitudes y comportamientos, frente a una situación particular o ante la sociedad como tal.

La **psicopatología** es la disciplina que analiza las motivaciones y las particularidades de las enfermedades de carácter mental desde un enfoque biomédico, psicodinámico, socio-biológico y conductual.

En concreto las psicopatología criminal analiza la relación entre el crimen y los trastornos psicológicos, identificándose las siguientes áreas de estudio:

1. Psicopatías
2. Psicosis
3. Neuropatías
4. Sociopatías o trastornos de la personalidad antisocial

A continuación se definen las cuatro tipos de trastornos y se profundiza en las diferentes características patológicas relacionadas con los sujetos que cometen un delito.

1. Psicópatas vs delincuentes comunes, delincuentes habituales y oportunistas

Las características que definen la psicopatía son el **egocentrismo, la grandilocuencia, el narcisismo, la auto-justificación, la impulsividad, la falta general de inhibiciones comportamentales y la necesidad de poder y control** (Pozueco *et. al.,* 2011b).

Hare (2003) señala estos rasgos como la combinación perfecta para los actos antisociales y criminales, pudiendo, incluso, afirmarse que los psicópatas presentan una mayor propensión que las otras personas a la comisión de actos antisociales, siendo unos candidatos perfectos para delinquir.

En este sentido, si bien es cierto que los psicópatas son responsables de una gran cantidad de delitos (Moltó *et. al*., 1997), no se puede aceptar de forma generalizada que estos sean unos criminales en potencia, siendo únicamente los psicópatas que se han conceptualizado como «**psicópatas criminales**» los que presentan una serie

de comportamientos que pueden relacionarse directamente con la comisión de actos delictivos (Hare, 2008).

Así, según Pozueco *et. al.,* (2011a) en el **plano afectivo**, estos individuos se caracterizan por experimentar emociones superficiales, por su falta de empatía, de ansiedad y de sentimientos de culpa o remordimiento, mostrándose incapaces para establecer vínculos duraderos con personas, principios u objetivos.

En cuanto al **plano interpersonal**, son arrogantes, egocéntricos, manipuladores, dominantes y enérgicos.

Finalmente, en el **plano conductual**, son irresponsables, impulsivos y buscadores de sensaciones. Suelen trasgredir con facilidad las normas sociales, y se caracterizan por un estilo de vida socialmente inestable que incluye comportamientos parasitarios y faltos de planificación.

Se puede afirmar, por tanto, que la personalidad psicópata posee **dos grandes áreas disfuncionales:** la afectiva y la conductual.

De la **disfunción afectiva** destaca su insensibilidad, fuerte narcisismo y frialdad emocional, mientras que las características de las **disfunciones conductuale**s coinciden con los síntomas recogidos del trastorno antisocial de la personalidad. Como consecuencia, la mayoría de los psicópatas serán considerados como poseedores de un trastorno antisocial pero no todos los diagnosticados con este último deberán ser considerados como psicópatas (Muñoz, 2010).

> «El psicópata criminal es un resultado de la interacción entre las circunstancias (el entorno) y las tendencias innatas; aunque podría señalarse que éste se autoconstruye, se hace a sí mismo en la medida en que tiene la posibilidad de elegir qué reacciones tomar ante lo que le sucede: así, cuando se habla de que «el delincuente se hace», se habla tanto de que las circunstancias lo construyen como de que él, en la medida en que tiene libertad de autorregulación y reacción, se autoconstruye como respuesta a esas circunstancias»

En este contexto, Garrido (2000) distingue entre las siguientes clases de psicópatas:

Psicópatas delincuentes. Divididos en dos grupos:

— **Antisociales o no integrados.** Crecen desde niños en un ambiente marginal y comparten con el resto de delincuentes comunes unas circunstancias que han propiciado su estilo de vida antisocial: padres que no les han enseñado un estilo de vida prosocial, tránsito decepcionante por la escuela, contacto temprano con la droga o asociación precoz con delincuentes. Son duros, egocéntricos y violentos. No tienen ninguna vinculación real con nadie y sólo buscan el placer más inmediato e intenso.

— **Integrados.** Son delincuentes, pero se camuflan como personas respetables. Son asesinos, agresores sexuales, maltratadores o delincuentes socioeconómicos, que tienen una «doble vida».

Son personas crueles y ambiciosas que se burlan de las leyes y de la sociedad sin reparo ninguno.

Psicópatas no delincuentes. Aunque no son técnicamente delincuentes, sus actos rayan en la ilegalidad. Pero, en su relación con los demás, sí que exhiben todas sus características de dominio y humillación.

En relación con los **psicópatas no integrados** y la ciberdelincuencia algunos psicólogos comienzan a profundizar en nuevos tipos de delincuentes tales como los «neópatas», **jóvenes usuarios de internet** de ambos sexos que utilizan la red como un **nuevo escenario** del cibercrimen y la ciberdelincuencia para expresar su agresividad o sus tensiones. Asistiéndose en los últimos años a la aparición de un grupo de ciberdelincuentes neópatas con edades más avanzadas.

Son sujetos con una vida social pobre e insatisfactoria, solitarios y que pueden perpetrar conductas antisociales o antijurídicas, escondiéndose tras el anonimato que les ofrece Internet, **con el único objetivo de dar salida a sus frustraciones, su odio, sus fantasías y a su necesidad narcisista de ser reconocidos por la sociedad a cualquier precio** (Velasco de la Fuente, 2016).

Algunas de las conductas delictivas que estos sujetos desarrollan a través de Internet son:

— Seleccionar a víctimas de violaciones a través de las redes sociales.

— Utilizar YouTube para difundir comportamientos agresivos tales como golpear a un indigente, pegar a una compañera en los baños del colegio, o actos vandálicos sobre propiedades ajenas.

— Acosar a terceros: trolls.

— Cometer delitos informáticos o contra los derechos de autor, con la única finalidad de lograr el aplauso y el reconocimiento de los demás internautas.

— Insultar, amenazar y calumniar amparándose en el pseudo-anonimato que ofrece la red.

— Anunciar masacres o anunciar un asesinato, etc.

Este tipo de ciberdelincuentes padecen, además, en la mayoría de los casos, trastornos de la personalidad antisocial o sociopatías.

A este respecto, Pueyo (2007) señala que **el comportamiento psicopático criminal puede desarrollarse como consecuencia de una reacción a vivencias individuales de estrés y tensión.** De esta manera la American Psychological Association (1994), define el estrés como «*la respuesta fisiológica y psicológica que desarrolla una persona después de estar expuesta a un suceso que presenta una amenaza a su integridad física o psicológica».*

De esta manera, autores como Agnew (2006) apuntan a que diversas fuentes de tensión pueden afectar al individuo y destacan la imposibilidad de lograr objetivos sociales positivos, ser privado de gratificaciones que posee o espera, y ser sometido a situaciones aversivas ineludibles.

Como resultado de las tensiones, se generan en el sujeto emociones negativas que como la ira energizan su conducta en dirección a corregir la situación, así una posible acción correctora contra una fuente de tensión experimentada es la conducta delictiva, haciéndose imprescindible entender que la supresión de la fuente alivia la tensión y de ese modo el mecanismo conductual utilizado para resolver la tensión se consolida.

Por otro lado Cleckley (1976), advierte que no debe confundirse el psicópata ni con el oportunista ni con el delincuente común.

Concretamente, este autor, afirma que **el oportunista**, que no tiene porqué presentar las características del psicópata, a menudo logra asentarse económicamente con provecho, mientras que el psicópata por su aversión a las reglas, difícilmente encaja en estructuras férreas.

Estos delincuentes son menos propensos a delinquir de forma impulsiva porque «*tienen un interés superior en ser deseables socialmente, y por lo tanto están sujetos a mayores restricciones personales y sociales sobre su comportamiento*» (Wortley, 2006: 15).

Cornish y Clarke (2003: 63) afirman en su teoría de la elección racional que éstos son delincuentes «*cuyos modos de vida son convencionales en lugar de delictivos, y cuyas necesidades están satisfechas en general. Como mínimo, este tipo de delincuente es el que siente la necesidad de justificar su conducta*».

Además, están comprometidos con la sociedad y demuestran tener razonamiento moral.

En comparación con el psicópata, los delincuentes oportunistas son mucho más propensos a involucrarse en la actividad delictiva de forma transitoria. Sus compromisos morales y sociales limitan su participación en la actividad delictiva, además del miedo al castigo y la posibilidad de ser descubierto.

Delincuente común y psicópata tampoco son conceptos equiparables. El psicópata rara vez se aprovecha de los beneficios que genera por el delito, y casi nunca se implica de modo consistente en la carrera criminal.

El delincuente común, por su parte, persigue objetivos comprensibles, aunque con medios y procedimientos rechazables. El psicópata, por el contrario, pretende metas no siempre asumibles, comprensibles por los demás e incluso, a menudo, comete el delito sin lograr ventaja material alguna.

El delincuente común suele protegerse a si mismo, el psicópata no pocas veces se pone en situaciones que le perjudican y actúa de forma notoriamente insensata, y sin necesidad alguna llevado por la impulsividad que le caracteriza (García Pablos de Molina, 2003, p. 632).

En relación a los delincuentes comunes podrían ser considerados como aquellos que se dedican a la comisión de actos delictivos de

forma permanente convirtiéndose en delincuentes habituales. Es la persona que vive del delito. Pueyo (2007) señala a este respecto que el inicio y mantenimiento de la carrera delictiva se relaciona con el desarrollo del individuo, especialmente en la infancia y la adolescencia.

Este colectivo se puede subdividir en atención a los fines y a la forma de realizar los actos delictivos. Así, podríamos diferenciar delincuentes habituales profesionales y delincuentes habituales neo-profesionales (Vic, 2016).

Los primeros serian aquellos delincuentes habituales que para la consecución de sus fines utilizan medios idóneos. Sus características son:

— realizan sus actos delictivos con una cuidadosa planificación.

— utilizan medios informáticos, electrónicos y mecánicos adecuados a cada acto.

— se encuentran integrados, normalmente, en una organización estable y

— pueden desplegar sus actos con operatividad internacional.

Los delincuentes habituales neo-profesionales se diferenciarían de los anteriores en que la planificación de los actos delictivos sería rudimentaria; presentarían carencias de tecnicismos que suplirían con habilidades; actuarían en grupos reducidos o de forma individual; los beneficios que obtendrían con sus actos serían menores; sería una delincuencia residual y artesanal y los delincuentes presentarían deficiencias culturales y sociales. Este tipo de delincuentes son personas antisociales que tienen predisposición para el crimen.

En lo referente a los ciberdelincuentes y la delincuencia habitual se podría hacer referencia, igualmente, al grupo de delincuentes especializados que actúan desde el conocimiento, mientras que existe un grupo de ciberdelincuentes que actúan sin especialización y que buscan un reconocimiento social rápido o el beneficio económico a corto plazo.

En este línea, en los siguientes epígrafes se hace una distinción entre lo que se ha conceptualizado como ciberdelincuentes especializados o maestros y ciberdelincuentes intrusos.

2. Psicóticos

Los trastornos psicóticos son psicopatologías graves donde la persona pierde el contacto con la realidad. Los síntomas más característicos son las **alucinaciones y los delirios**.

Los delirios son falsas creencias. En cambio, las alucinaciones son percepciones falsas, como oír, ver o sentir algo que en realidad no existe.

Los delirios son característicos del trastorno delirante, mientras que las alucinaciones predominan en el trastorno esquizofrénico. Ambas psicopatologías son los trastornos psicóticos más conocidos.

Tipos de Trastornos Psicóticos

Según la cuarta edición del Manual Diagnóstico y Estadístico de Trastornos Mentales (DSM IV) existen los siguientes trastornos psicóticos:

- **Esquizofrenia.** Trastorno en el que la persona que lo padece sufre alucinaciones y pensamientos perturbadores que le aíslan de la actividad social.

  Existen diferentes tipos de esquizofrenia:

  — **Esquizofrenia paranoide.** Es la más habitual. Predominio de ideas delirantes.

  — **Esquizofrenia hebefrénica.** Predominio de alteraciones emocionales.

  — **Esquizofrenia catatónica.** Caracterizada por alteraciones motoras. Con inmovilidad persistente, aunque puede ir alternando con crisis de agitación.

— **Esquizofrenia indiferenciada.** Cuando una esquizofrenia no reúne los criterios de los de los tipos anteriores o presenta varios síntomas a la vez.

- **Trastorno Delirante.** El trastorno delirante, también conocido como paranoia, se caracteriza porque el paciente tiene una o varias ideas delirantes y está convencido de que son ciertas. Los pacientes suelen resistirse y, en muchas ocasiones, tienden a ocultar el delirio, lo que se conoce como «delirio encapsulado».
- **Trastorno Psicótico Breve.** Tal y como su nombre indica es una psicopatología en la que puede aparecer un brote psicótico con los mismos síntomas que un trastorno esquizofrénico, pero que dura unos días y no vuelve a afectar al paciente nunca más. Por tanto, desaparece sin dejar secuelas. Suele ser una respuesta a un evento traumático como la muerte de algún familiar o a una época de estrés extremo.
- **Trastorno Esquizofreniforme.** El trastorno esquizofreniforme es parecido al trastorno psicótico breve, pero dura entre 1 mes y 6 meses. Los pacientes muestran distintos síntomas de la esquizofrenia: delirios, alucinaciones, discurso desorganizado o catatonia.
- **Trastorno Esquizoafectivo.** En este tipo de trastorno psicótico el paciente experimenta síntomas de la esquizofrenia junto con síntomas de un trastorno del estado de ánimo, ya sea al mismo tiempo o de manera alterna.
- **Trastorno Psicótico Compartido o «folie à deux».** Es una patología extraña y poco habitual, puesto que son dos las personas que comparten los mismos delirios y alucinaciones. Se desconoce la causa exacta de este trastorno psicótico, sin embargo, es posible que el estrés y el aislamiento social jueguen un papel importante en su desarrollo.
- **Trastorno Psicótico inducido por sustancias.** Este tipo de trastorno se caracteriza por ser provocado por la intoxicación debida

al uso drogas o fármacos. Los síntomas por lo general aparecen rápidamente y duran poco tiempo. Los síntomas más comunes son las alucinaciones visuales, desorientación, y problemas de memoria. Algunas sustancias que provocan este trastorno pueden ser: la marihuana, el alcohol, la cocaína, las anfetaminas, inhalantes alucinógenos, el MDMA, los opiáceos, los sedantes, los hipnóticos y los ansiolíticos.

- **Trastorno Psicótico debido a una enfermedad médica.** El trastorno psicótico debido a enfermedad médica ocurre cuando los síntomas de dicho trastorno son el resultado de enfermedades que afectan a la función cerebral, por ejemplo, un tumor cerebral.

En relación con el delito las personas que sufren algún tipo de psicosis y desarrollan una conducta criminal cometen en su mayoría delitos contra las personas, concretamente homicidio, delitos de lesiones y delitos sexuales.

Relacionándose los delitos contra el patrimonio y el orden socioeconómico con aquellos sujetos que padecen un trastorno delirante o esquizotípico, siendo este tipo de actos delictivos los que pueden relacionarse directamente con ciberataques empresariales.

En el caso de las personas que sufren un trastorno delirante suelen delinquir en solitario, porque piensan que se si asocian con alguien serán traicionados. Suelen ser delitos con altos niveles de impulsividad y frialdad emocional, ya que creen hacer justicia por el daño que los otros les están haciendo.

En muchas ocasiones, las personas con trastorno delirante de la personalidad se suicidan tras haber cometido el delito, ya que se dan cuenta de lo que han hecho.

Por otro lado, los sujetos que padecen trastornos esquizotípicos no suelen verse implicados en ningún tipo de acto delictivo, si bien en caso de desarrollar una conducta criminal suelen delinquir en solitario y las víctimas son indistintamente conocidas o desconocidas (Quejido, 2016).

3. Neuropatía

Las neuropatías son una enfermedad del Sistema Nervioso Periférico y representan, desde el punto de vista criminológico, los trastornos más complicados de determinar, debido, entre otros, a la dificultad de su diagnóstico.

Las neurosis pueden definirse como reacciones complejas de la personalidad asociadas a trastornos de la afectividad. A diferencia de otras enfermedades que se presentan de manera impulsiva o violenta, la neurosis se va estructurando paulatinamente, siendo el individuo consciente del proceso psíquico interno que vive en todo momento.

La sintomatología asociada a la neurosis se caracteriza por una sensación de angustia que es controlada a través de toda una serie de defensas de tipo psicológico. El neurótico responde a un perfil de sujeto que es incapaz de dominar su situación de stress y esto es lo que convierte a la angustia en la fuente dinámica común de la neurosis.

La neurosis puede clasificarse de la siguiente manera:

— Neurosis de angustia.

— Neurosis fóbica.

— Histeria.

— Neurosis obsesivo-compulsiva.

— Neurosis depresiva.

— Hipocondriaca.

Según Marchiori (1975) en la conducta delictiva del neurótico se advierten conductas ambivalentes, conflictivas, sentimientos de culpa y dudas.

Así, el neurótico puede proyectar un comportamiento de extrema violencia y agresividad exterior como es el homicidio o una hábil e

inteligente manipulación en las conductas de estafas hasta llegar a una problemática en su autoestima que lo conducen al suicidio.

La angustia de la personalidad neurótica es tan intensa que se exterioriza a través de comportamientos violentos y en una conflictiva interpersonal especial. Es decir, cabría pensar que la intensa angustia y frustración por sus vivencias e imágenes de desprotección interna, su inestabilidad emocional y la presión de las circunstancias ambientales se atenúan a través de la agresividad.

A pesar de esto, el neurótico no entra fácilmente en conflicto con la legalidad penal ya que su propia naturaleza insegura, angustiada e inestable se lo impide. De hacerlo, es más autoagresivo que heteroagresivo.

En líneas generales se puede afirmar que los trastornos de ansiedad pueden generar delitos contra el patrimonio y conductas sexualmente desviadas como el exhibicionismo, mientras que los trastornos obsesivos son proclives a conflictos como la cleptomanía o piromanía.

Por otro lado es importante señalar que este tipo de individuos por el hecho de ser sugestionables y, por tanto, manipulables, pueden ser coaccionados para que colaboren en actos delictivos como coautores o encubridores.

4. Sociópatas o trastorno antisocial de la personalidad

Siguiendo la definición del Manual Diagnóstico y Estadístico de los Trastornos Mentales en su cuarta edición revisada, el Trastorno Antisocial de la Personalidad se caracteriza por «*un patrón general de desprecio y violación de los derechos de los demás, que comienza en la infancia o el principio de la adolescencia y continúa en la edad adulta*».

Para Mora (2004) los sociópatas se diferencian de los psicópatas en algunas características psicológicas y conductuales, a pesar de que ambos manifiesten una clara inadaptación social y agresividad, pero esta última, en el caso del Trastorno Antisocial de la Personalidad,

es reactiva a una situación, mientras que la agresión y violencia sin motivo aparente, dirigida a conseguir un objetivo concreto, caracteriza a la psicopatía.

En este sentido, y como ya se había indicado en el epígrafe relativo a las psicopatías, la existencia de una psicopatía primaria, caracterizada por un temperamento innato y una psicopatía secundaria, con la posibilidad de tener una mayor capacidad de sentir ansiedad y culpa como resultado de un proceso inadecuado de socialización, aunque sin descartar la influencia de alteraciones biológicas e incluso retrasos madurativos, incide en la diferenciación entre psicópata y sociópata (Garrido, 2005).

La relación entre psicopatía y trastorno antisocial de la personalidad es, por lo tanto, asimétrica, es decir, prácticamente el 90% de los delincuentes psicópatas cumplen los criterios del Trastorno Antisocial de la Personalidad, pero sólo el 25% de éstos podría diagnosticarse de sociopatía.

Pueyo (2007) señala a este respecto que una de las explicaciones del acto delictivo reside en **la ruptura de los vínculos sociales.**

Así, por ejemplo, Hirschi (1969), postula qué existen una serie de contextos principales en los que las personas se unen a la sociedad: la familia, la escuela, el grupo de amigos y las pautas de acción convencionales, tales como las actividades recreativas o deportivas.

El enraizamiento a estos ámbitos se produce mediante cuatro mecanismos complementarios: el apego, o lazos emocionales de admiración e identificación con otras personas, el compromiso, o grado de asunción de los objetivos sociales, la participación o amplitud de la implicación del individuo en actividades sociales positivas (escolares, familiares, laborales...), y las creencias o conjunto de convicciones favorables a los valores establecidos, y contrarias al delito, siendo la ruptura de los anteriores mecanismos de vinculación en uno o más de los contextos sociales aludidos, la consecuencia más directa las conductas antisociales.

En este sentido, la teoría del autocontrol de Gottfredson y Hirschi (1990) señala que los individuos toman en la mayoría de las ocasiones decisiones racionales. Esto significa que los individuos eligen las acciones que les aportan mayor placer y menor dolor. Así las personas que tienen bajos niveles de autocontrol, o lo que es lo mismo, incapacidad de ver las consecuencias de sus acciones, encontrarán el crimen atractivos puesto que son «*impulsivos, insensibles, agresivos, temerarios, cortos de miras y no verbales*».

Según Gottfredson y Hirschi (1990) el bajo autocontrol, está muy relacionado con un control parental ineficaz.

Actualmente la teoría general del delito en cuanto a la relación entre bajo autocontrol y conducta antisocial ha demostrado que el bajo autocontrol se relaciona positivamente con ciberdelitos como la piratería digital.

4.2.2. Clasificación del ciberdelincuente atendiendo a su perfil psicológico

Atendiendo a la revisión de la literatura existente sobre el perfil psicológico del delincuente, así como al análisis realizado del ciberdelito se propone la siguiente clasificación del ciberdelincuente atendiendo a su personalidad (véase Tabla 4.1.).

Tabla 4.1. Clasificación del ciberdelincuente empresarial en función de su personalidad

PSICO-CIBERDELINCUENTE		NORMO-CIBERDELINCUENTE	
CIBER-PSICÓPATA	**INTEGRADO** Ciberdelincuente-exitoso **NO INTEGRADO** Ciberdelincuente-ejecutor	**CIBER–OPORTUNISTA**	Ciberdelincuente-ventajista
CIBER-NEURÓTICO	Ciberdelincuente-manipulable	**CIBER–COMÚN**	Ciberdelincuente - pandillero Ciberdelincuente – rebelde
CIBER-PSICÓTICO	Ciberdelincuente-enajenado Ciberdelincuente-salvador	**CIBER-HABITUAL**	Ciberdelincuente neo-profesionales Ciberdelicuente-profesional Ciberdelicuentes- a sueldo
CIBER-SOCIOPÁTA	Ciberdelicuente-inadaptado		

FUENTE: Elaboración propia

A continuación se define el comportamiento de cada uno los tipos de ciberdelincuentes identificados:

(1) Psico-ciberdelincuente

El perfil psicológico del psico-delincuente responde al de un sujeto que posee algún tipo de trastorno de la personalidad.

Según el DSM-IV (Manual Diagnóstico y Estadístico de los Trastornos Mentales), los rasgos de personalidad son tendencias persistentes de formas de percibir, relacionarse y pensar sobre el entorno y uno mismo y que se manifiestan en una amplia gama de contextos sociales y personales.

Dichos rasgos constituirán trastornos de personalidad cuando sean inflexibles, desadaptativos y causen deterioro funcional significativo o malestar subjetivo. Aunque la persona que padece un trastorno de personalidad mantenga íntegra las facultades intelectivas superiores

y comprenda que un hecho es ilícito, puede no llegar a poner en práctica estas capacidades de manera eficaz si el trastorno es grave.

Verdaderamente, no puede hablarse de una «personalidad delincuente» dadas las grandes diferencias individuales existentes aunque sí se ha demostrado que el infractor sistemático se caracteriza por los siguientes rasgos (Muñoz, 2010):

— hostilidad,

— búsqueda de sensaciones,

— desviación psicopática,

— hipomanía y depresión,

— bajo ajuste emocional y asertividad.

Por lo tanto y en líneas generales se puede concluir que un ciberdelincuente-psicopáticos *«es aquel sujeto que adopta un comportamiento delictivo en la red, valiéndose en muchas ocasiones de sus conocimientos tecnológicos y del anonimato que le confiere el entorno digital, adoptando un comportamiento caracterizado por la hostilidad, un bajo ajuste emocional y falto de empatía y dirigido por una desviación psicopatológica (psicosis, neurosis, trastorno de la personalidad antisocial o psicopatía)».*

Los diferentes tipos de psico-ciberdelincuentes vendrán definidos por el tipo de psicopatología que padezcan, estableciéndose cuatro grupos diferenciados que se definen a continuación (véase Tabla 4.2.).

TABLA 4.2. Clasificación de los psico-ciberdelincuentes

PSICO-CIBERDELINCUENTES
Ciber-psicópata
Ciber-psicótico
Ciber-neurótico
Ciber-sociópata

FUENTE: elaboración propia

Ciberpsicópata

La patología clínica que define al ciberdelincuente psicópata es la psicopatía. Siguiendo la clasificación de Garrido (2000) se identifican dos tipos de ciber-psicópatas: integrados y no integrados. Ambos perfiles se describen a continuación.

Integrado: ciberdelincuente-exitoso

Los ciberpsicópatas integrados se enmarcarían dentro del perfil que se ha denominado como ciberdelincuente-exitoso «*sujeto de clase media, media-alta, mayoritariamente varón y cuyo comportamiento estaría condicionado por la búsqueda de nuevas sensaciones a través de la comisión del delito, así como por la obtención de un beneficio de tipo económico. Son profesionales de éxito y su vida personal es aparentemente perfecta. Son narcisistas, tienen una gran capacidad para mentir y manipular, así como una total ausencia de remordimiento*».

Concretamente se podría resumir su perfil en los siguientes puntos:

— Otorga alto valor a los bienes materiales, hasta el punto de que su tensión patológica se libera con la ganancia.

— Es un sujeto egocéntrico, que compensa la soledad a través de gestos de generosidad en un intento por «comprar» el cariño y el reconocimiento.

— Es narcisista y suele sentirse superior al resto de las personas.

— No tiene límites éticos, lo que le convierte en una persona fría y calculadora.

— Nunca siente remordimientos.

Los ciberdelincuentes-exitosos protagonizan el delito durante el ejercicio de sus actividades profesionales. Las actividades delictivas más frecuentes relacionadas con estos sujetos son los fraudes, la evasión fiscal, la competencia desleal y los delitos contra el libre comercio.

En este contexto el ciberdelincuente-exitoso, es proclive a cometer actos relacionados con ganancias súbitas y especulativas y negocios con información privilegiada y confidencial atentando contra la ética empresarial.

Asimismo, se le puede ver involucrados en fraudes financieros, estafas colectivas, corrupción de funcionarios públicos y corrupción de empleados privados, manipulación contable y fraude corporativo o gestión de legitimación de capitales (blanqueo) de origen ilícito de organizaciones criminales.

Normalmente se infiltran en organizaciones que no dispongan de los medios de defensa adecuados y causar estragos en su seno. Pueden planear sus ataques desde dentro de la compañía como parte de la estructura de la misma o desde fuera. En este último caso y dado su carácter manipulador es frecuente que busque a otro individuo que le facilite la información necesaria para perpetuar el delito.

Este tipo de delincuente es una variante específica de lo que ya se ha tipificado como delincuencia *pret-a-porter* (ControCapital, 2014) enmarcada en la delincuencia económico-financiera, muy relacionada con la delincuencia de cuello blanco.

Generalmente, el delincuente económico financiero una vez se le hace responsable penalmente de algún acto delictivo que le suponga una pena privativa de libertad, continuará delinquiendo desde la cárcel. Por lo que la sanción con mayor carácter disuasivo para este perfil criminal es la confiscación de sus bienes y la extinción de dominio sobre su patrimonio.

Los Crakers podrían encajar en este tipo de perfil. En líneas generales los ataques protagonizados por este tipo de ciberdelincuentes son cometidos por sujetos egocéntricos, narcisistas, en busca de fama y con una clara motivación económica. Lo que situaría a los ciber-ventajistas como individuos con una alta especialización tecnológica.

No integrado: ciberdelincuente-ejecutor

El ciberdelincuente-ejecutor responde al perfil de un sujeto que ha crecido en un ambiente marginal, lo que le ha propiciado un estilo de vida antisocial. Son egocéntricos y violentos. No tienen ninguna vinculación real con nadie y sólo buscan el placer más inmediato e intenso.

Sienten la necesidad de satisfacer placeres ilícitos o moralmente reprobables incurriendo en acciones de riesgo. Además, carecen de determinados sentimientos básicos tales como compasión, vergüenza, sentido del honor, remordimientos o conciencia.

Disfrutan humillando, por lo que no dudaran en difamar todo aquello que no coincida con su forma de ver las cosas.

Los ciber-ejecutores son una combinación de dos perfiles ya definidos previamente, los *haters* y los *doxings*.

— *Haters* u «odiadores». Desprecian o critican destructivamente a una entidad por causas poco racionales o por el mero acto de difamar. Los mensajes de odio tienen como única pretensión causar el máximo daño posible.

— *Doxings*. Son los llamados ciber-acosadores. Su actividad se centra en la publicación de datos que sirven para avergonzar y difamar públicamente a sus víctimas, pudiendo llevar el acto criminal al mundo real.

Este tipo de ciberdelincuentes pueden utilizar los «*flame*[2]» como herramienta para hacer apología del terrorismo o de incitar a la comisión de otros delitos.

La elección de sus víctimas responde, en la mayoría de las ocasiones, a criterios totalmente aleatorios.

1 Mensajes enviados a un foro, lista de correo o redes sociales cuyo objetivo es provocar reacciones airadas de sus participantes. Suele contener insultos u ofensas y puede estar dirigido a todos en general, a un grupo de usuarios o a alguien en particular.

Ciberneurótico: ciber-manipulable

Los ciberdelincuentes manipulables son personas inseguras de sí mismas como consecuencia de la angustia que padecen. Viven constantemente una situación de miedo que les impide delinquir de motu propio, si bien podrían hacerlo en nombre de otros.

La figura más representativa de este grupo de ciberdelincuentes en el entorno laboral coincidiría con la de un empleado que es convencido por otro empleado o por alguien de fuera de la compañía para actuar como peón en la perpetración del ciberdelito.

Las razones que les pueden llevar a consentir cometer este tipo de delitos son las siguientes:

— Falta de confianza en uno mismo, lo que hace que otras personas asuman decisiones importantes sobre su propia vida.

— Sentimientos de incompetencia que le llevan a subordinar sus necesidades a las otras personas.

— Miedo a la soledad y al abandono.

— Temor a la discrepancia lo que le lleva a aceptar que se equivoca con tal de no perder la aprobación ajena.

— Baja autoestima.

Un ejemplo de ciber-manipulable serían los terroristas informáticos. Este tipo de ciberdelincuentes, son sujetos que poseen muy poco control sobre sus acciones, ya que muestran inseguridad y sensación de pérdida en la vida.

La sensación de pertenencia a grupo les invita a hacer cualquier cosa por ese grupo y sus creencias, aunque esto conlleve delinquir.

Ciberpsicótico: el ciber-enajenado

El perfil del ciber-enajenado está condicionado por un trastorno delirante que le sume en una serie de creencias falsas cuya consecuencia más directa es la pérdida del contacto con la realidad, como consecuencia, sus acciones son incontroladas y si sitúan fuera de todo sentido común.

Se caracterizan por su aspecto descuidado tanto en su aspecto personal como su domicilio, vehículo etc. y desorden en su vida tanto afectiva como social. Suelen ser solitarios y ofrecen una apariencia extraña a los demás.

El sujeto enajenado tiene sospechas infundadas y piensa que otros están complotando en contra de él/ella. La imagen de sí mismo es generalmente despreciada.

Estos individuos no dudarán en atacar a quien les ataque.

El modus operandi del ciber-enajenado es el mismo que el del ciber-ejecutor, con una salvedad, mientras que los ciber-ejecutores eligen sus víctimas de forma aleatoria, el enajenado las elige porque se siente amenazado, humillado o ultrajado por ellas. Este sentimiento es una creencia, por lo que se enmarcaría dentro del concepto ya definido de delirio.

Un ejemplo de este tipo de ciber delincuente sería el Hoaxer que actúa como reacción a lo que ellos han sentido como una amenaza. Si bien cuando no tengan un objetivo concreto y la elección de la víctima no responda a la venganza, se hablaría de un trastorno de carácter psicopático, el ciber-ejecutor.

Por otro lado, es importante tener en cuenta que existe una variante dentro del ciberdelincuente-enajenado y es aquel donde el sujeto cree haber sido elegido para desarrollar una misión muy importante

o para salvar al mundo de algún peligro indefinido. Este individuo sufrirá delirios de grandeza que le llevaran a cometer delitos de carácter muy específicos, entre otros motivos, porque dichos delirios pueden convertirse en alucinaciones que conviertan la creencia en realidad. **Es el ciber-salvador.**

Este delincuente no dudará en atacar todo aquello que se convierta en una amenaza o suponga un obstáculo en sus planes, siendo la diferencia fundamental con los enajenados el hecho de que actúen bajo la influencia de las alucinaciones y no de los delirios. Igualmente, mientras que los enajenados buscarán con la difamación a un grupo de personas que difundan y apoyen sus argumentos, el ciber-salvador buscará seguidores de su causa, ejerciendo de líder y guía, como consecuencia del sentimiento de superioridad que acompaña a sus delirios y alucinaciones.

Cibersociópata: ciber-inadaptado

Este tipo de ciberdelincuente no debe confundirse con el ciberpsicópata no integrado, si bien padece un trastorno de la personalidad antisocial no padece ningún tipo de psicopatía. Su compartimiento, como ya se vio en epígrafes anteriores es reactivo a una situación determinada.

Este tipo de delincuente no tiene una predosposición a la actividad delictiva, siendo las circunstancias vividas en su grupo de socialización primaria las que en la mayoría de las ocasiones les lleva a iniciarse en la delincuencia.

El ciber-inadaptado busca satisfacer necesidades de pertenencia a grupo, autoestima y autorrealización. Tienen problemas de identidad y el reconocimiento público les ayuda a sentirse seguros.

Por ello no dudarán en quebrantar la seguridad de su empresa, buscarán brechas demostrando su superioridad, puesto que no dudarán en descubrirse, argumentando que lo han hecho por el bien

de la organización, ofreciendo la posibilidad a la compañía de estar a salvo ante amenazas externas.

(2) Normo-ciberdelincuente

Se identifica el normo-ciberdelincuente como aquel delincuente en la red que comete actos delictivos sin sufrir ninguna de las patologías anteriormente citadas. Realmente las características del delito suelen ser las mismas que el en caso de los cometidos por los psicodelincuentes, sin embargo, la motivación es diferente, ya que en este caso rige el beneficio económico por encima de cualquier otro.

Ciberdelincuente oportunista: ciber-ventajista

El ciber-ventajista responde a una persona ambiciosa y sin escrúpulos. Normalmente encuentra en el delito una forma de enriquecerse. Son personas que llevan una vida normal pero en un momento determinado llevados por su afán de hacer dinero fácil ven en el delito una forma de aumentar sus ingresos.

Este tipo de delincuentes medirán muy bien las consecuencias de su delito, analizarán pros y contras y posteriormente ejecutarán el ataque.

En sus intenciones no hay una intencionalidad de continuar una carrera delictiva, si bien tampoco rechazarán ninguna oportunidad que consideren viable para la comisión del delito.

Los domainer forman parte de este grupo de ciberdelincuentes. Buscan la posibilidad de enriquecerse a través de la compra de dominios que prevén puedan convertirse en dominios muy demandados, tal es el caso de lo ocurrido tras la muerte de la cantante Amy WhiteHouse.

Ciberdelincuente Común: ciber-pandillero

La ciberdelincuencia común podría ser comparada con los delitos menores que se comenten en un entorno no digitalizado: robos de coches, carteristas o pequeños hurtos.

En líneas generales, el ciberdelincuente no busca nuevas experiencias, ni sensaciones y tampoco el reconocimiento social. Tampoco se puede hablar de una psicopatología.

Normalmente son jóvenes que buscan un beneficio económico a corto plazo a través de un medio que les resulta muy familiar. Pueden actuar en solitario o en grupo, sin embargo, aunque a veces no actúen de forma individual, en ningún caso se puede hablar de crimen organizado.

Los ciberpandilleros podrán abandonar la ciberdelincuencia, siendo su carrera delictiva el resultado de la suma de actos vandálicos en la red de forma aislada, o en su defecto, también es posible que consoliden esta carrera convirtiéndose en delincuentes habituales.

Normalmente se inician a edades muy tempranas y si hace unos años se identificaban con personas en estado de marginalidad o exclusión social, actualmente, se asiste a un incremento de este tipo delitos en adolescentes que provienen de entornos estructurados. Más si se hace referencia al ciberpandillero, quien debe tener acceso a determinados conocimientos informáticos así como a equipos que les permitan la comisión del delito.

Ciberdelincuente habitual: ciber-neoprofesional, ciber-profesional y ciber-a-sueldo

El ciberdelincuente-neoprofesional

Este ciberdelincuente supone un paso adelante desde la ciberdelincuencia común para llegar a la ciberdelincuencia profesional,

convirtiendo el delito es una forma de vida. Normalmente el ciberdelincuente-neoprofesional responderá al siguiente perfil:

— Conocimientos de programación limitados.

— Confía en los kits de herramientas para llevar a cabo sus ataques.

— Pueden causar daños a los sistemas, ya que no entienden cómo funciona el ataque.

—Buscan atención de los medios.

El ciberdelincuente profesional y el ciberdelincuente a sueldo

La diferencia fundamental entre ambas categorías de ciberdelincuentes es que el primero comete el delito en beneficio propio, mientras que el segundo es contratado por un segundo cobrando por sus servicios.

En ambos casos hablamos de dos perfiles de sujetos que han convertido el ciberdelito en su modo de vida, especializándose en esta categoría, e iniciando una carrera criminal.

Los **agentes especiales** podrían ser considerados ciberdelincuentes a sueldo. Venden y trafican con sus servicios y únicamente buscan un beneficio económico. Tienen, además, una expensa carrera criminal. Estos sujetos poseen un alto grado de especialización tecnológica.

Otro ejemplo serían **los traficantes de armas** ya que su cometido principal, como si de un trabajo se tratara, es el desarrollo e intercambio con otros ciberdelincuentes de herramientas de hackeo. Se les considera dentro de la comunidad hacker, sin embargo, ellos no se consideran dentro ya que solo hacen negocios y su único interés es el económico.

Por otro lado, el perfil de un **banquero** coincidiría con el perfil de un ciberdelincuente profesional. Utilizan la información robada de forma física en cajeros para duplicar tarjetas, como mecanismo de soborno o directamente como robos de identidad dentro de la web.

Su fin último es el de lucrarse económicamente, es por esto que se les clasificaría como ciberdelincuentes habituales profesionales. Utilizan la información robada y trafican con ella de forma que hacen este trabajo diariamente y reciben pagos de los intercambios o los robos como si fueran sueldos por trabajos realizados.

4.3. PERFIL DEL CIBERDELINCUENTE EN LA EMPRESA: NIVEL DE ESPECIALIZACIÓN Y PSICOPATOLOGÍAS

Se identifican dos tipos de ciberdelincuentes en el ámbito empresarial, aquellos que atentan desde dentro de la organización y aquellos que atentan desde fuera, pudiendo encontrarse una combinación de ambos.

En el primer caso se hará referencia al ciberdelincuente *insider* y en el segundo al ciberdelincuente *outsider*.

4.3.1. El ciberdelito desde dentro de la empresa: el ciberdelincuente insider

El ciberdelincuente *insider* es aquel sujeto que actúa desde dentro de la empresa formando parte de la estructura de la misma.

En este sentido, es importante que las empresas comiencen a ser conscientes de que los ciberataques pueden provenir de dentro de la organización, es decir, que los propios empleados pueden ser aquellos que agredan a la compañía.

Igualmente, es importante que se den cuenta que para que un empleado se convierta en un *insider* son muchas las ocasiones en las que no hacen falta unos conocimientos avanzados, puesto que solo necesitan saber diferenciar entre los archivos que les interesen o que puedan usar y el método que van a emplear para la sustracción de datos ya sea por USB, email u otras técnicas.

Andrés Galindo, director de Negocios de Digiware, describe siete características que sirven para identificar a un ciberdelincuente *insider*:

1. Es un individuo que posee conocimientos de informática y redes de nivel medio o alto.
2. Tienen conocimientos informáticos por encima del promedio como por ejemplo, saben realizar cambios de IP, usan *keyloggers*, etc.
3. Instalan programas espía sin autorización.
4. Desactivan el antivirus de su equipo de trabajo.
5. Muestran interés por datos de clientes u otro tipo de información restringida.
6. Usan otras terminales o dispositivos de los demás miembros de la empresa sin permiso.
7. Suelen ser empleados que se quedan a trabajar en la oficina fuera del horario laboral sin dar justificación alguna.

Otro dato importante es que las principales fuentes de ciberataques a las empresas son llevadas a cabo no solo por los actuales empleados de la organización, también por los antiguos empleados que ya no forman parte de la compañía.

Al respecto, y según un estudio publicado en el Manual de las Naciones Unidas en la Prevención y Control de Delitos Informáticos (Nº 43 y Nº 44), el 90% de los ciberdelitos ejecutados en la empresa fueron realizados por empleados de la propia compañía afectada.

4.3.2. El ciberdelito desde fuera de la empresa: el ciberdelincuente outsider

El sujeto que actúa desde fuera de la empresa se conceptúa como *outsider*, pudiendo responder a un nivel alto de especialización o no y a un perfil psicopatológico o normalizado.

Normalmente estos sujetos actuarán motivados por el beneficio económico, sin embargo existe un grueso de ellos cuyas motivaciones atienden a un ánimo de venganza que estará condicionado, en muchos casos, por la creencia de que la organización tiene algo en contra de él. En este caso concreto hablaremos de un ciberdelincuente-psicótico (ciber-enajenado).

Otra posibilidad es que un *outsider* contacte con un *insider* para colaborar en la perpetuación del ciberataque. En esta ocasión, el perfil del insider puede coincidir con el de un ciberdelincuente-neurótico (ciber-manipulable), mientras que la figura del outsider podrá ser la de un normo-ciberdelincuente (ciber-profesional).

El Instituto Nacional de Investigación ha fijado, en cinco pasos, el procedimiento que siguen los ciberdelincuentes cuando se disponen a atacar a una empresa cuando no forma parte de su estructura interna:

1. Obtención de información

El primer paso trata de obtener toda la información posible acerca de la empresa que pueda resultar interesante o de utilidad para el ataque. Puede tratarse de información personal, como los nombres de los empleados, sus números de teléfono o sus cuentas en las redes sociales, pero también puede obtener una información más técnica como el dominio de la empresa o la dirección IP a través de la cual podrá acceder a la empresa.

Es por ello que es tan importante concienciar al personal para prevenir cualquier infección o que sean plenamente conscientes de que síntomas se pueden presentar si se está infectado.

2. Escaneo de sistemas

Una vez que se conocen los datos técnicos, podrá detectar los puertos abiertos, analizando los servidores de fichero o los sistemas operativos que se estén ejecutando. Para ello, el ciberdelincuente realizará análisis a IP concretas para calcular la vulnerabilidad de las mismas.

Se recomiendo tener todos los softwares actualizados, de manera que se pueda evitar todo lo posible que se lleven a cabo estas acciones.

3. Acceso remoto

Tras haber realizado los pasos anteriores, el ciberdelincuente posee la información necesaria para encontrar las vulnerabilidades del sistema que sea haya detectado anteriormente y poder acceder remotamente al sistema aprovechando los fallos de seguridad. Este tipo de ataques intentarán pasar desapercibidos y se realizarán de la manera más silenciosa posible para que no se puedan tomar contramedidas.

Para evitar las conexiones remotas se recomienda, al igual que en el paso anterior, establecer una política de actualización de aplicaciones y sistemas de manera continuada.

4. Mantener el acceso

Una vez que se accede al sistema, el ciberdelincuente abrirá las denominadas «puertas traseras» a través de las cuales podrá mantener el acceso, de manera que si se detectara el ataque y se cerrara

el acceso remoto, el atacante aún podrá acceder a los sistemas a través de las vías a las que se ha dado acceso.

Esto se puede evitar usando un software que solo permita realizar este tipo de tareas a un administrador y que los empleados no trabajen en su equipo con permisos de administrador.

5. Borrado de huellas

Habiendo establecido un acceso al sistema, el atacante procederá a eliminar cualquier rastro de su actividad para pasar desapercibido y no ser detectado, de manera que no se tomarían medidas contra él.

Estableciendo un perfil de administrador que no fuera usado por el empleado, se evitaría la eliminación de datos puesto que el ciberdelincuente tendría los mismos permisos que el empleado. También se recomienda centralizar los registros de actividad en un solo servidor de forma que se pueda detectar a qué información ha accedido el atacante.

Existen otros métodos a través los cuales se atacan a las empresas, un ejemplo de ello sería lo que se conoce como «la estafa del CEO». En este caso se hace uso del correo corporativo, a través del cual el ciberdelincuente suplante la identidad del consejero delegado de la empresa u otro puesto directivo de la compañía y ordena a un empleado que transfiera una cantidad de dinero a una cuenta bancaria del extranjero pero cuando la empresa se da cuenta de que ha sido estafada, es demasiado tarde y se ha perdido el rastro del dinero. Según un informe facilitado por el FBI, en 2016 se han estafado más de 2000 millones de euros siguiendo este método. El fraude cibernético afecta tanto a grandes como pequeñas empresas.

4.4. CONCLUSIONES

Atendiendo a los diferentes perfiles definidos y a modo de conclusión se describe al ciberdelincuente empresarial de la siguiente forma:

«*Sujeto joven, sin antecedentes penales y sexo masculino mayoritariamente. Inteligente, socialmente aceptado y con un nivel medio, medio-alto de especialización tecnológica. Muchos de estos individuos son autodidactas y aunque actúan bajo motivaciones económicas, suelen crecerse ante aquellos ataques que les suponen un reto. Por otro lado, y si bien es cierto que existe la ciberdelincuencia organizada, el ciberdelincuente empresarial suele actuar de forma individual y dentro de la estructura de la organización se le conceptúa como personas muy trabajadoras*».

Teniendo en cuenta la personalidad del mismo, se puede establecer una dicotomía en función de si el comportamiento del ciberdelincuente empresarial está determinado por algún trastorno psicopatológico o no.

En el primer caso se haría referencia al psico-ciberdelincuente y en el segundo al normo-ciberdelincuente.

El psico-ciberdelincuente empresarial responde al perfil de un sujeto que sufre algún tipo de trastorno de la personalidad (psicopatía, neurosis, psicosis o trastorno de la personalidad antisocial). Estos individuos no tienen un patrón de comportamiento único, aunque en líneas generales podría afirmarse que:

— Los neróticos son introvertidos y más sensibles que los extrovertidos a presiones externas. Normalmente sus habilidades sociales no son muy sofisticadas.

— Los sociópatas (trastornos de la personalidad antisocial) apenas tienen tolerancia a la frustración y generan actitudes negativas a todo lo que les venga impuesto. Tienen un historial de problemas en los primeros años de vida asociados a los

grupos de socialización primarios (familia y escuela). Prefieren el carácter predecible de los ordenadores a las relaciones personales. De tal manera que muchos de ellos reemplazan sus interacciones profesionales o sociales directas y «crean» su propia personalidad online.

— Los psicópatas se caracterizarán por la falta de ética, remordimientos y empatía hacia la víctima. Pueden incluso llegar a justificar el delito pensando que la culpa es del propio sistema por no estar correctamente protegido. Cuando el ciberdelito es cometido por un *insider* (desde dentro de la organización) no desarrollan ningún tipo de lealtad hacia la empresa de la que forman parte.

— Los psicóticos serán aquellos sujetos que sienten que tienen derecho a realizar este tipo de ataques. Sienten que las organizaciones que atacan son merecedoras de las consecuencias del delito pudiendo fundamentar este tipo de justificación en delirios o incluso en alucinaciones.

Por otro lado, las conclusiones alcanzadas también permiten diferenciar entre el ciberdelincuente con un alto nivel de especialización o un nivel bajo de conocimiento. Igualmente se diferencia entre aquellos sujetos que actúan desde dentro de la empresa (*insiders*) y los que actúan desde fuera (*outsiders*).

4.5. BIBLIOGRAFÍA

Agnew, R. (2006). General Strain Theory: Current Status and Directions for Further Researches. En Cullen, F.T., Wright, J.P., & Blevins, K.R. (Eds.) *Taking stock: The Status of Criminological Theory* (P.121-123). New Brunswick, NJ: Transaction Publishers.

Cleckley, H. (1976): *The Mask of Sanity*. St. Louis, MO: Mosby. 5th ed.

Control.Capital (2014): Delincuente prêt à porter, un perfil criminal para la nueva delincuencia económico financiera. http://www.controlcapital.

net/noticia/3041/firmas/delincuente-prt—porter-un-perfil-criminal-para-la-nueva-delincuencia-economico-financiera.html (Consultado el 22 de marzo de 2017)

Malatesta, J. (2008): *Exploring the Effects of the Internet Environment on Online Sexual Deviance*. (Tesis doctoral). ProQuest: State University of New York (Albany).

García de Pablos Molina, P. (2003): *Tratado de Criminología*. Tirant Lo Blanch (Madrid)

Garrido, V. (2005). Qué es la Psicología Criminológica. Editorial Biblioteca Nueva (Madrid).

Garrido, V. (2000): *El psicópata*. Editorial Algar. 4ª edición.

Gottfredson, M. R. y Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Hare, R.D. (2008): «An Overview of Psychopathy». Ponencia presentada en las Jornadas Sobre Prevención del Delito a Partir de la Detecciоón del Riesgo. Facultad de Psicología, Universidad de Santiago de Compostela, 20 de noviembre de 2008.

Hare, R.D. (2003): *Sin Conciencia: El Inquietante Mundo de los Psicópatas que nos Rodean*. Barcelona: Ediciones Paidos.

Hirschi T. (1969): *Causes of Delinquency*. University of California Press.

Marchiori (1975): Psicopatología criminal. Universidad de Texas. Porrúa.

Molto, J. y Poy, R. (1997): *La psicopatia: Un constructo necesario en la Psicologia Juridica.* En M. Clemente y J. Nunez (Eds.), Psicologia juridica penitenciaria (Vol. II) (pp. 291-317). Madrid: Fundacion Universidad-Empresa.

Mora, F. (2004). *¿Cómo Funciona el Cerebro?* Alianza Ensayo (Madrid).

Muñoz, E. (2010): Enfermedad mental y delincuencia. Psicología Jurídica. http://psicologiajuridica.org/psj278.html

Pozueco J.M., Romero S.L. y Casas N. (2011a): Psicopatía, violencia y criminalidad: un análisis psicológico-forense, psiquiátrico-legal y criminológico (Parte I). *Cuadernos de Medicina Forense*. Vol. 17, no.3. (http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1135-76062011000300004)

Pozueco J.M., Romero S.L. y Casas N. (2011b): Psicopatía, violencia y criminalidad: un análisis psicológico-forense, psiquiátrico-legal y criminológico (Parte II). *Cuadernos de Medicina Forense*. Vol. 17, no.4.
(http://dx.doi.org/10.4321/S1135-76062011000400002)

Pueyo, A. (2007): Evaluación del riesgo de violencia. Publicado en http://www.ub.edu/geav/contenidos/vinculos/publicaciones/public1_6/publicac_pdf/1_8%20Andr%C3%A9s%20Pueyo,%20A%20(2007).pdf (Consultado el 21 de enero de 2016).

Quejido (2016): Trastornos de la personalidad y tipología delictiva (I). Publicado en http://www.centta.es/sin-categoria/trastornos-de-la-personalidad-y-tipologia-delictiva-i (Consultado el 13 de marzo de 2017)

Velasco de la Fuente, P. (2016): Internet como escenario para nuevos delincuentes: los «neópatas». Publicado en http://criminal-mente.es/2016/05/09/internet-como-escenario-para-nuevos-delincuentes-los-neopatas/ (Consultado el 14 de marzo de 2016).

Vic, G. (2016): Delincuentes habituales. Publicado en http://www.academia.edu/7509821/DELINCUENTES_HABITUALES (Consultado el 12 de marzo de 2016).

Wortley, R. y Smallbone, S. (2006): Situational Prevention of Child Sexual Abuse. Criminal Justice Press.

5 ANÁLISIS DE LA PERSPECTIVA EMPRESARIAL SOBRE EL CIBERDELITO EN ESPAÑA: ENFOQUE CUALITATIVO

Introducción

Las técnicas de análisis cualitativo tienen cada vez más importancia en el ámbito de las ciencias sociales (Caceres, 2003).

La mayoría de los métodos de investigación cualitativa se fundamentan en la experiencia y el juicio de individuos expertos en el área que se estudia. De esta forma la investigación cualitativa no se interesa por la estimación de los valores concretos que una variable pueda tomar, sino más bien en la determinación de los límites o rangos de variación en los que se puede encontrar.

El presente análisis cualitativo se plantea con el objetivo de identificar el rango completo de posibilidades que deben ser investigadas y obtener una visión más completa y exhaustiva del fenómeno investigado. Como consecuencia se plantea un estudio con una perspectiva más amplia de lo que significa el ciberdelito en las empresas españolas.

5.1. TÉCNICAS DE INVESTIGACIÓN CUALITATIVA

En la investigación cualitativa existen diferentes técnicas de recogida de datos. En este caso y con el objeto de conocer la realidad desde la perspectiva de las empresas españolas se ha considerado como técnica de análisis cualitativo más adecuada la entrevista personal. Esta técnica permite describir e interpretar aspectos de la realidad que no son directamente observables, tales como los sentimientos, impresiones, emociones, intenciones o pensamientos de las personas entrevistadas (Del Rincón *et al.*, 1995).

Con este planteamiento Folgueiras (2009) define la **entrevista personal** como una técnica orientada a obtener información de forma directa y personalizada, sobre acontecimientos vividos y aspectos subjetivos de los informantes, con respecto a la situación que se está estudiando.

La entrevista personal es un método de análisis cualitativo diseñado fundamentalmente para obtener información de un número limitado de entrevistados, más que para obtener resultados estadísticos de una muestra amplia. Se distinguen **diferentes categorías de entrevista personal** (Blasco *et al.*, 2008):

— **Entrevista estructurada.** Consiste en proporcionar cuestionarios estructurados, que incluyen preguntas predeterminadas tanto en su secuencia como en su formulación. Es decir, el entrevistador formula, en la mayoría de los casos, un número fijo de preguntas de forma estándar y en el mismo orden. Las respuestas pueden estar prefijadas de antemano.

— **Entrevista semiestructurada.** Al igual que las entrevistas estructuradas en las entrevistas semiestructuradas las preguntas están definidas previamente en un guión, pero la secuencia así como su formulación pueden variar en función de cada sujeto entrevistado. El investigador realiza una serie de preguntas generalmente abiertas al principio de la entrevista, que definen el área a investigar, pero tiene libertad para profundizar en alguna idea que pueda ser relevante, realizando nuevas preguntas.

— **Entrevista en profundidad.** Generalmente suele cubrir solamente uno o dos temas pero con mayor profundidad. Las preguntas que el investigador realiza van emergiendo de las respuestas del entrevistado y se centran fundamentalmente en la aclaración de los detalles, con la finalidad de profundizar en el tema objeto de estudio.

Para la realización de esta investigación se ha utilizado la **entrevista estructurada**. En concreto se han formulado un total de ocho preguntas abiertas siguiendo un orden preestablecido en función de los objetivos que se pretenden alcanzar. Los entrevistados han tenido plena libertad para manifestar sus respuestas, si bien el hecho de plantear las mismas preguntas en el mismo orden a todos los participantes introduce un fuerte elemento de rigidez en la dinámica de la entrevista.

La utilización de una entrevista estructurada combinada con la elaboración de un cuestionario abierto responde a tres motivos fundamentales:

1. **La singularidad de las situaciones.** La perspectiva del ciberdelito del empresario español dependerá no solo de sus preferencias o motivaciones personales sino también del tamaño de su empresa o de si ha sufrido algún ciberataque previo.
2. **La variedad de respuestas posibles.** La imprevisibilidad de las respuestas ante preguntas generalistas así como la imposibilidad de sintetizarlas en pocas palabras, dificulta el hecho de definir con precisión todas las alterna vas de respuesta posibles.
3. **El fin de la entrevista.** Es importante que los entrevistados formulen sus propias respuestas y no escojan estrategias predeterminadas por los investigadores, como ocurre con las encuestas personales.

Las preguntas se organizaron de acuerdo con los siguientes ámbitos de análisis:

1. Conocimiento de la evolución del ciberdelito empresarial en España.
2. Conocimiento de los tipos de ciberdelitos más frecuentes.
3. Conocimiento de los perfiles de ciberdelincuentes empresariales.
4. Comportamiento y protocolos de actuación ante el ciberdelito: prevención.

5.2. DISEÑO DE LA INVESTIGACIÓN

La fase cualitativa de esta investigación incluye 20 entrevistas personales. Dada su naturaleza se ha establecido un único perfil básico en el diseño de la investigación. Este perfil se define como directivos de empresas, gerentes y propietarios que son susceptibles de sufrir un ciberataque dado el volumen de datos que manejan.

En líneas generales se puede afirmar que la investigación cualitativa emplea muestras elegidas intencionalmente atendiendo a dos cuestiones fundamentales, ¿quién tiene mayor conocimiento del tema objeto de investigación? y ¿en que contexto se puede obtener la información más objetiva sobre el hecho investigado?

Para abordar estas cuestiones se han tomado en consideración las siguientes variables (1) número de empleados y (2) categoría profesional del entrevistado.

El conjunto de las 20 entrevistas se realizaron entre el 01 de marzo de 2017 y el 15 de marzo del mismo año.

5.3. SELECCIÓN DE LOS PARTICIPANTES Y ENTREVISTAS

Una vez definido el perfil básico de los participantes para la selección de los entrevistados y con el objeto de dar mayor fiabilidad a los resultados se estableció una única condición. En concreto se exigió que la experiencia laboral de los entrevistados en fuera igual o superior a cinco años en un puesto de dirección. Esta condición viene definida porque la experiencia otorga una visión más amplia y objetiva sobre el tema de estudio.

Para la captación de los participantes se elaboró un listado de posibles entrevistados. Con este objetivo se realizó un contacto previo mediante los siguientes medios:

— Redes sociales como Linkedin y Facebook

— Contactos personales de los investigadores

Este primer contacto obtuvo un total de 38 respuestas de empresarios interesados en participar en la investigación. Finalmente un total de 20 se ajustaban al perfil requerido.

Seguidamente se estableció contacto con los 20 entrevistados que respondían al perfil definido con el objeto de explicarles exhaustivamente la naturaleza de la investigación así como las características de la entrevista. En la mayoría de los casos el contacto se realizó vía email, aunque un total de 9 casos necesitaron contacto telefónico. La entrevista fue realizada mediante teléfono o personalmente.

5.4. ANÁLISIS DE LA INFORMACIÓN

El análisis de datos cualitativos es el proceso mediante el cual se organiza e interpreta la información recogida por los investigadores para establecer relaciones, interpretar y extraer conclusiones (Rodríguez *et al.*, 2005).

En este caso el proceso de análisis de la información se centró en transcribir, revisar y analizar la información recogida, con el objeto de elaborar un argumento explicativo la visión del ciberataque del empresario español, de acuerdo con los ámbitos de estudio definidos anteriormente.

La labor de revisión consistió en filtrar y eliminar aquellas respuestas cuya información no resultaba relevante por caracterizarse por un contenido ambiguo y sin interés para la investigación.

En el análisis de los datos obtenidos se conservó su naturaleza textual, obteniendo los resultados a partir de los códigos asignados a los diferentes ámbitos de análisis.

Siguiendo a Rubin y Rubin (1995) el **proceso de codificación** consiste en agrupar la información obtenida en categorías que concentran las ideas, conceptos o temas similares descubiertos por el investigador.

El proceso de codificación se realizó manualmente por los investigadores. Este hecho no comprometió el resultado final del análisis ya que aunque los programas de *software* para el análisis de datos cualitativos ofrecen diferentes herramientas y formatos para codificar, los principios del proceso analítico son los mismos, tanto si se hace manualmente o se utiliza un programa informático (Patton, 2002).

Existen varios métodos para crear códigos, en este caso se creó una lista inicial de códigos previa. Esta lista se elaboró antes de realizar el trabajo de campo teniendo en cuenta las preguntas de la investigación.

5.5. RESULTADOS

Los resultados obtenidos son los siguientes:

1. Conocimiento sobre el ciberdelito

La mayor parte de las empresas entrevistadas, tienen constancia del aumento del ciberdelito en la empresa en los últimos años. Concretamente 13 de ellas admiten haber consultado información acerca de los ciberataques en los últimos tres meses.

Atendiendo al número de empleados dentro de la empresa, la mayoría de los entrevistados que han afirmado estar informados sobre la evolución del ciberataque contra las organizaciones, pertenecen a pequeñas empresas.

En cuanto al cargo que ocupaban los mismos, los altos cargos están al tanto de que existe un aumento del riesgo dentro de la empresa dado el incremento progresivo del ciberdelito, mientras que los mandos intermedios se mantienen al margen.

Por otro lado resulta llamativo que las personas que no han consultado información, reconozcan en los ciberataques una amenaza

contra la empresa, tal y como queda de manifiesto en las siguientes afirmaciones:

> «He escuchado en los últimos meses dicho aumento en los medios de comunicación, pero en la empresa no tenemos noticias».

> «Tengo constancia de un aumento del ciberataque contra las empresas pero no he consultado».

Igualmente, llama la atención que los entrevistados que si se mantienen informados sean conscientes de que este tipo delitos suponen una amenaza constante debido a los grandes avances tecnológicos. Esta afirmación puede constatarse a través de las siguientes respuestas:

> «Aunque las medidas de seguridad que se adoptan son cada vez más sofisticadas aparecen todos los días nuevas técnicas delictivas que las vulneran».

> «La alta especialización de los empleados y sus conocimientos informáticos, unidos a los avances tecnológicos, potencian el incremento de los ciberataques».

2. Adopción de medidas de seguridad contra el ciberdelito

La mayoría de los entrevistados sí adopta alguna medida contra el ciberdelito, siendo las más comunes el uso de firewall (cortafuegos) y antivirus, así como no abrir E-Mails desconocidos.

En este sentido, es importante señalar que un grupo minoritario de los encuestados delega la responsabilidad de la seguridad en terceras partes, confiando en que lleven de manera correcta la seguridad de la empresa.

Atendiendo al tamaño de la empresa, se puede afirmar que, en general, las PYMES no toman medidas de seguridad básicas contra el ciberdelito.

Por otro lado, en cuanto al cargo ocupado, se puede extraer que altos cargos han respondido que sí, no, o no están seguros, pero

sin indicar en su gran mayoría qué medidas adoptan, por lo que puede existir un desconocimiento. En cambio, puestos con un nivel jerárquico inferior sí han nombrado algunas medidas, aunque éstas sean insuficientes.

3. Conocimiento de ciberataques contra la empresa específicos

Los ciberdelitos más conocidos son el phishing, el robo de identidad y la privacidad y, por último, el hacking.

La respuesta obtenida es sorprendente, puesto que el hacking es la acción de *hackear* pero no siempre es considerado un delito, tal y como, se expuso en el capítulo 4 sobre el perfil del ciberdelincuente y su nivel de conocimiento informático.

Es igualmente llamativo que el phising sea la técnica más conocida.

Por otro lado no se aprecian diferencias significativas entre las respuestas de los mandos intermedios y de los mandos superiores de las empresas entrevistadas.

4. Protección de los equipos con softwares específicos

La mayor parte de los entrevistados ha respondido que si protege sus equipos informáticos con softwares específicos. Sin embargo, las medidas adoptadas se corresponden con niveles de seguridad muy básicos. Esta afirmación queda patente en algunas respuestas como las siguientes:

«Protejo mis equipos con los antivirus profesionales»

«El antivirus gratuito de Windows es suficiente»

«Los antivirus corporativos y … nada más»

Un dato a tener en cuenta es que los usuarios de Apple sienten que no tienen por qué defenderse de posibles ataques:

«Protejo mis equipos Windows, pero no los Mac»

«Todos nuestro equipos son Apple y esto asegura que no haya virus en ellos»

5. Protección de la empresa frente a sus empleados

A la pregunta sobre si tienen conciencia acerca de ataques informáticos realizados por los empleados con el fin de dañar los intereses de la empresa, gran parte de los entrevistados ha contestado que sí.

Pese a los resultados expuestos, muchos de ellos tienen plena confianza en sus empleados, tal y como se puede comprobar en las siguientes respuestas:

«No pienso que mis empleados puedan atacarme, pero soy consciente de que ha ocurrido en otras compañías y que hay que tomar medidas preventivas»

«No necesito protección frente a mis trabajadores. Al menos con mi plantilla actual»

«Confío en la buena fe de mis empleados»

6. Controles de seguridad

A pesar de la respuesta obtenida en la pregunta 5, la mayor parte de los entrevistados sí considera que realiza controles de seguridad a sus trabajadores, siendo la medida más común la restricción de acceso a webs externas a la empresa, así como redes sociales personales, llevándose, además, un registro del historial de los trabajadores.

En cuanto al número de trabajadores, las empresas pequeñas no acostumbran a poseer controles de seguridad más allá de no permitir el acceso a determinadas webs, ya que suelen ser empresas familiares o formadas por socios y confían en ellos, tal y como se puede comprobar en las siguientes respuestas:

«Las redes sociales, es donde está el peligro»

«Limitarles el acceso a redes sociales es suficiente»

En cambio, las medianas empresas sí realizan algún tipo de control, aunque sólo sea el registro del historial de navegación web.

7. La figura del Hacker

La mayoría de los entrevistados no contrataría a un *hacker* en su empresa, ya que asocian la figura del hacker a actividades ilegales y éticamente inmorales, tal como queda demostrado en las siguientes afirmaciones:

«No lo contrataría por razones puramente éticas y morales»

«No, ya que invaden la privacidad y los recursos de información sin autorización»

«No somos una empresa que se pueda beneficiar de esos servicios e información»

«Es ilegal y me parece que sería un delito»

«No, ya que no hace falta invadir la privacidad de alguien»

Por otro lado, los encuestados cuya respuesta ha sido afirmativa a la contratación de un hacker, lo harían por sus conocimientos, ya que ayudarían a la empresa en calidad de prevención y protección.

8. La seguridad condicionada al tamaño de la empresa

De forma unánime, los encuestados consideran que el tamaño de la empresa sí afecta a la visión del delito, considerando más susceptibles de ser atacadas las empresas de mayor tamaño, llegando a afirmar que las micropymes no se sitúan en el punto de mira de los ciberdelincuentes.

5.6. ANÁLISIS DE LOS RESULTADOS Y CONCLUSIONES

1. Consulta de información sobre el ciberdelito empresarial

Las respuestas obtenidas en la pregunta 1 arrojan los siguientes resultados:

— Las empresas entrevistadas tienen constancia del ciberdelito y del aumento de la actividad delictiva en la empresa.

— Aun así no se informan acerca de los peligros a los que están expuestos, aunque le parezca un tema preocupante.

2. Adopción de medidas de seguridad contra el ciberdelito

En lo que respecta a la adopción de medidas, las respuestas obtenidas permiten concluir que:

— Actualmente las empresas no adoptan medidas de seguridad específicas en materia de ciberdelito.

— Las medidas más populares son el *firewall* y los antivirus.

— El tamaño de la empresa está relacionado con las medidas adoptadas, siendo las PYMES las que menos percepción de peligro tienen.

— Igualmente, son los mandos intermedios de la empresa los que sienten la desprotección.

3. Conocimiento de ciberataques contra la empresa específicos

Los ciberdelitos más concocidos son el phishing, el robo de identidad y la privacidad y, por último, el hacking.

La respuesta obtenida es sorprendente, puesto que el hacking es la acción de hackear pero no siempre es considerado un delito, tal y

como, se expuso en el capítulo 4 sobre el perfil del ciberdelincuente y su nivel de conocimiento informático.

Es igualmente llamativo que el phishing sea la técnica más conocida.

Por otro lado no se aprecian diferencias significativas entre las respuestas de los mandos intermedios y de los mandos superiores de las empresas entrevistadas.

4. Protección de los equipos con softwares específicos

Tras el análisis de las respuestas obtenidas al respecto de la protección de los equipos informáticos las conclusiones alcanzadas son las siguientes:

— Los virus se reconocen como las principales amenazas en el ciberespacio, por lo que la prevención en la empresa pasa principalmente por la instalación de un antivirus profesional en el mejor de los casos y en el peor por la descarga de un antivirus gratuito de Internet.

— La percepción de Apple como invulnerable ante los ciberataques conlleva la no protección de los equipos.

— En ningún caso se contempla la posibilidad de proteger otro dispositivos como las impresoras o las cámaras de seguridad (Internet de las Cosas).

5 y 6. Protección de la empresa frente a sus empleados y controles de seguridad

El análisis de las respuestas a las preguntas 6 y7 arroja los siguientes resultados:

— Las empresas, en líneas generales son conscientes de que pueden ser atacadas por sus empleados, sin embargo, confían plenamente en sus trabajadores.

— Este resultado confirma los resultados obtenidos en la pregunta número 6, donde los entrevistados dejan de manifiesto que no adoptan ningún tipo de control salvo el relacionado con las restricciones de navegación o el registro de navegación.

7. La figura del Hacker

La pregunta 7 pone de manifiesto el desconocimiento de los conceptos relacionados con el ciberataque, puesto que en la mayoría de los casos la figura del hacker se relaciona con la de un ciberdelincuente.

8. La seguridad condicionada al tamaño de la empresa

Por último resulta llamativo que las empresas entrevistadas relaciones el ciberdelito con el tamaño de la empresa. Esto condiciona la seguridad de las PYMES españolas, donde no existe la percepción de peligro y, y por tanto, no existe la prevención ni el control.

5.7. BIBLIOGRAFÍA

BLASCO HERNANDE , T. y OTERO GARC A, L. (2008): Tecnicas conversacionales para la recogida de datos en investigación cualitativa: la entrevista (1), Nure Investigacion, nº 33, (version online).

CACERES, P. (2003): «Analisis cualitativo de contenido: una alternativa metodologica alcanzable», Revista de la Escuela de Psicologia, Facultad de Filosofía y Educacion Pontificia, Universidad Catolica de Valparaiso, Vol. II, pp. 53-82.

DEL RINCÓN, D., ARNAL, J., LA TORRE, A. y SANS, A. (1995): *Técnicas de investigación en Ciencias Sociales*, Madrid, Dyckinson.

PATTON, M. Q. (2002): *Qualitative Research and Evaluation Methods* (3a ed.). Thousand Oaks, Sage Publications.

RODRÍGUEZ , C., LORENZO, O. y HERRERA, L. (2005): «Teoria y Practica del analisis de datos cualitativos. Proceso general y criterios

de calidad», Revista Internacional de Ciencias Sociales y Humanidades , Vol. 15 (2), pp.133-154.

RUBIN, H.J. y RUBIN, I.S. (1995): *Qualitative interviewwing. The art of hearing data*. Thousand Oaks, Sage Publications.

ANEXO 1

Tabla 1. Herramientas del ciberataque

	Descripción	Síntomas	Riesgos	Métodos de prevención
Troyano	Un tipo de virus que aparenta ser un software de ayuda o divertido para pasar inadvertido pero que en realidad está provocando daños o el robo de datos.	Aquellos terminales que se encuentren infectados por troyanos mostrarán algunas señales como que aparezcan o desparezcan archivos, que se ejecuten o se cierren programas sin razón alguna o que algunos periféricos dejen de funcionar. Estos son algunos de los muchos síntomas de un sistema infectado.	Su propósito principal es dar acceso remoto a un sistema al ciberdelincuente para que pueda usar otro tipo de software como un keylogger para registrar las teclas pulsadas y obtener información.	Además de tener todos los software de tu ordenador actualizado, existen otras formas de protegerse de este tipo de ataques como no conectarse a una red Wifi abierta o diferenciar las cuentas de usuario de las cuentas de administrado, en caso de que se infecte la cuenta de usuario, el atacante no tendrá permisos de administrador y no tendrá un acceso completo.
Troyano bancario	Una variedad del troyano que está orientado al robo de datos bancarios.	En general, al igual que el troyano clásico, la existencia de un troyano bancario en un sistema suele reducir la velocidad de este hasta el punto de que puede provocar errores entre los periféricos o algunos software.	Tienen como principal objetivo robar datos privados de las cuentas bancarias de los usuarios. Utilizan diferentes técnicas para obtener los datos de acceso a todo tipo de entidades financieras.	Este tipo de ataques se aprovechan de la ingenuidad de las personas, es por ello que sería primordial la concienciación de los trabajadores y evitar descargarse archivos de páginas web poco fiables.
Rootkit	Están diseñados para proporcionar a los hackers un acceso administrativo a la computadora sin el conocimiento del usuario.	La evidencia de un sistema infectado por un rootkit es más compleja de detectar, es por ello que debería ser un programa antivirus el que detectara archivos ocultos, inicios de sesión ocultas al usuario o datos que se están enviando fuera de la terminal.	Da el control total de la terminal al ciberdelincuente desde el momento en el que se enciende el ordenador y dificulta la detección de otros archivos dañinos que haya en el sistema.	Es necesario un programa que no solo analice los archivos del ordenador, sino que también debe controlarse lo que se hace al ejecutar cada programa.
Keylogger	Un tipo de software usado para registrar todo lo que se escribe en el teclado, de esta forma los ladrones pueden leer cualquier información que se escriba, como contraseñas, tarjetas de crédito, correos electrónicos, etc.	Suelen presentar los comportamientos que comparten la mayoría de los virus informáticos, estos son: un uso excesivo del disco duro o de la red, un enlentecimiento del sistema o algún tipo de retraso en el comportamiento y uso del ordenador.	Quien controla este software puede ver que teclas está pulsando su víctima, de manera que junto a otro tipo de malware puede obtener contraseñas o incluso lograr tener acceso a los datos bancarios del infectado.	Se debe utilizar un antivirus actualizado, evitar acceder a redes Wifi abiertas y no manipular información personal en ordenadores públicos.

Tabla 1. Herramientas del ciberataque *(cont.)*

	Descripción	Síntomas	Riesgos	Métodos de prevención
Gusanos	Se divide de manera similar a las células del cuerpo humano y se propaga a través de las redes de los terminales. Este tipo de malware es capaz de reproducirse a través de algún medio de comunicación como, por ejemplo, el correo electrónico. Todo esto con la finalidad de infectar el mayor número de terminales posibles.	Para poder infectar una terminal con un gusano, primero ha de penetrar el sistema. Para ello se suelen enviar archivos por correo y, cuando se tratan de gusanos informáticos suelen tener una doble extensión pero para poder observar esto, el ordenador debería tener desactivada la función de "ocultar las extensiones del archivo para tipos de archivos conocidos". Una vez infectado, un claro síntoma sería que la disquetera se abra y se cierre continuamente y sin razón aparente.	Se podría decir que el mayor riesgo de un gusano informático es su velocidad de propagación. Infecta un gran número de terminales y, combinado con otras herramientas, puede recabar información o llevar a cabo actividades perjudiciales para la empresa.	Para evitar ser infectado por un gusano es recomendable mantener actualizado el sistema operativo en todo momento al igual que otros softwares que se tengan instalados. También se debe realizar una navegación segura y prudente, tratando de evitar páginas con dudosa reputación y evitar ejecutar archivos sospechosos, esto incluye los archivos adjuntos que recibamos por email.
Botnets	Es el nombre con el que se denomina a un grupo de PC que estén infectados y sean controlados por un atacante de forma remota. Los ordenadores que forman la botnet son los llamados *bots* o *zombies*.	El ordenador vaya más lento de lo normal o que algunas aplicaciones dejen de funcionar son unos de los principales indicadores de que nuestro ordenador puede haber sido infectado y estar siendo usado como lo que se conoce como un ordenador "zombie".	Alguien puede estar usando la terminal de forma remota y puede conseguir datos personales que se guarden en el ordenador, puede ser utilizado para reenviar spam o infectar a otros terminales o incluso puede cometer otro tipo de delitos desde tu ordenador suplantando tu identidad.	Mantener actualizado el sistema operativo y un antivirus y tener unos buenos hábitos de uso son unas de las maneras de evitar ser infectado y convertir tu ordenador en parte de una botnet. También se debe evitar instalar nada que no se haya elegido, pulsar enlaces de emails cuyo remitente desconoces o desconfiar de los chollos que te anuncian por Internet.
Backdoor	Son accesos, desconocidos por el usuario, dejados por el ciberdelincuente para poder acceder al sistema de su víctima en cualquier momento.	No tienen unos síntomas claros, puesto que existen backdoors que han sido instalados a propósito para poder llevar a cabo tareas de mantenimiento o administración de forma remota.	Da un acceso, que normalmente pasa inadvertido, al sistema que el ciberdelicuente puede usar para obtener información sensible de la empresa o llevar a cabo otras acciones perjudiciales entre otras muchas otras actividades que podría llevar a cabo.	Es muy importante eliminar un backdoor por completo para eliminar cualquier posibilidad de fallar al intentar removerlo del sistema. Es recomendable disponer de un programa que realice esta limpieza de forma automática puesto que es muy difícil e improbable lograr eliminar un backdoor por completo de forma manual.

Tabla 1. Herramientas del ciberataque *(cont.)*

	Descripción	Síntomas	Riesgos	Métodos de prevención
Adware	Es un tipo de software gratuito patrocinado mediante publicidad que suele aparecer en ventanas emergentes, o pop-ups. La mayoría de veces el adware es molesto pero seguro, aunque a veces se suele usar para recopilar información personal sin autorización.	Señales de que estamos infectados por un adware serían que nos saltan pop-ups de publicidad continuamente, que nos instalen barras de herramientas o añadan páginas como favoritos en nuestros navegadores.	Aunque no suele representar una gran amenaza, el adware pone la información personal de los usuarios a disposición de quien distribuya o publique el software, además de resultar muy molesto para la persona afectada.	Se pueden eliminar manualmente pero dependiendo del adware, puede resultar demasiado complejo. Por ello, existen programas que automatizan la eliminación de este tipo de software.
Sniffing	En términos generales, el sniffing consiste en la detección o retención de toda la información que circula por una red. Una vez que se obtiene la información, se almacena y se interpreta para poder conseguir datos sensibles como contraseñas, información bancaria o cualquier otra información que pueda ser usada en beneficio del ciberdelincuente. Este método es uno de los principales que se realizan cuando se intenta robar información.	El sniffer entra al pc a través de su instalación y para ello el usuario debe aceptar la instalación. En el caso de que se solicitara la instalación de un archivo sospechoso y se aceptara, existen programas que detectan el sniffer en el sistema o a través de la red.	El atacante obtiene acceso a la información almacenada en el sistema atacado, dejando información personal en manos del ciberdelincuente y podrá usarla de la forma que le plazca.	Es recomendable no hacer uso de una red wifi pública puesto que tal vez se trate de una red fraudulenta que esté esperando a que un usuario se conecte para poder capturar la información. También se debe evitar enviar información sensible a través de la red para no dar la oportunidad de un robo de datos.
Rogueware	El rogueware es una aplicación que intenta parecerse a otra, por apariencia o nombre, para engañar y timar a los usuarios.	Al tratarse de un programa que se hace pasar por otro, simplemente haría falta comprobar si el programa en cuestión está llevando a cabo con su función o que el programa sospechoso está usando más memoria de lo que debería.	Generalmente se utiliza para conseguir dinero pero mediante esta estafa también se puede obtener información.	Este tipo de programas intentan suplantar la identidad de otros softwares, por ello el principal método de prevención sería evitar descargar programas desde páginas no oficiales.

Tabla 1. Herramientas del ciberataque *(cont.)*

	Descripción	Síntomas	Riesgos	Métodos de prevención
Spear phising	Un ataque a una organización específica en la que el phisher simplemente obtiene detalles de un empleado y los utiliza para obtener un acceso más amplio al resto de la red a través de un envío de un email fraudulento u otras medidas.	Un empleado consciente de las amenazas que existen en la red, no tendrá problemas en identificar una acción de spear phising. Esto gira alrededor de la ingeniería social y generalmente suele llevar a cabo sus ataques a través de correos electrónicos. Estos correos llegan a un empleado en concreto con la intención de que se descarguen el archivo adjunto y les permita entrar en el sistema. Es por esto que resulta de suma relevancia el instruir y concienciar a los empleados sobre los riesgos existentes.	El atacante obtiene acceso a la red a la que esté conectado la terminal infectada, pudiendo acceder a toda la información de esa red.	Para prevenir ser atacados de esta manera, los empleados deben ser conscientes de que pueden recibir emails falsos que les pidan información. Algunos especialistas también recomiendan usar un buen gestor de contraseñas.

ANEXO 2

Tabla 2. Técnicas del ciberataque

	Descripción	Síntomas	Riesgos	Métodos de prevención	Principales herramientas utilizadas
Ataque DoS	Un ataque a una organización específica en la que el phisher simplemente obtiene detalles de un empleado y los utiliza para obtener un acceso más amplio al resto de la red a través de un envío de un email fraudulento u otras medidas.	Un empleado consciente de las amenazas que existen en la red, no tendrá problemas en identificar una acción de spear phising. Esto gira alrededor de la ingeniería social y generalmente suele llevar a cabo sus ataques a través de correos electrónicos. Estos correos llegan a un empleado en concreto con la intención de que se descarguen el archivo adjunto y les permita entrar en el sistema. Es por esto que resulta de suma relevancia el instruir y concienciar a los empleados sobre los riesgos existentes.	El atacante obtiene acceso a la red a la que esté conectado la terminal infectada, pudiendo acceder a toda la información de esa red.	Para prevenir ser atacados de esta manera, los empleados deben ser conscientes de que pueden recibir emails falsos que les pidan información. Algunos especialistas también recomiendan usar un buen gestor de contraseñas.	Dado que este tipo de ataque trata de sobrecargar un sistema o una red, la herramienta fundamental sería la botnet, cuanto más ordenadores zombies sobrecarguen el sistema que está siendo atacado, mayor será la efectividad del ataque.
Advanced Persistent Threat (APT)	Se trata de un conjunto de procesos informáticos sigilosos y continuos que involucra técnicas complejas las cuales utilizan softwares maliciosos para explotar vulnerabilidades en los sistemas., dirigidos a traspasar la seguridad de una empresa en concreto. Una APT, suele fijar sus objetivos en organizaciones o naciones por motivos de negocios o políticos.	Una APT es un ataque a gran escala que, dado a su elevado coste, se suele llevar a cabo contra empresas o incluso gobiernos . No tiene unos síntomas predefinidos puesto que cada APT es diferente y trata de pasar desapercibido.	Los riesgos a los que se somete una víctima de APT varían según el ataque dada la caracterización única de cada ataque. En general, cualquier víctima de APT está expuesta a grandes riesgos ya sean de tipo financiero o social.	Es un ataque muy complejo y hará falta un equipo especialista en seguridad para intentar detenerlo.	En cada APT se emplean herramientas distintas dado que cada ataque es único en su género pero todos comparten una característica, y es que no se trata de un simple ataque sino de un conjunto de procesos que dependiendo del atacante, puede emplear unas herramientas u otras.

Tabla 2. Técnicas del ciberataque *(cont)*

	Descripción	Síntomas	Riesgos	Métodos de prevención	Principales herramientas utilizadas
Stealth Virus	Virus que se adjuntan por sí solos a ciertos archivos del ordenador, para atacar y esparcirse rápidamente por todo el equipo. Tienen una gran habilidad para camuflarse y no ser descubiertos.	No se suelen detectar síntomas evidentes puesto que la función principal de esta técnica es el sigilo. Por ello es importante realizar análisis en la terminal cada cierto tiempo.	El riesgo principal de esta técnica sería que un tercero tuviera algún tipo de control sobre el sistema y pasara de forma inadvertida de manera que no se tomarían medidas y el ciberdelincuente gozaría de total libertad.	Un antivirus actualizado que realice análisis continuamente sería, en un principio, una forma de protegerse contra un virus furtivo.	Es un virus informático que suele emplear un troyano u otra herramienta que le permita instalarse en el sistema sin ser detectado.
Zero Day Attack	Es un tipo de exploit, un tipo de ataque que aprovecha y explota las vulnerabilidades de un sistema, las cuales son desconocidas por la empresa atacada y el público en general.	El Zero Day Attack no muestra unos síntomas claros, es por ello que es tan importante contar con buenas medidas de seguridad dado que, por lo general, cuando una empresa se da cuenta de que ha sido atacada, ya es demasiado tarde.	Los riesgos dependen de la gravedad de la vulnerabilidad existente en el sistema.	Depende principalmente de la habilidad para detectar y neutralizar exploits zero-day y así evitar cualquier tipo de ataque de este tipo. En general, la defensa ante este tipo de ataque consiste en las medidas de seguridad empleadas y los programas dedicados a ello.	Se suelen emplear principalmente un virus informático, un troyano, un gusano o una backdoor aprovechando la reciente vulnerabilidad del sistema y asegurarse un acceso en el futuro.
HOAX	Es como se conoce a los fraudes que se llevan a cabo a través de los bulos en internet.	El ciberdelincuente intenta que facilites dinero o información para lo que parecer ser una causa con fines sociales y sin ánimo de lucro pero que en realidad es mentira y solo quiere obtener información personal	Se cometen estafas en las que se obtiene tanto dinero como información del usuario que posteriormente utilizará para llevar a cabo otro tipo de ataques.	Ser consciente de la posibilidad de que existen fraudes que se cometen a través del correo electrónico o las redes sociales e ir con cuidado en relación a cualquier petición de información que no hayas solicitado previamente.	El HOAX se llevaba tradicionalmente a través de correos electrónicos masivos pero con la aparición de las redes sociales, se ha facilitado su distribución y aumentado su alcance potencial por lo que cada vez más, se pueden observar este tipo de ciberdelitos en las redes sociales.

Tabla 2. Técnicas del ciberataque *(cont)*

	Descripción	Síntomas	Riesgos	Métodos de prevención	Principales herramientas utilizadas
Control IoT	Este ataque se aprovecha y toma control del IoT, esto es, tomar el control de la interconexión digital de objetos cotidianos a través de internet.	Aquellos dispositivos u objetos que estén interconectados a través de internet, actuarán de manera sospechosa o realizarán acciones que no se le ha ordenado. Esto significaría que está siendo controlado por otra persona.	Dependiendo del nivel de interconexión que haya en la empresa, el riesgo puede ser distinto pero aquella persona que tome el control del IoT sin autorización podrá controlar todo aquello que esté conectado a la red y hacer un uso ilimitado de ello. No solo representan un riesgo de seguridad sino que son una amenaza a nuestra privacidad.	Existen herramientas que escanean todos los dispositivos que se encuentran conectados a una red para comprobar si existen vulnerabilidades que puedan ser explotadas para acceder a ellos y tomar el control.	El control del Iot se basaría principalmente en el uso de exploits, aprovechando vulnerabilidades de la red para introducirse en ella. Aunque previamente se empleará un sniffer para conseguir información como la dirección ip de la red u otros datos que puedan ser de utilidad en el ataque.
Phising	Son aquellas estafas en las que se suplanta la imagen de una empresa o entidad pública y se engaña a la víctima solicitando datos como si fueran la empresa en la que está interesada la víctima.	La recepción de una solicitud que aparenta pertenecer a una empresa, normalmente reconocida, que pida que se faciliten unos datos personales para alguna promoción de algún tipo u otras razones que resulten sospechosas.	Los riesgos a los que está expuesta una persona víctima de phising son incontables. Dado que el phising permite hacerse con los datos de su víctima para acceder a cuentas personales, pero el phising también puede ser utilizado para instalar algún tipo de malware en ordenador que recibe la acción de phising.	La forma más segura para no resultar víctima de phising es nunca responder a ninguna solicitud de información personal, ya sea a través de correo electrónico, llamada telefónica o SMS.	El phishing puede llevarse a cabo de diversas maneras, desde un simple mensaje a un teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente o la recepción de un correo electrónico.

Tabla 2. Técnicas del ciberataque *(cont)*

	Descripción	Síntomas	Riesgos	Métodos de prevención	Principales herramientas utilizadas
Spyware	El spyware o programas espías son programas que, sin conocimiento o consentimiento para ello, recopilan la información de la que disponga el terminal afectado.	Los síntomas de infección son, entre otros, que habría un cambio en la página de inicio del navegador y que no se podría cambiar, se abrirían varios pop-ups, barras que se añaden en el navegador que no podemos eliminar o que la navegación se hace más lenta.	A través del spyware se puede tener acceso por ejemplo, al correo electrónico, a contraseñas, a la dirección IP, se puede obtener otra información como las páginas webs que visita, que software tienen instalados, cuales se descargan, que compras se hace por internet y datos más importantes como la tarjeta de crédito y las cuentas de banco. Quien se haga con esta información la podrá usar con la misma libertad que su propietario original.	Suelen entrar en los sistemas a través de páginas web que descarguen el malware u ocultos en programas gratuitos. Por ello, con un programa anti-spyware y una navegación prudente, se reducirían las probabilidades de infección.	Existen distintos tipos de spyware y cada uno se dedica a una acción distinta pero en general, los spyware suelen utilizar keyloggers, troyanos, backdoor, gusanos y otros métodos que les permite tanto infectar al usuario como ampliar las posibilidades del delincuente.
Crimeware	SCualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un crimen financiero en la red.	El crimeware es bastante difícil de detectar, sin embargo, suele presentar algunos síntomas como la ralentización general del sistema o la recepción no solicitada de correo electrónico, que pueden incluir archivos adjuntos. Incluso que el proveedor de servicios de Internet le avise de que el equipo está enviando spam, esto significaría que está siendo utilizado por un tercero.	Existen dos riesgos diferentes en el crimeware. Por un lado estaría la víctima contra la que se lleva a cabo el delito financiero en donde se le roba parte de su capital. Por otro, se encontrarían aquellas personas infectadas, pertenecientes a la botnet a través la cual se ha atacado y se ha llevado a cabo el ciberdelito financiero pudiendo ser confundidos con el ciberdelincuente.	Disponer de programas antivirus y mantener actualizados los softwares instalados en el ordenador es la manera más básica de evitar cualquier infección. También puede consultar con su proveedor de servicios de Internet el nivel de protección que ofrece contra el crimeware.	Virus informáticos, troyanos bancarios, gusanos o botnets son unas de las herramientas más utilizadas por los ciberdelincuentes que realizan acciones de crimeware.

Tabla 2. Técnicas del ciberataque *(cont)*

	Descripción	Síntomas	Riesgos	Métodos de prevención	Principales herramientas utilizadas
Ransomware	La finalidad de este ciberataque es bloquear o restringir el acceso del usuario al sistema hasta que se realice un pago al ciberdelincuente.	Que el usuario no pueda usar el sistema como habitualmente hace, que el sistema no deje instalar ni desinstalar software o que aparezcan programas que te piden, de la forma que sea, dinero son indicadores de que la terminal ha sido infectada.	Se pueden perder todos los datos que han sido retenidos por el ransomware y la tramitación del pago del rescate no garantiza la recuperación de dichos datos. Las perdidas pueden variar según el valor de la información que se tenga almacenado en el sistema.	Es necesario estar protegidos con programas antivirus especializados y que estén actualizados de forma que no baje su efectividad. También se pueden realizar copias de seguridad en dispositivos que no estén conectados al sistema.	Un método de llevar a cabo este tipo de ataque es emplear el correo electrónico para propagar un troyano que llevará a cabo la función de restringir el acceso a los archivos afectados.

ANEXO 3


CIBERDELINCUENTES
Perfil tecnológico
LOS EXPERTOS O MAESTROS
La ciberdelincuencia especializada responde a un perfil de delincuente con altos conocimientos informáticos cuyo móvil es fundamentalmente económico, si bien, en algunos casos se busca el reconocimiento personal.
LOS HACKERS
Máximos exponentes de la ciberdelincuencia especializada. Si bien según su filosofía pueden actuar de buena fe poniendo sus conocimientos al servicio social y de la empresa.
Los hackers que cometen actos delictivos son conocidos como Black Hat Hackers o hackers de sombrero negro. Son altamente peligrosos.
LOS INTRUSOS
LOS INTRUSOS
Delincuentes informáticos con un nivel de conocimientos tecnológicos bajos. Su móvil puede estar relacionado con la venganza personal, la pertenencia a grupo y el reconocimiento social. En algunos casos sus fines pueden ser económicos.
Este tipo de ciberdelincuente puede tener aspiraciones más altas y convertirse en aspirantes a hackers, convirtiéndose en maestros.
BLACK HAT HACKERS
• Crackers
• Hacktivistas
• Piratas informáticos
• Spammers
• Hoaxers
• Contratistas
• Viruckers
• Domainers
• Banqueros
• Agentes especiales
• Sniffers
• Terrorista informático
• Traficantes de armas
• Phishers
• Agentes especiales
• Ninjas pesos pesados
INTRUSOS
• Lammers
• Emmuger
• Wannabe
• Poseur
• Scrip kiddie
• Newbie

CIBERDELINCUENTES

Maestros o expertos

LOS HACKERS PERFIL

Persona o comunidad experta en el área informática y entorno digital, **que domina el lenguaje de programación, la manipulación de hardware y software y las telecomunicaciones, dedicando sus conocimientos y esfuerzos a intervenir o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o servicio.**

WHITE HAT HACKER

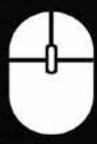
Son los Hackers Éticos o Tradicionales. Utilizan sus conocimientos técnicos para descubrir vulnerabilidades o brechas en los sistemas informáticos, y ponerlas en conocimiento del administrador del sistema con el fin de solventarlas.

Es habitual que los white hat hackers hayan pertenecido con anterioridad a bandas organizadas del cibercrimen.

BLACK HAT HACKERS

Los sombreros negros se dedican a realizar actividades orientadas a vulnerar la seguridad de sistemas, ingresar de forma violenta e ilegal a sistemas privados y extraer información restringida con fines económicos o personales.

Se sienten orgullos de sus habilidades y cuanto mayor sea la repercusión del delito mayor será su grado de autorrealización.



GREY HAT HACKERS

Sujetos cuya ética es ambigua. Poseen conocimientos comparables a los de un Black Hat Hacker que utilizan para encontrar vulnerabilidades o fallos de seguridad, ofreciéndose, posteriormente a solventarlos bajo un acuerdo económico.

«HACKER» varón, de entre 25 y 35 años de edad y con altos conocimientos informáticos y tecnológicos que le permiten considerar la red como el medio que mejor se ajusta a sus necesidades para desarrollar sus actividades.

Desconfía de la autoridad opresora y considera que el acceso a cualquier información que pueda servir para conocer el funcionamiento del mundo debería ser ilimitado y gratuito.


CIBERDELINCUENTES
Maestros o expertos
BLACK HAT HACKERS
TIPOS
CRACKERS. Expertos programadores que utilizan sus conocimientos para modificar el comportamiento de sistemas y redes explotando cualquier vulnerabilidad encontrada, actuando de manera obsesiva y guiados por un afán destructivo y ególatra.
Cyberpunk. Vándalos de páginas web o sistemas informatizados. Destruyen el trabajo ajeno.
Crackers de criptografía. Se dedican a la ruptura de criptografía (crackear códigos)".
Crackers de sistemas. Programadores y decoders que alteran el contenido de un programa.
Phreaker. Cracker especializado en telefonía. Reprograma centrales telefónicas, graba conversaciones, etc.
VIRUCKER. Creadores de virus.
BANQUERO. Robo de información financiera.
DOMAINER. Compra y venta de dominios para reventa.
SPAMMER. Difusión de mensajes no deseados. Publicidad.
HOAXER. Difusión de bulos.
CONTRATISTA. Hacker por contrato.
AGENTE ESPECIAL. Alto nivel de especialización. Espionaje.
SNIFFER. Robo de información a través de software especializado.
BUCANEROS. Comerciantes en la red. Material ilegal.
PHISHER. Suplantación de identidad. Robos.
TRAFICANTES DE ARMAS. Venta de malware a otros ciberdelincuentes.
HACKTIVISTA. Hakers que luchan por sus intereses e ideales.
TERRORISTA INFORMÁTICO. Difusión del terror entre la población. Fines religiosos, políticos o sociales.
NINJA PESO PESADO. Crimen organizado. Robo de información. Estructura muy jerarquizada. Fin económico.
CIBER-SOLDADOS. Objetivos militares. Pueden dirigir sus esfuerzos hacia las grandes corporaciones.

CIBERDELINCUENTES

Intrusos

INTRUSOS TIPOS

EMUGGER. Grupo más numeroso de ciberdelincuentes. No poseen grandes habilidades o conocimientos técnicos. Desarrollan códigos maliciosos, *adwares* o *spams* y una vez que perfeccionan la técnica, lo repiten una y otra vez con el fin de obtener ganancias económicas de manera muy rápida.

WANNABE. Aficionado que desea integrarse en un conjunto de especialistas. Es un usuario que sabe más que el promedio, aunque es consciente de que no posee el mismo nivel del grupo al que desea acceder y que debe adquirir más conocimiento. Etimológicamente proviene del inglés «*want to be*» que quiere decir: quiero ser

POSEUR. Parecido al Wannabe, pero este usuario sólo tiene interés por intentar ser participante del grupo, sin que le importe en verdad los ideales, el conocimiento o cualquier otra cosa del mismo. Sin embargo, se diferencia del Wannabe en que el Poseur se aplica con mayor frecuencia en el ámbito fuera de internet, es decir, las personas que utilizan algunos estilos musicales o modas y apariencias con la finalidad de sentirse miembro de la misma.

NEWBIE. Es el considerado novato, que siente curiosidad por el mundo del hacking, busca información sobre el tema y descarga todas las utilidades y programas que puede en su ordenador para ver qué hacen. Pocas veces son capaces de penetrar en un sistema vulnerable, pero cuando lo hacen, se pierden debido a sus escasos conocimientos y no saben qué hacer. Muchas veces se les confunde con los lammers, ya que suelen presumir de las habilidades que han aprendido.

LAMMER. Es el usuario que alardea de poseer algunos conocimientos que en verdad no tiene. Con frecuencia, son aficionados con poca madurez, falta de sociabilidad o habilidades que intentar una manera falsa de destacar sobre los demás.

SCRIPT KIDDIE. Un script kiddie es un usuario con poca experiencia en los sistemas informáticos que, utilizando herramientas y mecanismos automáticos que han sido pre-empaquetados y definidos por otros, interrumpen en los sistemas informáticos. Suelen tener poca capacidad de comprensión del concepto subyacente, por eso provienen del término script, que quiere decir guión o plan pre-establecido y kiddie que significa niño o usuario inmaduro e inexperto.

ANEXO 4


EL CIBERDELITO EN LA EMPRESA
INSIDERS VS OUTSIDERS
INSIDER
Actúa desde el interior de la empresa.
Perfil tecnológico medio / alto.
Motivación económica o venganza.
OUTSIDER
ACTÚAN DESDE FUERA
MOTIVACIÓN ECONÓMICA
VENGANZA
RECONOCIMIENTO
PERFIL TECNOLÓGICO
¿SABÍAS QUÉ ...
... El 90% de los ciberdelitos contra la empresa los cometen sus empleados.
El resto de los delitos en un porcentaje muy amplio (7%) son cometidos por antiguos empleados.
Mientras que en el resto (1,5%) el empleado es simplemente un instrumento?

ANEXO 5
Entrevista estructurada

Pregunta 1
¿Ha consultado o tiene constancia del aumento del ciberdelito en la empresa en los últimos años?

Pregunta 2
¿Adopta algún tipo de medida contra el ciberdelito?

Pregunta 3
¿Podría citar al menos 3 tipos de ciberdelito?

Pregunta 4
¿Protege sus equipos informáticos con softwares específicos?

Pregunta 5
¿Ha pensado alguna vez que un empleado puede atacar los intereses de su empresa mediante un ataque informático?

Pregunta 6
¿Ejerce algún tipo de control en materia informática en el desarrollo de las tareas diarias de sus trabajadores?

Pregunta 7
¿Contrataría a un hacker? ¿Porqué?

Pregunta 8

Por último, teniendo en cuenta todas las respuestas, ¿considera que el tamaño de la empresa afecta a su visión del ciberdelito?

CONCEPTUALIZACIÓN, EVOLUCIÓN Y CLASIFICACIÓN DEL CIBERDELITO EMPRESARIAL

DEFINICIÓN DEL PERFIL DEL CIBERDELINCUENTE. IMPLICACIONES ESTRATÉGICAS

En los últimos años el estudio de las Tecnologías de la Información y Comunicación (TIC) se ha convertido en un elemento fundamental para el conocimiento de la gestión empresarial. Concretamente, los expertos señalan el análisis de los cambios que han generado las nuevas tecnologías, en las diferentes esferas de la empresa, como una herramienta imprescindible para la adecuación de las estrategias de las organizaciones al entorno.

En este sentido, las investigaciones han ido evolucionando de forma paulatina a medida que las nuevas tecnologías han pasado a formar parte de lo cotidiano, pudiendo incluso afirmarse que la normalización del uso de Internet ha dotado a la tecnología de capacidad suficiente como para transformar las relaciones en el mundo empresarial.

En este contexto, el ciberespacio se ha convertido en un nuevo lugar para la comisión de nuevas formas de delito que atentan contra la intimidad, el honor o la propiedad, entre otros, y que ponen en riesgo el ciclo de vida de cualquier organización.

ISBN: 978-84-946590-5-8

AMEC
EDICIONES