XXIII SEMINARIO "DUQUE DE AHUMADA"

CIBERAMENAZAS Y REDES SOCIALES

IuIsI

Instituto Universitario de Investigación sobre Seguridad Interior

Academia de Oficiales de la Guardia Civil
Aranjuez, 24 de octubre de 2012

Inscripciones en: www.iuisi.es

UNED

Facultad de Derecho (UNED)
Madrid, 25 de octubre de 2012

MINISTERIO
DEL INTERIOR

Academia de Oficiales
de la Guardia Civil

XXIII SEMINARIO «DUQUE DE AHUMADA»

"CIBERAMENAZAS Y REDES SOCIALES"

DIRECTOR AOGC:
Ángel Arancón García.

DIRECCIÓN:
Academia de Oficiales de la Guardia Civil
Paseo de la Princesa, s/n - 28300 ARANJUEZ (Madrid)
Teléf. 91 891 21 45
e-mail: en-aca-aranjuez@guardiacivil.org

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES:
http://www.060.es

En esta publicación se ha utilizado papel reciclado libre de cloro, de acuerdo con los criterios medioambientales de contratación pública.

Edita:

MINISTERIO DEL INTERIOR

EC E A ÍA
GENE AL CNICA

Febrero, 2013

Depósito legal: M-14141-2013
NIPO EDICIÓN PAPEL RECICLADO: 126-13-041-9
NIPO EDICIÓN EN LÍNEA: 126-13-042-4
ISBN: 978-84-8150-308-1

IMPRIME: Asociación Pro Huérfanos de la Guardia Civil (Imprenta-Escuela)
Príncipe de Vergara, 248 - 28016 MADRID

XXIII SEMINARIO "DUQUE DE AHUMADA"

"CIBERAMENAZAS Y REDES SOCIALES"

PRESIDENCIA DE HONOR

D. Arsenio Fernández de Mesa Díaz del Río. Director General de la Guardia Civil.

D. Juan Antonio Gimeno Ullastres. Rector de la Universidad Nacional de Educación a Distancia.

ORGANIZACIÓN

DIRECTORES

D.ª Ana Rosa Martín Minguijón. Decana de la Facultad de Derecho de la UNED.

D. Ángel Arancón García. Coronel Director de la Academia de Oficiales de la Guardia Civil.

COORDINACIÓN

D.ª Consuelo Maqueda Abreu. Directora del Instituto Universitario de Investigación sobre Seguridad Interior.

SECRETARIA

D.ª María Isabel Solís Gil. Guardia Civil. Academia de Oficiales de la Guardia Civil.
D.ª Karen Vilacoba Ramos. Secretaría IUISI.

COMISIÓN ORGANIZADORA

D. Miguel Gómez Jene. Vicedecano de Relaciones Internacionales e Institucionales de la Facultad de Derecho de la UNED.

D. Fernando Moure Colón. Teniente Coronel de la Guardia Civil. Academia de Oficiales de la Guardia Civil.

D. Rafael Junquera de Estefani. Vicedecano Profesorado y Espacio Europeo de la Facultad de Derecho UNED.

DISEÑO GRÁFICO

D. Gregorio Arteaga Serrano. Guardia Civil. Academia de Oficiales de la Guardia Civil.

ÍNDICE

Págs.

Presentación. Ideas y reflexiones

D.ª Consuelo Maqueda Abreu
Directora del Instituto Universitario de
Investigación sobre la Seguridad Interior
IUISI

De acuerdo con los objetivos y la finalidad del Seminario Duque de Ahumada, su edición número XXIII se ha ocupado de un tema de actualidad, como no podía ser menos. Un tema ineludible por su naturaleza y las circunstancias que estamos viviendo.

En efecto. A nadie se le oculta la importancia que las redes sociales tienen en nuestro tiempo, hasta el punto de que se han convertido en el espacio de sociabilidad más intenso y multiforme de los que existen actualmente. Y esas redes, como tantas otras dimensiones nutren el ciberespacio de todo género de elementos: relaciones humanas, informaciones de la naturaleza más variada, ayudas, amenazas... elementos donde no faltan los de naturaleza criminal.

El ciberespacio se convierte así en un ámbito donde es necesario garantizar la seguridad. Por eso, en el Seminario Duque de Ahumada no podíamos dejar de abordar este tema, pues somos conscientes de los peligros que implica, de los riesgos que entraña y de su insuficiente regulación procesal. Tenemos plena conciencia de que, por un lado, es necesario determinar la competencia y la autoridad judicial, además de la necesidad de estudios periciales, cuestiones para las que es útil la jurisprudencia que van estableciendo los Tribunales Constitucional y Supremo. Por otro lado, también tenemos presente las oportunidades que ofrecen los nuevos medios para los Cuerpos y Fuerzas de Seguridad del Estado en ámbitos tan variados como la información, la comunicación, la participación ciudadana y la identificación de las distintas formas de delincuencia que inciden en las redes sociales, sobre todo las relacionadas con menores (grooming, sexting, ciberbullying, distribución de pornografía infantil...).

Pero aún queda mucho por hacer, dado el espectacular incremento de los usuarios de Internet y la tremenda expansión de las redes sociales; es necesario desarrollar planes de I+D nacional, potenciar la capacitación de los miembros de los Cuerpos y Fuerzas de

Seguridad, generalizar los consejos y recomendaciones para utilizar con seguridad las redes sociales, desarrollar organismos como el CNPIC (que hace frente a las amenazas del ciberespacio sobre las infraestructuras críticas), conocer los riesgos y soluciones informáticas para neutralizarlas, llegado el caso.

Nuestro Seminario comenzó por abordar el tema del cibercrimen, la "otra" delincuencia, en la ponencia de D. Fernando Miró Llinares y continuó con la intervención del ponente D. Antolín Herrero Ortega, quien se ocupó de plantearnos una síntesis legislativa sobre el particular. La tercera sesión se centró en un panel relativo a las redes sociales, en el que intervinieron D. José María Blanco Navarro, quien se centró en el tema redes sociales y seguridad, y D. Oscar de la Cruz Yagüe, que se ocupó de la delincuencia en dichas redes.

El Seminario continuó con el panel dedicado a las ciberamenazas, analizadas primero por D. Juan Antonio Gómez Bule, que las contrapuso a la ciberseguridad y D. Fernando Sánchez Gómez, que se ocupó de las infraestructuras críticas frente a las ciberamenazas.

El colofón lo constituyó una mesa redonda dedicada a los retos presentes y futuros en materia de ciberseguridad, que contó con los ponentes D. Álvaro Ortigosa Juárez, D. Antonio Ángel Ramos Varón, D. Mario Farnós Buesa y D. Óscar Casado Oliva.

Como siempre, esta edición del Seminario Duque de Ahumada ha sido posible gracias a la colaboración de la Facultad de Derecho de la UNED y de la Academia de Oficiales de la Guardia Civil, que con el IUISI, constituyen el trípode que sostiene esta actividad desde hace varios lustros.

Como Directora del IUISI, quiero expresar mi agradecimiento a todos los que han colaborado tan generosamente en las sesiones del Seminario, tanto a los ponentes, que nos han dado lo mejor de su buen hacer y de su solvencia profesional, como a los asistentes, pues sin ellos, el Seminario carecería de sentido. Y en mis agradecimientos quiero singularizar a la Profa. Ana Rosa Martín Minguijón, Decana de la Facultad de Derecho y D. Ángel Arancón García, Coronel Director de la Academia de Oficiales de la Guardia Civil.

Y ya sin más preámbulos, el lector puede adentrarse en las páginas que siguen, que contienen el texto de las ponencias e intervenciones habidas en el Seminario y que estoy segura resultarán de su interés, pues una vez más el Seminario Duque de Ahumada aborda un tema de actualidad con la Seguridad como objetivo en sus más variadas dimensiones. En este caso, una dimensión de indudable actualidad.

Muchas gracias a todos

Palabras en la clausura del Seminario

D. Francisco Gabella Maroto
General de División de la Guardia Civil
Subdirector General de Apoyo

Nos encontramos en un foro de conocimiento en el que desde el año 1989 se han celebrado jornadas para analizar y reflexionar sobre contenidos directamente relacionados con la misión atribuida a la Guardia Civil, de garante de la seguridad y de la libertad de los ciudadanos.

Fruto del esfuerzo compartido de la Universidad Nacional de Educación a Distancia, el Cuerpo de la Guardia Civil y del Instituto Universitario de Investigación sobre Seguridad Interior (IUISI), han compartido sus conocimientos expertos universitarios, científicos, juristas, políticos y reconocidos especialistas de las Fuerzas y Cuerpos de Seguridad del Estado, entre otros. Todo ello ha permitido aproximar el mundo de la Universidad a nuestra Institución con el doble objetivo de acercarla aún más a la sociedad a la que sirve y servir de punto de encuentro para el intercambio de conocimientos y experiencias en materias relacionadas con la seguridad.

No menos importante ha sido el nivel de los asistentes a esta tradicional actividad formativa que, como es habitual, colaboran con su activa participación a fomentar el debate y la puesta en común de otras perspectivas a tener en consideración.

La temática que se ha abordado en el marco del presente seminario constituye uno de los asuntos de mayor actualidad tanto en el entorno social en el que vivimos como en el campo de la Seguridad en su más amplio sentido, lo que incluye también al ámbito de la Defensa.

Durante estos dos días se han tratado de manera especial las ciberamenazas y las redes sociales analizándolas desde todas las perspectivas posibles, puesto que sólo desde un enfoque integral se pueden afrontar los desafíos que supone el uso malintencionado de internet, y sólo así, es posible responder con éxito a los fines que se pretenden.

La aparición y la generalización del uso de las Tecnologías de la información y de las comunicaciones (1) ha traído consigo un extraordinario cambio en todas las facetas de nuestra vida. Se han modificado sustancial y positivamente los métodos de trabajo, las transacciones comerciales o las relaciones humanas en el sentido que nos permiten ser más eficientes, nos facilitan el acceso a la información e incrementan nuestras capacidades de comunicación en todos los ámbitos.

Y además, hay que destacar la potencialidad que presentan, puesto que las nuevas tecnologías proporcionan unas importantes oportunidades en cuanto a su uso futuro por parte de los Cuerpos de Seguridad.

Sin embargo, como cualquier avance tecnológico, aunque con mayor trascendencia, "la red de redes" es también utilizada para todo tipo de fines ilícitos, alentados por el anonimato o por la facilidad de ocultamiento, como algunas sus principales fortalezas.

Ante este escenario un gran número de países e instituciones han incluido la delincuencia tecnológica y la ciberseguridad entre sus principales prioridades, al igual que lo han hecho el Ministerio del Interior y la Guardia Civil. Es preciso subrayar la presentación del Gobierno en el pasado mes de junio de la "Estrategia Española de Ciberseguridad", que establece objetivos, líneas de acción y la forma de organización de la ciberseguridad.

También es preciso tener presente la nueva Directiva de Defensa Nacional, que el Gobierno dio a conocer el pasado mes de agosto, que identifica los ataques cibernéticos como una de las principales amenazas globales que afectan a los estados democráticos, basta recordar los casos ocurridos en algunos países donde un ataque masivo a sus sistemas de comunicación o un envío masivo de correos electrónicos estuvo a punto de conseguir el colapso del país (2). Esto ha provocado que organizaciones de defensa como la OTAN creara en 2008 un Centro de Excelencia para la Ciberdefensa.

En este sentido se viene desarrollando el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) como un organismo que dirija la protección de todas las infraestructuras consideradas críticas para la estabilidad y seguridad del país y que puedan ser objeto de ataques, no sólo de índole física sino también de índole informática.

Pero aparte de las amenazas a la estabilidad y la propia supervivencia de los Estados, existe un cibercrimen que afecta directamente y cada día a los ciudadanos. Los ciberdelincuentes han encontrado un entorno ideal de bajo riesgo y alta rentabilidad, del que se aprovechan el crimen organizado y los grupos terroristas, los cuales hacen cada día un mayor uso de internet, no sólo para la comisión de actos delictivos sino también para sus comunicaciones y organización.

Sin embargo, en este ciberespacio las redes sociales ocupan un lugar destacado. Las redes sociales forman parte de la revolución que ha supuesto el uso de internet en las rela-

---

(1) Conocidas comúnmente como TIC,s.

(2) En 2005 se produjo un ataque masivo en EEUU que paralizó numerosas organizaciones gubernamentales como el Pentágono, la Casa Blanca o la Agencia de seguridad Nacional entre otras. Igualmente en Corea de Sur en 2009 se produjo un ataque similar y en 2007 Estonia quedó virtualmente paralizada.

ciones humanas, como se ha podido ver claramente en la denominada "Primavera Árabe", y son un claro ejemplo del rápido cambio asociado a las TIC´s y de sus efectos adversos, principalmente por el desconocimiento en el uso y los derechos en torno a la actividad de sus usuarios.

Los datos de los usuarios de estas tecnologías en relación a su identidad y privacidad están expuestos y accesibles, lo que resulta especialmente preocupante en el caso de los menores, potenciales víctimas de acosos a través de internet (cyberbullying, grooming, sexting, etc.).

La firme voluntad de proteger a los colectivos más vulnerables constituye uno de los pilares de toda nación democrática por lo que se han realizado varias actuaciones en dicho sentido. Así, se ha creado recientemente la figura del Fiscal de Sala de Criminalidad Informática (3) y se ha establecido un marco competencial que constituye una referencia para las unidades policiales dedicadas a combatir esta forma de criminalidad.

Por otro lado, la Secretaría de Estado de Seguridad en el año 2007 puso en marcha el Plan Director para la Mejora de la Convivencia y Seguridad Escolar, aprobado en la Instrucción 3/2007 y prorrogado en la Instrucción 9/2009, en los que participan las Fuerzas y Cuerpos de Seguridad del Estado para la formación de padres, profesores y alumnos de centros escolares y de educación secundaria y en los que se tratan temas relacionados con el cibercrimen y ciberacoso.

Conscientes de la importancia y alarma social que provocan el cibercrimen, y más en concreto cuando afecta a nuestros jóvenes, la Guardia Civil ha articulado una respuesta adecuada a dicha amenaza en varios niveles. En el primer nivel estarían los Equipos de Investigación Tecnológica de las Unidades Orgánicas de Policía Judicial de las Comandancias. Se trata de miembros de esas Unidades que han recibido una preparación específica y desarrollan entre otros, cometidos propios de Policía Judicial, las investigaciones relacionadas con la red.

En un segundo nivel, estarían los Grupos de Delitos Telemáticos de la Unidad Central Operativa de Policía Judicial y el Grupo de Ciberterrorismo de la Jefatura de Información. Se trata de grupos dotados de unos mejores medios y capacidades que realizan investigaciones complejas y apoyan a las unidades territoriales. En un nivel superior por encima de éste estarían las unidades con capacidad de realizar análisis e inteligencia, las cuáles se sitúan en las propias Jefaturas de Policía Judicial e Información.

De una manera transversal a estos niveles, se han tomado una serie de medidas y acciones para tratar de llegar precisamente a esos colectivos más vulnerables y concienciar a la ciudadanía. Así, la Guardia Civil (y otras FCS) ha abierto cuentas en facebook, twitter y un canal de youtube, a la vez que se han creado plataformas, aplicaciones telemáticas para smartphones y cuentas de correo electrónico para facilitar el acercamiento a las víctimas de delitos en la red y ofrecer consejos y alertas de seguridad.

---

(3) Instrucción 2/2011 de la Fiscalía General del Estado.

Existe un nivel más, si bien no está directamente dentro del Cuerpo, pero en el que está plenamente involucrado. Se trata del CNPIC, en el que las Fuerzas y Cuerpos de Seguridad tienen un papel fundamental. La Guardia Civil con un gran número de infraestructuras críticas en su demarcación, se configura como un actor fundamental y por ello participa en el sistema en todos sus planos, desde el puramente estratégico del diseño del sistema hasta el más operativo en lo que a la protección de las propias instalaciones se refiere.

Pero si estamos hablando de la complejidad del cibercrimen por su anonimato, su transnacionalidad y dinamismo, se hace necesario el hablar forzosamente de la cooperación entre todos los diferentes sectores. Por un lado la colaboración policial internacional a través de Europol e Interpol para la coordinación de las operaciones entre diferentes países, el intercambio de información e inteligencia y la futura puesta en marcha del European Cybercrime Centre (EC3), que tiene el cuádruple objetivo de ser el punto información de la UE en materia de cibercrimen, ser el centro de referencia para la formación de expertos, apoyar las investigaciones de los países miembros y, por último, ser el interlocutor de la UE en dicha materia.

Pero además, debe haber una cooperación con el sector privado mediante el establecimiento de canales de comunicación con los administradores de las redes sociales y de los proveedores de servicios entre otros, a la vez que debe existir una intensa colaboración con la comunidad académica, ya que juega un importante papel, tanto en la investigación y desarrollo de nuevas herramientas que faciliten la lucha contra la ciberdelincuencia como en la formación de los investigadores policiales. En este sentido, me gustaría recordarla la colaboración existente entre Guardia Civil y la Universidad de Alcalá de Henares por la que miembros del Cuerpo vienen recibiendo el Curso de Experto Universitario en Investigación Tecnológica, que constituye el primer curso universitario realizado exclusivamente para el Cuerpo, para la formación de alto nivel técnico que permite afrontar investigaciones de una mayor complejidad.

En definitiva, el cibercrimen constituye una de las principales amenazas para los estados y constituye uno de los más difíciles retos que las Fuerzas y Cuerpos de Seguridad debemos afrontar. La innovación y el rápido cambio de las nuevas tecnologías, su anonimato, la variedad de formas delictivas que originan y su transnacionalidad van a suponer un esfuerzo constante por nuestra parte, para tratar de dar una respuesta adecuada, que debe estar basada en un enfoque multidisciplinar y una cooperación interagencias intensa y lo más fluida posible.

Muchas gracias

El cibercrimen, "la otra" delincuencia

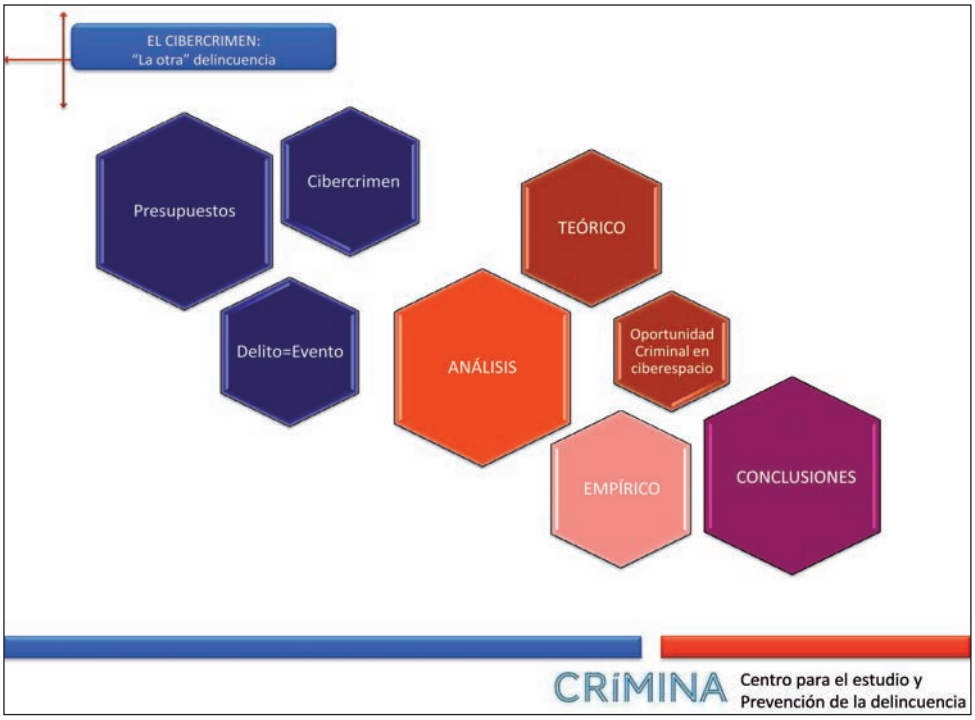
Ponencia de D. Fernando Miró Llinares
Profesor Titular de Derecho Penal
Universidad Miguel Hernández de Elche

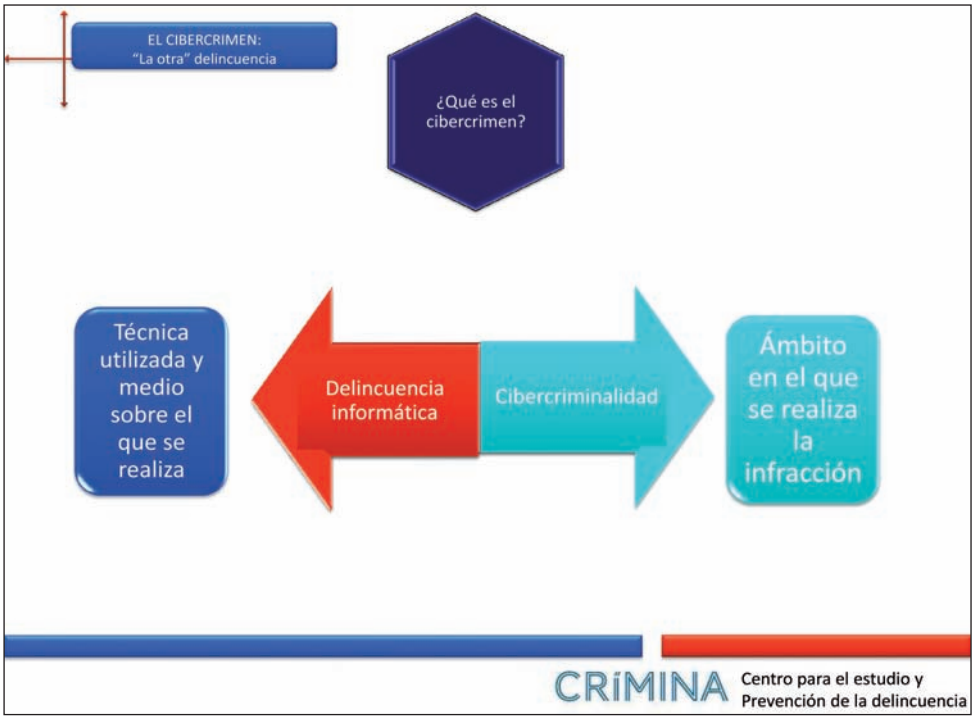
Desarrollando su labor docente e investigadora desde hace más de quince años. En la actualidad compagina tales labores con el cargo de Decano de la Facultad de Ciencias Sociales y Jurídicas de dicha Universidad, así como con la de Director del Centro Crímina para el estudio y prevención de la delincuencia.

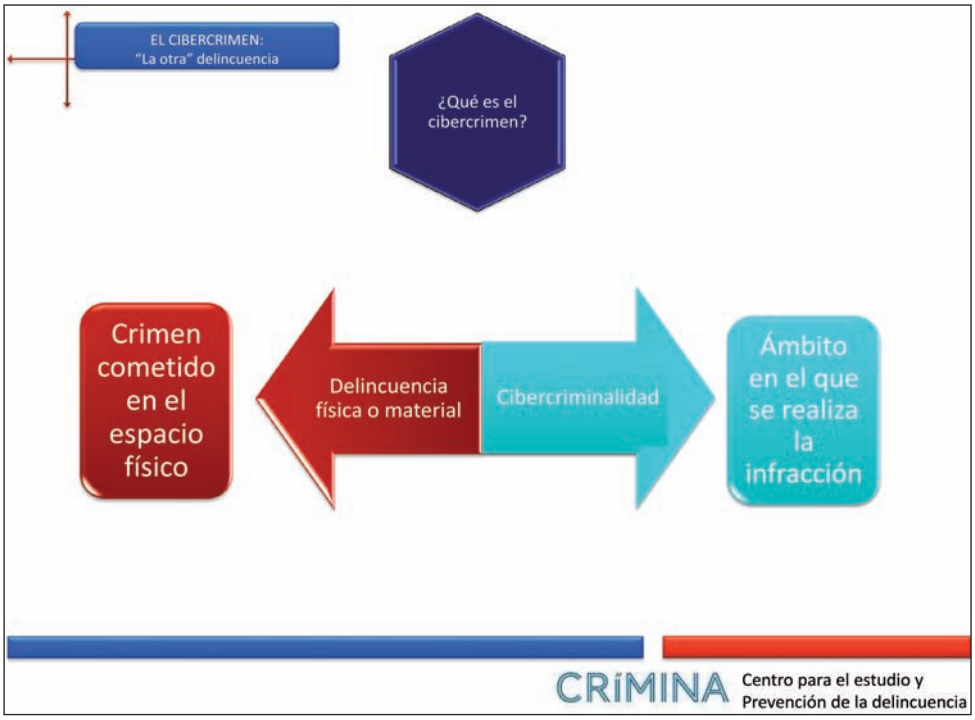
El profesor Miró ha impartido docencia en diferentes programas de master y grados en múltiples univesidades españolas como la UNED, la Universidad de Granada, la Universidad Pompeu Fabra, la Universidad de Sevilla, La Universidad de Barcelona, La Universidad del País Vasco, entre muchas otras, y extranjeras como la University of Texas at San Antonio, la Universidad de Tübingen, la Universidad de Twente, la Universidad de Los Andes en Bogotá o la Universidad de Buenos Aires. Además, en el ámbito docente, dirige en la actualidad diferentes títulos universitarios: Máster oficial en Intervención Criminológica y Victimológica, Máster en Análisis y Prevención del Crimen, Diploma Superior en Seguridad y Ciencias Policiales, Título de Experto universitario en Investigación Criminal y Criminalística y Título de Experto universitario en Gestión y Dirección de Seguridad.

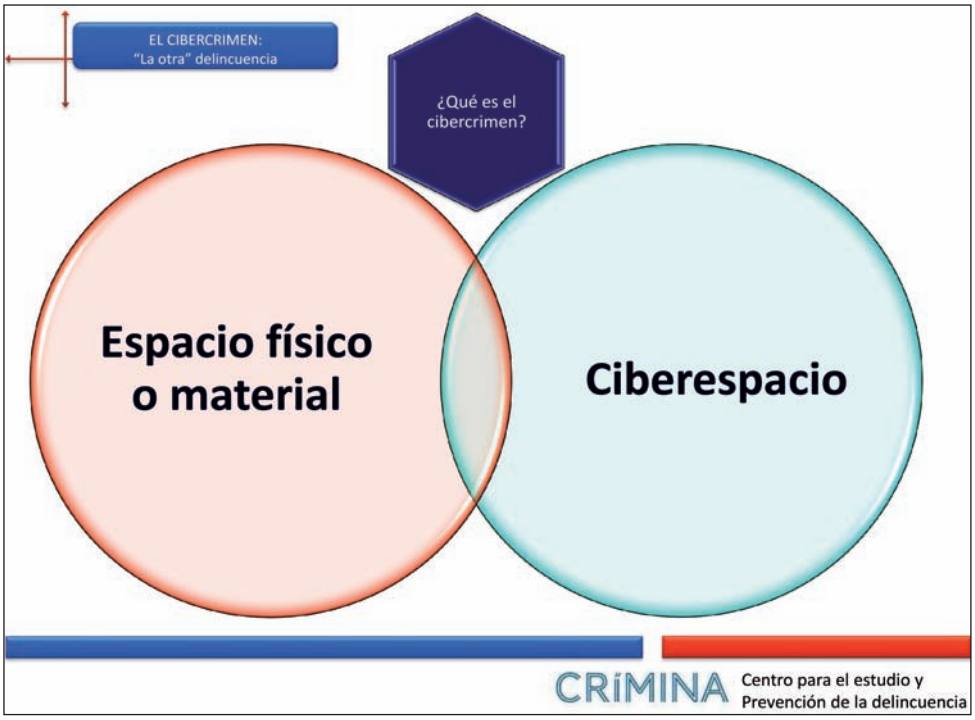
El Profesor Miró es autor de más de cincuenta publicaciones sobre diversos temas del Derecho penal moderno, destacando sus investigaciones sobre teoría general del delito, sobre Derecho penal económico y empresarial y, en los últimos años, sobre temas relacionados con la seguridad desde una perspectiva preventiva como el terrorismo, la seguridad vial, la delincuencia juvenil y, muy en particular, el cibercrimen. En esta materia el profesor Miró dirige en la actualidad un proyecto de investigación financiado por el Ministerio de Economía y competitividad y titulado "Cribercriminalidad: detección de déficits en su prevención jurídica y determinanción de los riesgos de victimización para una mejor prevención situacional criminológica", a partir del cual ha publicado varios trabajos de entre los que destaca "La oportunidad criminal en el ciberespacio", en el que trata de desarrollar la teoría criminológica de las actividades cotidianas al nuevo ámbito de oportunidad delictiva que es Internet. En las próximas semanas verá la luz su último libro, *"El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio"*.

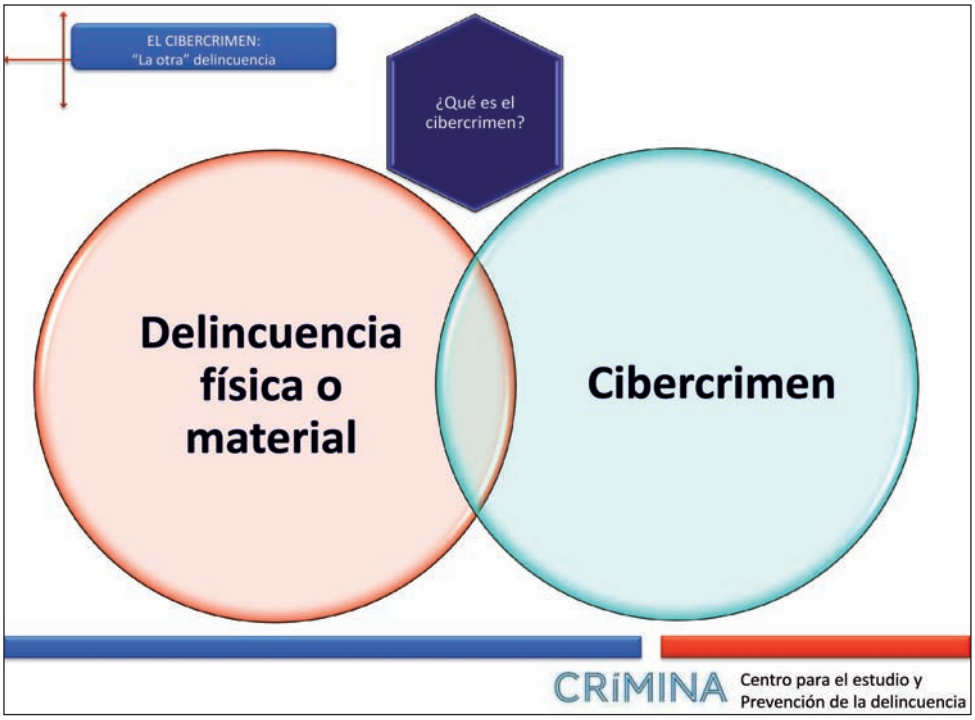

CRÍMINA
Centro para el estudio y
Prevención de la delincuencia
EL CIBERCRIMEN:
"La otra" delincuencia
XXIII SEMINARIO "DUQUE DE AHUMADA"
"CIBERAMENAZAS Y REDES SOCIALES"
Prof. Dr. Fernando Miró Llinares


EL CIBERCRIMEN:
"La otra" delincuencia
Presupuestos
Cibercrimen
Delito=Evento
TEÓRICO
ANÁLISIS
Oportunidad Criminal en ciberespacio
EMPÍRICO
CONCLUSIONES
CRÍMINA
Centro para el estudio y
Prevención de la delincuencia

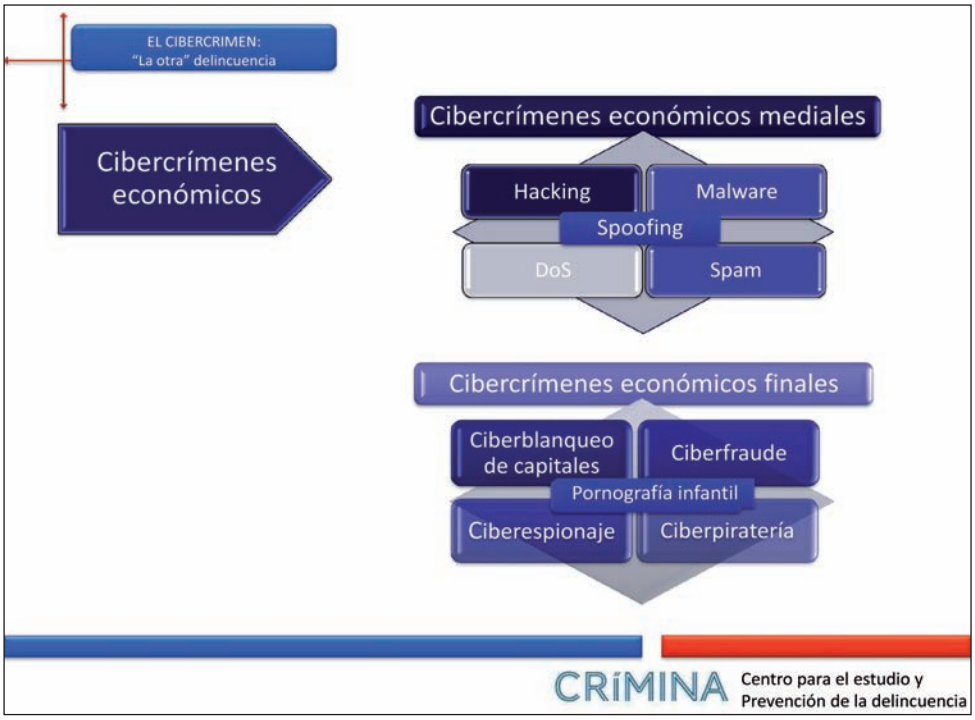

EL CIBERCRIMEN:
"La otra" delincuencia
¿Qué es el cibercrimen?
Técnica utilizada y medio sobre el que se realiza
Delincuencia informática
Cibercriminalidad
Ámbito en el que se realiza la infracción
CRIMINA
Centro para el estudio y Prevención de la delincuencia

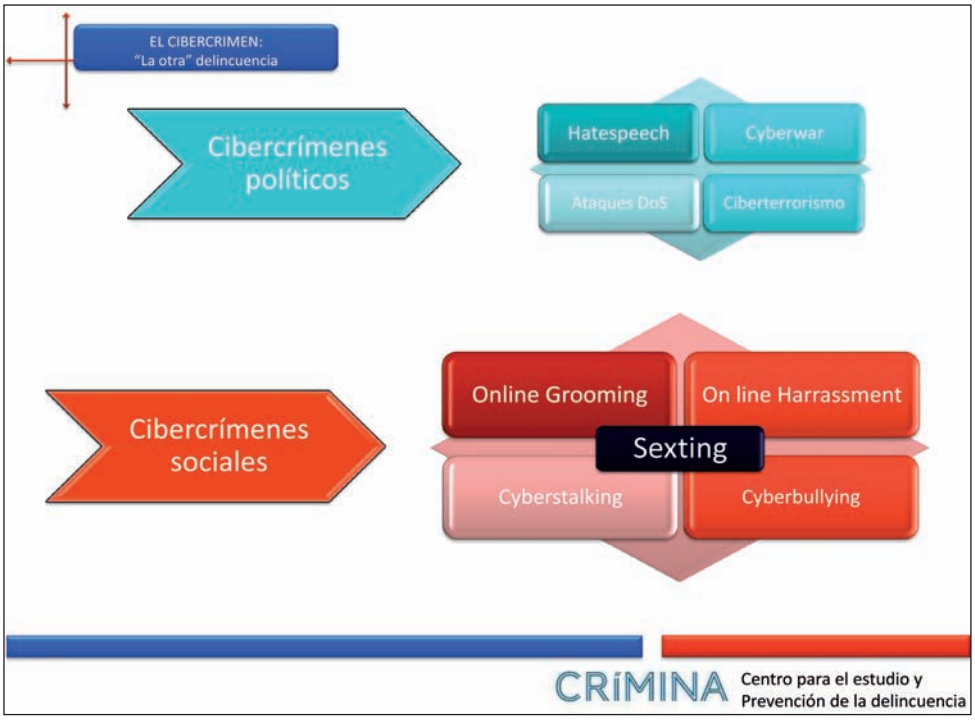

EL CIBERCRIMEN:
"La otra" delincuencia
¿Qué es el cibercrimen?
Crimen cometido en el espacio físico
Delincuencia física o material
Cibercriminalidad
Ámbito en el que se realiza la infracción
CRIMINA
Centro para el estudio y Prevención de la delincuencia

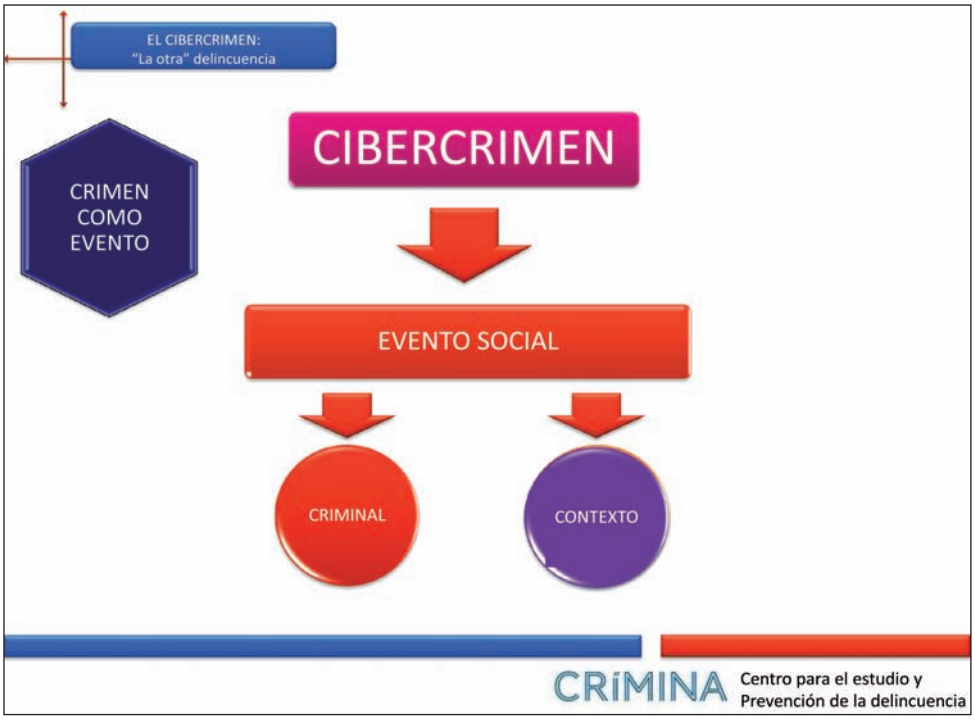

EL CIBERCRIMEN:
"La otra" delincuencia
¿Qué es el cibercrimen?
Espacio físico o material
Ciberespacio
CRIMINA
Centro para el estudio y Prevención de la delincuencia

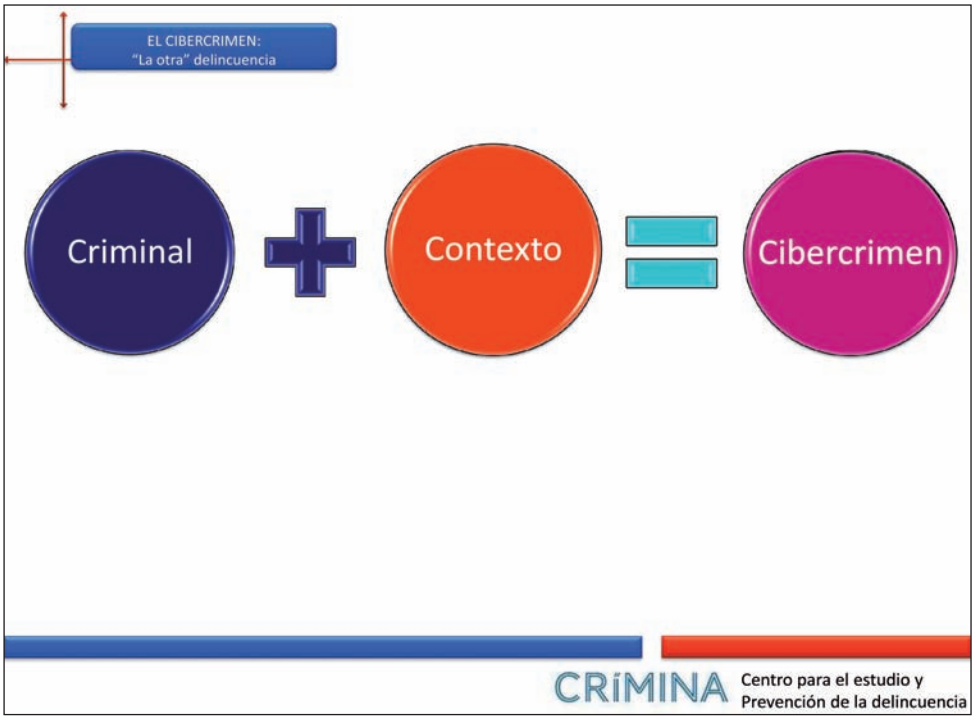

EL CIBERCRIMEN:
"La otra" delincuencia
¿Qué es el cibercrimen?
Delincuencia física o material
Cibercrimen
CRIMINA
Centro para el estudio y Prevención de la delincuencia

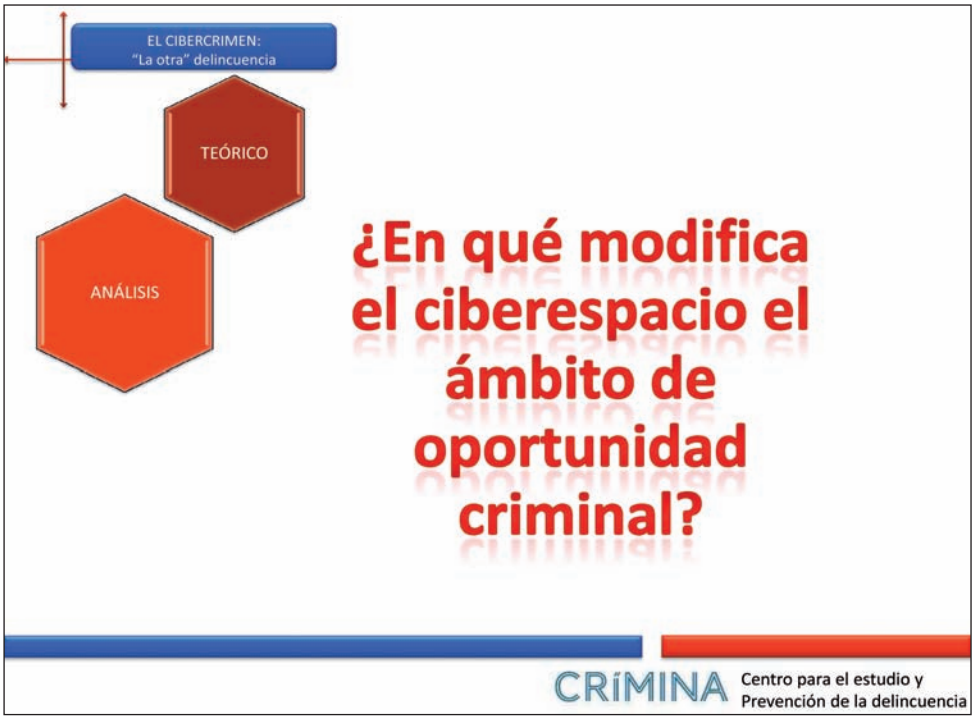

EL CIBERCRIMEN:
"La otra" delincuencia
¿Qué es el cibercrimen?
Todos los crímenes cometidos en el ámbito de intercomunicación personal que es el ciberespacio
CRIMINA
Centro para el estudio y Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
Cibercrímenes económicos
Cibercrímenes económicos mediales
Hacking
Malware
Spoofing
DoS
Spam
Cibercrímenes económicos finales
Ciberblanqueo de capitales
Ciberfraude
Pornografía infantil
Ciberespionaje
Ciberpiratería
CRIMINA
Centro para el estudio y Prevención de la delincuencia

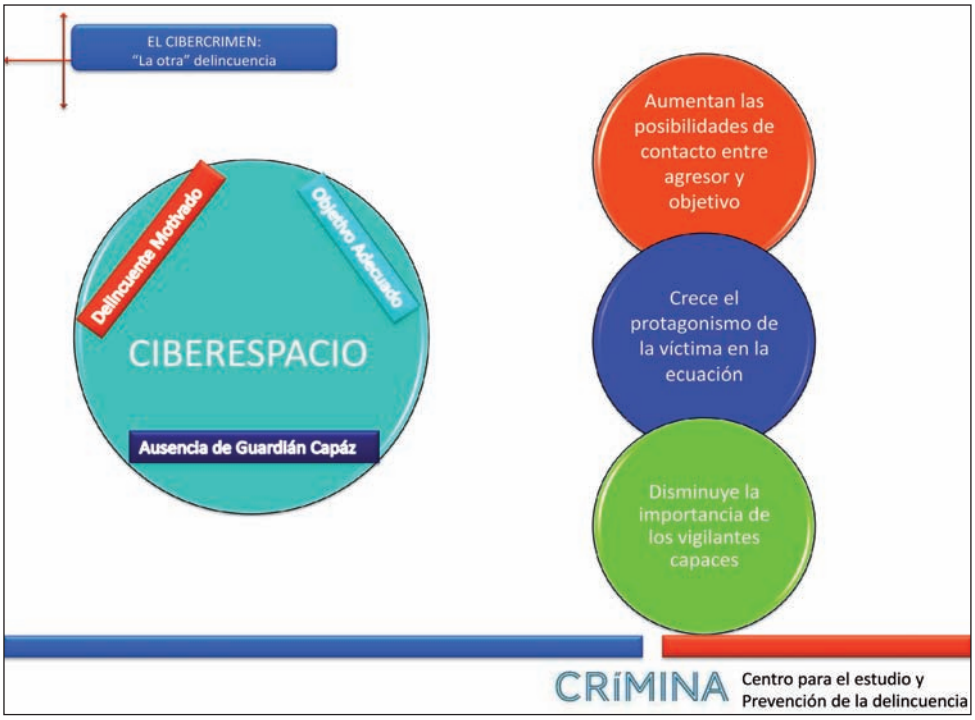

EL CIBERCRIMEN:
"La otra" delincuencia
Cibercrímenes políticos
Hatespeech
Cyberwar
Ataques DoS
Ciberterrorismo
Cibercrímenes sociales
Online Grooming
On line Harrassment
Sexting
Cyberstalking
Cyberbullying
CRIMINA
Centro para el estudio y Prevención de la delincuencia

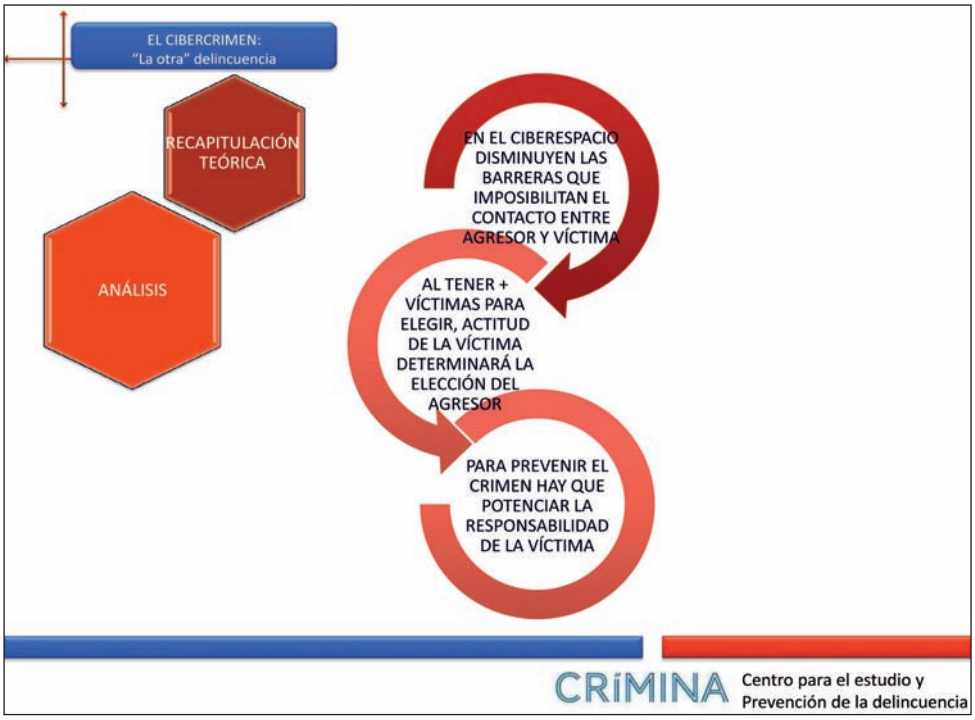

EL CIBERCRIMEN:
"La otra" delincuencia
CRIMEN COMO EVENTO
CIBERCRIMEN
EVENTO SOCIAL
CRIMINAL
CONTEXTO
CRIMINA
Centro para el estudio y Prevención de la delincuencia

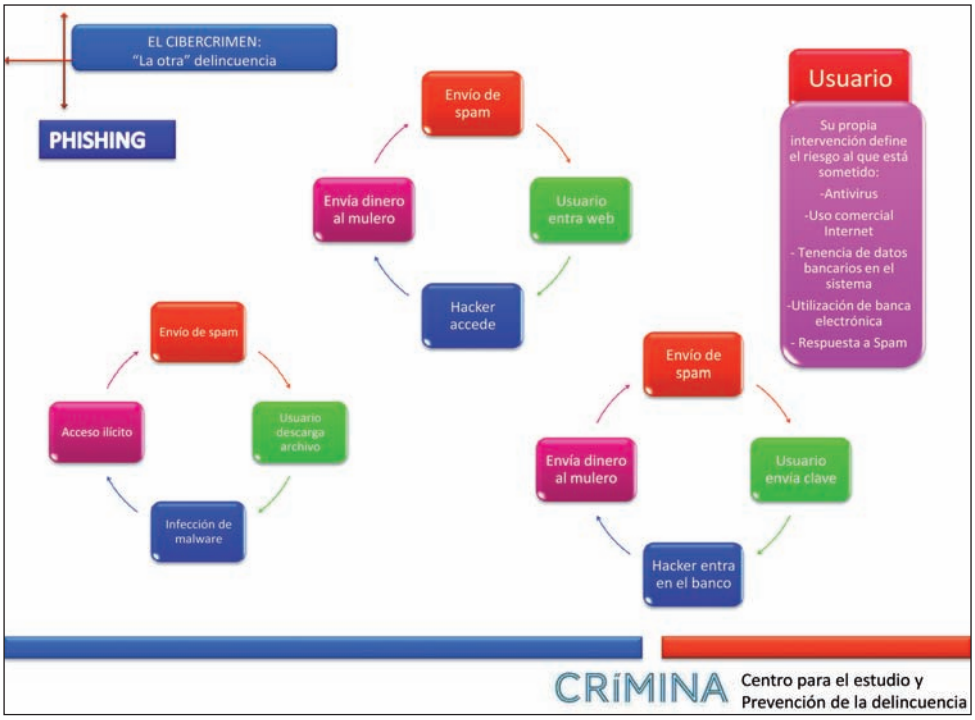

EL CIBERCRIMEN:
"La otra" delincuencia
Criminal
Contexto
Cibercrimen
CRíMINA
Centro para el estudio y
Prevención de la delincuencia

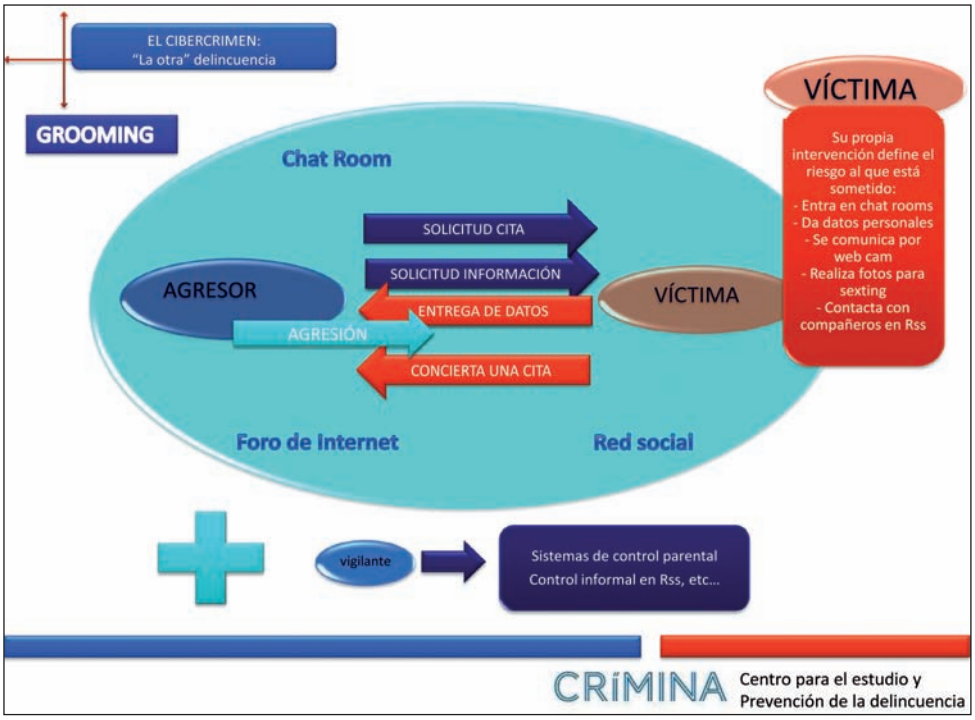

EL CIBERCRIMEN:
"La otra" delincuencia
TEÓRICO
ANÁLISIS
¿En qué modifica el ciberespacio el ámbito de oportunidad criminal?
CRíMINA
Centro para el estudio y
Prevención de la delincuencia

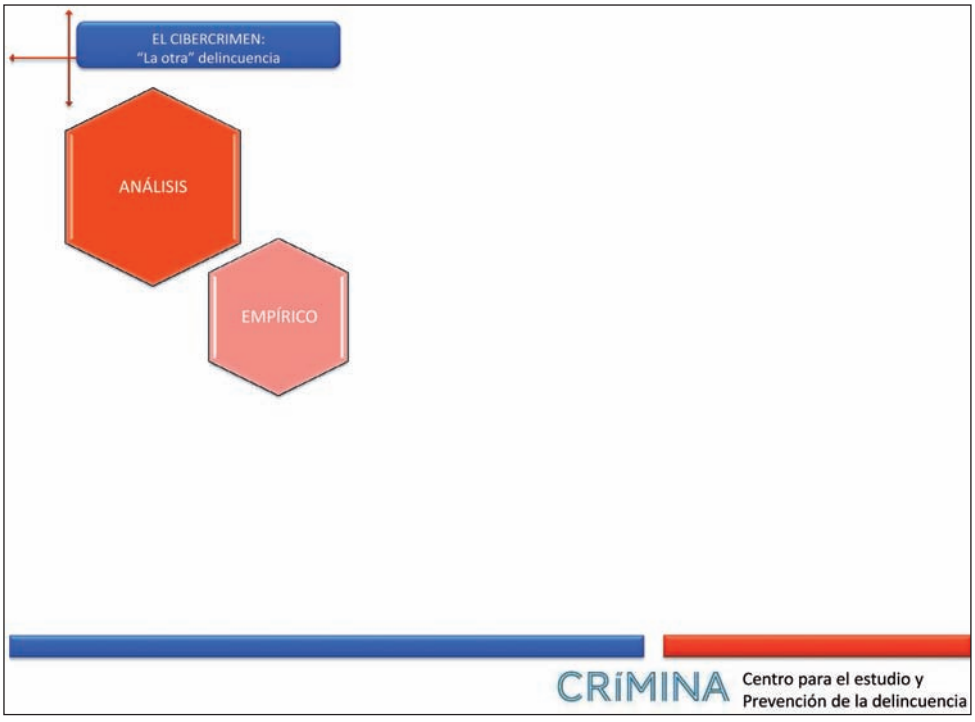

EL CIBERCRIMEN:
"La otra" delincuencia
Triángulo de la delincuencia (y de su prevención situacional)
Motivated offender
Suitable Target
CRIMEN
OPORTUNIDAD
Absence of Capable Guardian
CRíMINA
Centro para el estudio y
Prevención de la delincuencia

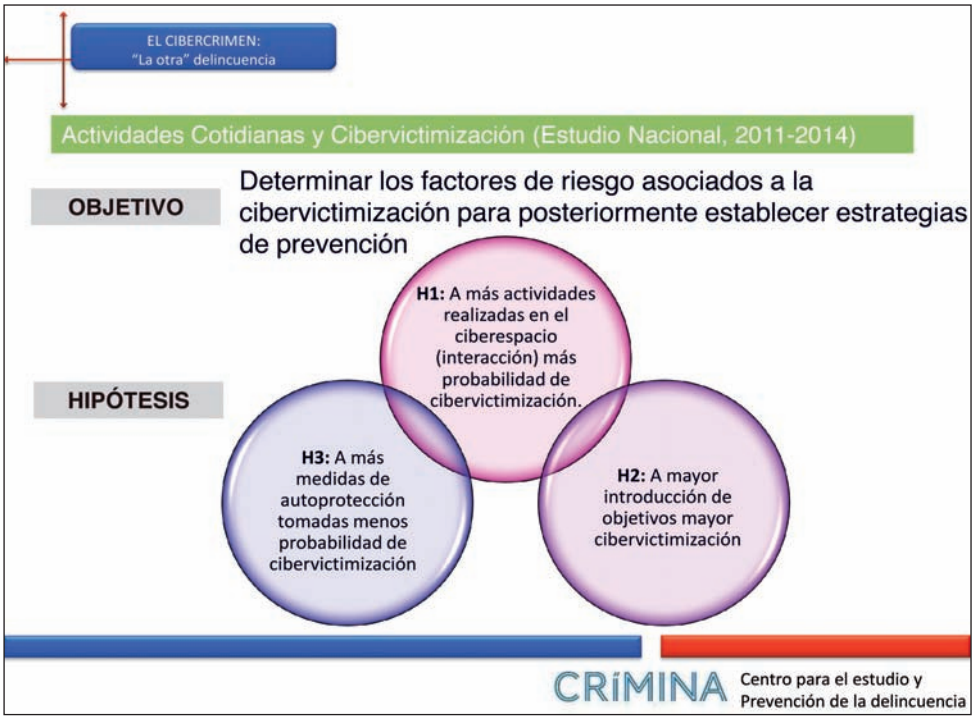

EL CIBERCRIMEN:
"La otra" delincuencia
Delincuente Motivado
Objetivo Adecuado
CIBERESPACIO
Ausencia de Guardián Capáz
Aumentan las posibilidades de contacto entre agresor y objetivo
Crece el protagonismo de la víctima en la ecuación
Disminuye la importancia de los vigilantes capaces
CRíMINA
Centro para el estudio y
Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
RECAPITULACIÓN TEÓRICA
ANÁLISIS
EN EL CIBERESPACIO DISMINUYEN LAS BARRERAS QUE IMPOSIBILITAN EL CONTACTO ENTRE AGRESOR Y VÍCTIMA
AL TENER + VÍCTIMAS PARA ELEGIR, ACTITUD DE LA VÍCTIMA DETERMINARÁ LA ELECCIÓN DEL AGRESOR
PARA PREVENIR EL CRIMEN HAY QUE POTENCIAR LA RESPONSABILIDAD DE LA VÍCTIMA
CRIMINA
Centro para el estudio y Prevención de la delincuencia

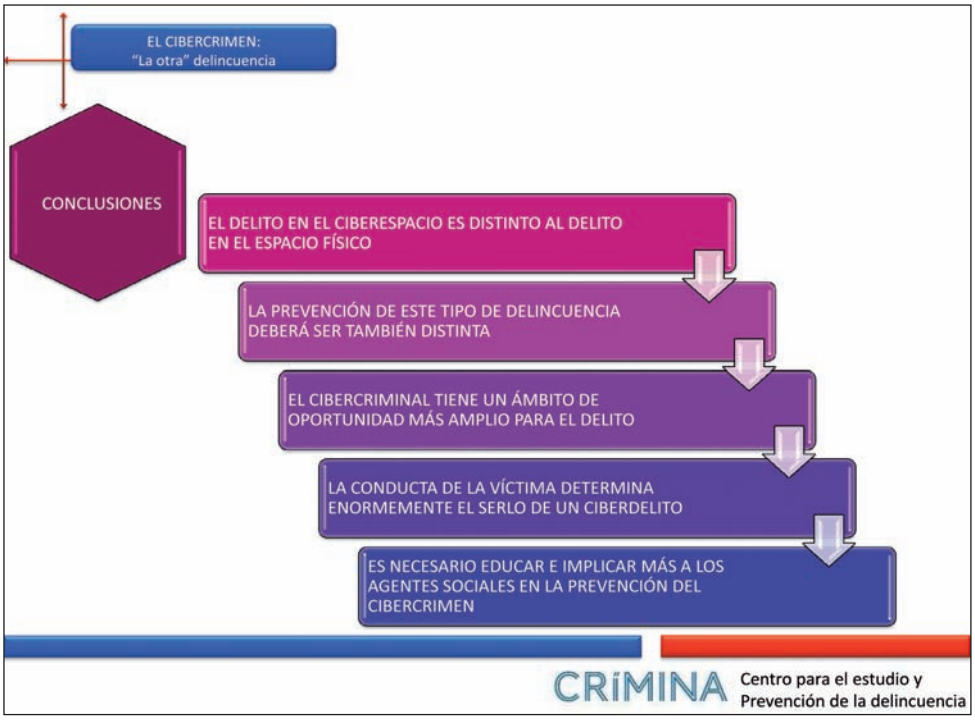

EL CIBERCRIMEN:
"La otra" delincuencia
PHISHING
Envío de spam
Usuario entra web
Hacker accede
Envía dinero al mulero
Usuario
Su propia intervención define el riesgo al que está sometido:
-Antivirus
-Uso comercial Internet
- Tenencia de datos bancarios en el sistema
-Utilización de banca electrónica
- Respuesta a Spam
Envío de spam
Usuario descarga archivo
Infección de malware
Acceso ilícito
Envío de spam
Usuario envía clave
Hacker entra en el banco
Envía dinero al mulero
CRIMINA
Centro para el estudio y Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
GROOMING
Chat Room
SOLICITUD CITA
SOLICITUD INFORMACIÓN
ENTREGA DE DATOS
AGRESIÓN
CONCIERTA UNA CITA
AGRESOR
VÍCTIMA
Foro de Internet
Red social
VÍCTIMA
Su propia intervención define el riesgo al que está sometido:
- Entra en chat rooms
- Da datos personales
- Se comunica por web cam
- Realiza fotos para sexting
- Contacta con compañeros en Rss
vigilante
Sistemas de control parental
Control informal en Rss, etc...
CRíMINA
Centro para el estudio y Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
ANÁLISIS
EMPÍRICO
CRíMINA
Centro para el estudio y Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
Actividades Cotidianas y Cibervictimización (Estudio Nacional, 2011-2014)
OBJETIVO
Determinar los factores de riesgo asociados a la cibervictimización para posteriormente establecer estrategias de prevención
HIPÓTESIS
H1: A más actividades realizadas en el ciberespacio (interacción) más probabilidad de cibervictimización.
H3: A más medidas de autoprotección tomadas menos probabilidad de cibervictimización
H2: A mayor introducción de objetivos mayor cibervictimización
CRíMINA
Centro para el estudio y Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
FACTORES DE RIESGO
RESULTADOS
A más INTERACCIÓN más CIBERVICTIMIZACIÓN
A más INTRODUCCIÓN más CIBERVICTIMIZACIÓN
A menor AUTOPROTECCIÓN más CIBERVICTIMIZACIÓN
Contactar con desconocidos a través de Internet
Uso del correo electrónico
Realizar compras por Internet
Consumir pornografía online
Uso de mensajería instantánea
Uso de chat
Escribir en foros
Uso de redes sociales
Realizar videoconferencias
Realizar movimientos bancarios
Realizar descargas
Tener fotos personales en el ordenador
Facilitar información personal a través de Internet
Tener un archivo con las contraseñas en el ordenador
Tener vídeos personales en el ordenador
Tener información de la empresa
Abrir o descargar enlaces o archivos enviados por desconocidos
Uso de software pirata
No poseer antivirus en el ordenador que se conecta a Internet
Usar la misma contraseña o similar para todo
Cambiar las contraseñas mínimo una vez al año
CRíMINA
Centro para el estudio y Prevención de la delincuencia


EL CIBERCRIMEN:
"La otra" delincuencia
CONCLUSIONES
EL DELITO EN EL CIBERESPACIO ES DISTINTO AL DELITO EN EL ESPACIO FÍSICO
LA PREVENCIÓN DE ESTE TIPO DE DELINCUENCIA DEBERÁ SER TAMBIÉN DISTINTA
EL CIBERCRIMINAL TIENE UN ÁMBITO DE OPORTUNIDAD MÁS AMPLIO PARA EL DELITO
LA CONDUCTA DE LA VÍCTIMA DETERMINA ENORMEMENTE EL SERLO DE UN CIBERDELITO
ES NECESARIO EDUCAR E IMPLICAR MÁS A LOS AGENTES SOCIALES EN LA PREVENCIÓN DEL CIBERCRIMEN
CRÍMINA
Centro para el estudio y Prevención de la delincuencia


MUCHAS GRACIAS.....
XXIII SEMINARIO "DUQUE DE AHUMADA"
"CIBERAMENAZAS Y REDES SOCIALES"
Prof. Dr. Fernando Miró Llinares
www.crimina.es
CRÍMINA

Síntesis legislativa

Ponencia de D. Antolín Herrero Ortega
Fiscal Jefe de Sala de la Fiscalía del Tribunal Supremo

El Ponente ingresó en la Carrera Fiscal en 1977 y ha desempeñado entre otros puestos los de Fiscal de la Audiencia Territorial de Madrid, Fiscal Jefe de la Audiencia Provincial de Guadalajara, Teniente Fiscal del Tribunal Superior de Justicia de Madrid y Fiscal del Tribunal Supremo. Desde enero de 2005 era Fiscal de Sala del Tribunal Supremo.

SÍNTESIS DE LEGISLACIÓN DE CIBERDELINCUENCIA

1. Ley de Enjuiciamiento Criminal. Art. 579, redacción L.O 4/1988, de 25 de mayo
2. Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001
3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
4. DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).
5. Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
6. DIRECTIVA 2006/24/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
7. Ley 25/2007, de 18 de octubre 2007. Ley Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

8. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

9. Ley 2/2011, de 4 de marzo, de Economía Sostenible. Disposición final cuadragésima tercera. Modificación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, el Real Decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, para la protección de la propiedad intelectual en el ámbito de la sociedad de la información y de comercio electrónico.

Las disposiciones que se extractan a continuación, en los aspectos que se relacionan, tienen como objetivo provocar una reflexión sobre si los instrumentos legales puestos a disposición de instituciones judiciales, fiscales y unidades de policía judicial de las Fuerzas y Cuerpos de Seguridad son suficientemente nítidos para el eficaz desarrollo de investigación y enjuiciamiento de delitos informáticos, en sentido amplio, o por el contrario contienen espacios de inseguridad del marco jurídico que regula tales instrumentos.

Es obligado deber, aprovechar la ocasión, para agradecer la colaboración de la Unidad de Policía Judicial de la Guardia Civil, dirigida por el General Rico, en la etapa en que por designación del Fiscal General del Estado, desempeñé el cargo de Delegado para delincuencia informática, cuya ayuda para la formación de los Fiscales en materia de investigación y formación técnica resultó extremadamente fructífera.

2. Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001.

8. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Madrid 20 de mayo de 2010.

Capítulo I. Terminología

Artículo 1. Definiciones

A los efectos del presente Convenio, la expresión:

a) *«Sistema informático»* designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos.

b) *«Datos informáticos»* designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función.

c) *«Prestador de servicio»* designa:

i. Toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático.

ii. Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios.

(El Convenio recoge, en la versión francesa, la expresión «fournisser de services», cuya traducción literal sería la de «proveedor de servicios». En la presente traducción, se ha optado por emplear el término «prestador de servicios», en la línea seguida por la Directiva 2000/31 y el Proyecto de LSSI, como concepto o categoría omnicomprensiva que hace referencia a aquellos sujetos que desempeñan, profesionalmente, la actividad de prestación y gestión de accesos y servicios en Internet.)

d) «Datos de tráfico» designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II. Medidas que deben ser adoptadas a nivel nacional

Sección 1. Derecho penal material

Título 1. Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2. Acceso ilícito.

Artículo 3. Interceptación ilícita.

Artículo 4. Atentados contra la integridad de los datos.

Artículo 5. Atentados contra la integridad del sistema.

Artículo 6. Abuso de equipos e instrumentos técnicos.

Título 2. Infracciones informáticas

Artículo 7. Falsedad informática.

Artículo 8. Estafa informática.

Título 3. Infracciones relativas al contenido

Artículo 9. Infracciones relativas a la pornografía infantil.

Título 4. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

Título 5. Otras formas de responsabilidad y sanción

Artículo 11. Tentativa y complicidad.

Artículo 12. Responsabilidad de las personas jurídicas.

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un

órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:

a) Un poder de representación de la persona jurídica.

b) Una autorización para tomar decisiones en nombre de la persona jurídica.

c) Una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, los Estados firmantes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en *sede penal,* civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

TÍTULO I

Disposiciones Generales

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

TÍTULO II

Principios de la protección de datos

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por *destinatario* al *Defensor del Pueblo,* el *Ministerio Fiscal* o los *Jueces* o *Tribunales* o el *Tribunal de Cuentas,* en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la *represión de infracciones penales,* debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

6. DIRECTIVA 2006/24/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de marzo de 2006, sobre la *conservación de datos* generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

De conformidad con el procedimiento establecido en el artículo 251 del Tratado,

Considerando lo siguiente:

(9) De conformidad con el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), toda persona tiene derecho al respeto de su vida privada y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de ese derecho salvo cuando esa injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o *delitos,* o la protección de los derechos y las libertades de terceros. Dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva. Por consiguiente, la adopción de un instrumento de conservación de datos que cumpla los requisitos del artículo 8 del CEDH es una medida necesaria.

(17) Es esencial que los Estados miembros adopten medidas legislativas para asegurar que los datos conservados de conformidad con la presente Directiva solamente se faciliten a las *autoridades nacionales competentes de conformidad con la legislación nacional,* respetando plenamente los derechos fundamentales de las personas afectadas.

(21) Dado que los objetivos de la presente Directiva, a saber, armonizar las obligaciones de los proveedores de conservar determinados datos y asegurar que éstos estén disponibles con fines de investigación, detección y *enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado* miembro, como el terrorismo y la delincuencia organizada, no pueden ser alcanzados de manera suficiente por los Estados miembros y, debido a la dimensión y los efectos de la presente Directiva, pueden lograrse mejor a nivel comunitario, la Comunidad puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado. De conformidad con el principio de *proporcionalidad* enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

Artículo 1

Objeto y ámbito

1. La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y *enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado* miembro.

Artículo 4

Acceso a los datos

Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las *autoridades nacionales competentes,* en casos específicos y de conformidad con la legislación nacional.

Artículo 6

Períodos de conservación

Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de *tiempo* que *no* sea *inferior a seis meses ni superior a dos años* a partir de la fecha de la comunicación.

7. Ley 25/2007, de 18 de octubre 2007. Ley Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

PREÁMBULO

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo (LCEur 2006\820), sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio (LCEur 2002\2070), cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por *agentes facultados* los miembros de los Cuerpos Policiales autorizados para ello en el marco de una *investigación criminal* por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la *privacidad y la intimidad* de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el *derecho al secreto de las comunicaciones,* ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero *en ningún caso reveladores del contenido de ésta;* y, en segundo lugar, que la cesión de tales

datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por *delitos graves,* definidos éstos de acuerdo con la *legislación interna de cada Estado* miembro.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de *doce meses* desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

Artículo 1. Objeto de la Ley.

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente *autorización judicial* con fines de detección, investigación y enjuiciamiento de *delitos graves* contemplados en el *Código Penal* o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios *para identificar al abonado* o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. Sujetos obligados.

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos* objeto de conservación.

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación: ...

b) Datos necesarios para identificar el destino de una comunicación: ...

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación: ...

d) Datos necesarios para identificar el tipo de comunicación. ...

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación: ...

f) Datos necesarios para identificar la localización del equipo de comunicación móvil: ...

Artículo 4. Obligación de conservar datos.

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. Período de conservación de los datos.

1. La obligación de conservación de datos impuesta cesa a los *doce meses* computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

Artículo 6. Normas generales sobre cesión de datos.

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y *previa autorización judicial*.

2. La cesión de la información se efectuará únicamente a los agentes facultados.

A estos efectos, tendrán la consideración de *agentes facultados:*

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia.

Artículo 7. Procedimiento de cesión de datos.

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La *resolución judicial* determinará, conforme a lo previsto en la *Ley de Enjuiciamiento Criminal* y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8.00 horas del día laborable siguiente a aquel en que el sujeto obligado reciba la orden.

Disposición Final primera. Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones*.

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos *18.3* y 55.2 de la *Constitución,* debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las *interceptaciones* que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de *ley orgánica*. Asimismo, deberán

adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de *vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles*. El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los *datos* indicados en la orden de *interceptación* legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación. Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de *cualquiera de las partes* que intervengan en la comunicación que sean *clientes* del sujeto obligado, los siguientes *datos:*

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones, y, aunque *no* sea *abonado,* si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la *situación geográfica* del terminal o punto de terminación de red *origen* de la llamada, y de la del *destino* de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la *estación base* afectada.

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los *abonados* con sus números de documento nacional de *identidad,* tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles. Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación».

9. Ley 2/2011, de 4 de marzo, de Economía Sostenible. Disposición final cuadragésima tercera.

Modificación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, el Real Decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, para la protección de la propiedad intelectual en el ámbito de la sociedad de la información y de comercio electrónico.

Uno. Se introduce una nueva letra e) en el artículo 8.1 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico con el siguiente tenor:

«e) La salvaguarda de los derechos de propiedad intelectual.»

Dos. Se introduce un nuevo apartado segundo del artículo 8 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, con renumeración correlativa de los actuales 2, 3, 4 y 5:

«2. Los órganos competentes para la adopción de las medidas a que se refiere el apartado anterior, con el objeto de *identificar al responsable del servicio* de la sociedad de la información que está realizando la conducta presuntamente vulneradora, podrán requerir a los prestadores de servicios de la sociedad de la información la cesión de los datos que permitan tal identificación a fin de que pueda comparecer en el procedimiento. Tal requerimiento exigirá la *previa autorización judicial* de acuerdo con lo previsto en el apartado primero del artículo 122 bis de la Ley reguladora de la Jurisdicción contencioso-administrativa. Una vez obtenida la autorización, los prestadores estarán obligados a facilitar los datos necesarios para llevar a cabo la identificación.»

Tres. Se introduce una disposición adicional quinta en el Texto Refundido de la *Ley de Propiedad Intelectual,* aprobado por el Real Decreto legislativo 1/1996, de 12 de abril, con la siguiente redacción:

«El Ministerio de Cultura, en el ámbito de sus competencias, velará por la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de servicios de la sociedad de información en los términos previstos en los artículos 8 y concordantes de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.»

Cuatro. Se modifica el artículo 158 del Texto Refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto legislativo 1/1996, de 12 de abril con la siguiente redacción:

«Artículo 158. *Comisión* de Propiedad Intelectual.

1. Se crea en el *Ministerio de Cultura* la Comisión de Propiedad Intelectual, como órgano colegiado de ámbito nacional, para el ejercicio de las funciones de mediación y arbitraje, y de salvaguarda de los derechos de propiedad intelectual que le atribuye la presente Ley.

2. La Comisión actuará por medio de dos Secciones.

La Sección Primera ejercerá las funciones de mediación y arbitraje que le atribuye la presente Ley.

La Sección Segunda velará, en el ámbito de las competencias del Ministerio de Cultura, por la *salvaguarda de los derechos de propiedad intelectual* frente a su vulneración por los responsables de servicios de la sociedad de información en los términos previstos en los artículos 8 y concordantes de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

3. Corresponde a la Sección Segunda, que actuará conforme a los principios de objetividad y proporcionalidad, el ejercicio de las funciones previstas en los artículos 8 y concordantes de la Ley 34/2002, para la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de servicios de la sociedad de información.

La Sección podrá adoptar las medidas para que se interrumpa la prestación de un servicio de la sociedad de la información que vulnere derechos de propiedad intelectual o para retirar los contenidos que vulneren los citados derechos siempre que el prestador, directa o indirectamente, actúe con ánimo de lucro o haya causado o sea susceptible de causar un daño patrimonial.

Antes de proceder a la adopción de estas medidas, el prestador de servicios de la sociedad de la información deberá ser requerido a fin de que en un plazo no superior a las 48 horas pueda proceder a la retirada voluntaria de los contenidos declarados infractores o, en su caso, realice las alegaciones y proponga las pruebas que estime oportunas sobre la autorización de uso o la aplicabilidad de un límite al derecho de Propiedad Intelectual. Transcurrido el plazo anterior, en su caso, se practicará prueba en dos días y se dará traslado a los interesados para conclusiones en plazo máximo de cinco días. La Comisión en el plazo máximo de tres días dictará resolución. La retirada voluntaria de los contenidos pondrá fin al procedimiento. En todo caso, la ejecución de la medida *ante el incumplimiento del requerimiento exigirá de la previa autorización judicial,* de acuerdo con el procedimiento regulado en el apartado segundo del artículo 122 bis de la Ley reguladora de la Jurisdicción Contencioso-Administrativa.

Lo dispuesto en este apartado se entiende *sin perjuicio de las acciones* civiles, *penales* y contencioso-administrativas que, en su caso, sean procedentes.

La Sección, bajo la presidencia del Subsecretario del Ministerio de Cultura o persona en la que éste delegue, se compondrá de un vocal del Ministerio de Cultura, un vocal del Ministerio de Industria, Turismo y Comercio, un vocal del Ministerio de Economía y Hacienda y un vocal del Ministerio de la Presidencia.

Reglamentariamente se determinará el funcionamiento de la Sección y el procedimiento para el ejercicio de las funciones que tiene atribuidas.

El procedimiento para el restablecimiento de la legalidad, que se iniciará siempre a instancia del titular de los derechos de propiedad intelectual que se consideran vulnerados o de la persona que tuviera encomendado su ejercicio y en el que serán de aplicación los

derechos de defensa previstos en el artículo 135 de la Ley 30/1992, estará basado en los principios de celeridad, proporcionalidad y demás previstos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La falta de resolución en el plazo reglamentariamente establecido tendrá efectos desestimatorios de la solicitud. Las resoluciones dictadas por la Comisión en este procedimiento ponen fin a la vía administrativa.»

Cinco. Se modifica el artículo 9 de la *Ley* 29/1998, de 13 de julio, reguladora de la Jurisdicción *Contencioso-administrativa,* numerando su texto actual como apartado 1 y añadiendo un apartado 2, con el contenido siguiente:

«2. Corresponderá a los *Juzgados Centrales* de lo Contencioso-Administrativo, la autorización a que se refiere el artículo 8.2 de la Ley 34/2002 así como autorizar la ejecución de los actos adoptados por la Sección Segunda de la Comisión de Propiedad Intelectual para que *se interrumpa* la prestación de servicios de la sociedad de la información o para que *se retiren* contenidos que vulneren la propiedad intelectual, en aplicación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la información y de Comercio Electrónico.»

Seis. Se modifica la letra d) del apartado 1 del artículo 80 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, con el siguiente tenor:

«d) Los recaídos sobre las autorizaciones previstas en el artículo 8.6 y en los artículos 9.2 y 122 bis.»

Siete. Se introduce un nuevo artículo 122 bis en la Ley 29/1998, de 13 de abril, reguladora de la Jurisdicción Contencioso-administrativa, con el siguiente tenor:

«1. El procedimiento para obtener la autorización judicial a que se refiere el artículo 8.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, se iniciará con la solicitud de los órganos competentes en la que se expondrán las razones que justifican la petición acompañada de los documentos que sean procedentes a estos efectos. El Juzgado, en el plazo de 24 horas siguientes a la petición y, *previa audiencia del Ministerio Fiscal,* dictará resolución autorizando la solicitud efectuada siempre que no resulte afectado el artículo 18 apartados 1 y 3 de la Constitución.

2. La ejecución de las medidas para que se interrumpa la prestación de servicios de la sociedad de la información o para que se retiren contenidos que vulneren la propiedad intelectual, adoptadas por la Sección Segunda de la Comisión de Propiedad Intelectual en aplicación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la información y de Comercio Electrónico, requerirá de autorización judicial previa de conformidad con lo establecido en los párrafos siguientes.

Acordada la medida por la Comisión, solicitará del Juzgado competente la autorización para su ejecución, referida a la posible afectación a los derechos y libertades garantizados en el artículo 20 de la Constitución.

En el plazo improrrogable de dos días siguientes a la recepción de la notificación de la resolución de la Comisión y poniendo de manifiesto el expediente, el Juzgado convoca-

rá al representante legal de la Administración, al Ministerio Fiscal y a los titulares de los derechos y libertades afectados o a la persona que éstos designen como representante a una audiencia, en la que, de manera contradictoria, el Juzgado oirá a todos los personados y resolverá en el plazo improrrogable de dos días mediante auto. La decisión que se adopte únicamente podrá autorizar o denegar la ejecución de la medida.»

La jurisprudencia de la Sala de lo Penal del Tribunal Supremo puede resultar suficientemente expresiva de la complejidad legislativa en la materia.

Pleno de la Sala 2.ª del Tr. Supremo de 20/01/10.

SEGUNDO ASUNTO: Si el Ministerio Fiscal precisa de la autorización judicial para que le sea desvelada la identidad de la persona adjudicataria de la dirección IP con la que operan los ciudadanos en Internet.

ACUERDO: Es necesaria la *autorización judicial* para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio fiscal precisara de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre.

Sentencia: N.º: 247/2010

Fecha Sentencia: 18/03/2010

"Como quiera que la Guardia Civil no podía conocer los datos de filiación del titular o titulares de aquellas dos direcciones de la IP antes reseñadas, solicitó de la Fiscalía del Tribunal Superior de Justicia de Cataluña que acordara requerir a la empresa (Net-Arsys-Euro2) para que ésta proporcionara a dicha Fiscalía cuantos datos obraran en su poder sobre el usuario o usuarios a los que le fueron asignadas esas dos direcciones IP, así como el número de teléfono desde el cual se hicieron unas conexiones de Internet determinadas, indicando la hora de inicio y de finalización de cada una de las conexiones, así como la titularidad del teléfono o teléfonos desde los que se habrían hecho las conexiones.

La mencionada Fiscalía accedió a dicha solicitud de la Guardia Civil y en las diligencias preprocesales número 350/06 acordó requerir a aquella entidad mercantil para que proporcionara tales datos de dicho usuario o usuarios, y efectivamente Net-Arsys-Euro2) indicó a la Fiscalía que el nombre del usuario de tales direcciones de IP era A.V. con número de identificación X 5014103B, con domicilio en la calle H... de Vitoria-Gasteiz y con el número de teléfono contacto a Internet número 945 ...

La referida Fiscalía, con los datos suministrados por la empresa Net-Arsys-Euro2 (y los extraídos de los oficios remitidos por otras empresas de telefonía), presentó una denuncia en los Juzgados de Instrucción de Barcelona, que fue repartida al Juzgado de Instrucción número 27 de esa ciudad, que incoó las Diligencias Previas con número de registro 5472/2006, formando una pieza separada respecto de las actuaciones relativas a A... V....

"La Ley 25/2007, tiene muy en cuenta el campo aplicativo de la *Ley Orgánica* n.º 15 de 1999 de Protección de Datos de carácter personal y le reconoce su mayor rango, aunque en el ámbito de vigencia de la Ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, se erigía como preferente esta *Ley,* por la materia *específica* a la que se refería, esto es, a las comunicaciones, su contenido y todos los datos externos o de tráfico que de modo exhaustivo enumera la ley.

Prueba del respeto que muestra la Ley 25/2007 a las previsiones normativas de la Ley de Protección de Datos, es que la menciona en multitud de ocasiones, incluida la exposición de motivos. A título de ejemplo el art. 8 la cita hasta cuatro veces, estableciendo, entre otras cosas, que *"las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999 de 13 de diciembre y su normativa de desarrollo"*. Y a continuación declara el mismo art. 8 que *"El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999 de 13 de diciembre y en su normativa de desarrollo"*.

Pero independientemente de que ambas leyes operen en ámbitos diferentes, no excluye la posibilidad de producirse ciertas coincidencias o *colisiones,* sobre todo cuando se relacionan con el derecho fundamental al secreto de las comunicaciones regulado en el art. 18-3 C.E.

La Sala General no jurisdiccional aprobó el 23 de febrero de 2010 el siguiente acuerdo: *"Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el M.º Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007 de 18 de octubre"*.

Las sentencias 236/2008 de 9 de mayo y la 292/08 de 28 de mayo, condensan los principios o criterios a tener en cuenta, como en su momento dijimos. Recordemos las más importantes afirmaciones de la primera de ellas:

"Planteado así el problema, se hace preciso o cuando menos conveniente esbozar un esquema de los criterios legales y jurisprudenciales en orden a la calificación de la actuación policial de acuerdo con la legalidad procesal y constitucional.

En este sentido y en cuanto al alcance del contenido del derecho al secreto de las comunicaciones previsto en el art. 18-3 C.E., la sentencia recurrida concreta acertadamente su alcance material, circunstancia que concuerda con las tesis del Fiscal recurrente.

Desde la sentencia del Tribunal Constitucional nº 123 de 20 de mayo de 2002, se establece, haciéndose eco del caso Malone (2-8-82), resuelto por el Tribunal de Estrasburgo de Derechos Humanos, que la obtención del ***listado de llamadas*** *hechas por los usuarios mediante el mecanismo técnico utilizado por las compañías telefónicas constituye una injerencia en el derecho fundamental al secreto de las comunicaciones reconocido en el art. 8 del Convenio Europeo, equivalente al 18-3 C.E. En cuanto el concepto de secreto de*

la comunicación no sólo cubre su contenido, sino otros aspectos de la comunicación, como la ***identidad subjetiva de los interlocutores.*** *Consecuentemente podemos afirmar que el secreto a las comunicaciones telefónicas garantiza también la confidencialidad de los comunicantes, esto es, alcanzaría no sólo al secreto de la existencia de la comunicación misma y el contenido de lo comunicado, sino a la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino..... Hasta este nivel discursivo existe coincidencia entre la posición del tribunal de instancia y el M.º Fiscal".*

La sentencia referida sigue diciendo: *"Queda en pie la duda, de si para solicitar el número telefónico o identidad de un titular de un terminal telefónico o un IP, es necesario acudir a la autorización judicial, si no han sido positivas las actuaciones policiales legítimas integradas por injerencias leves y proporcionadas, que puede respaldar la Ley Orgánica de Cuerpos y Fuerzas de Seguridad del Estado o Ley de Seguridad Ciudadana, en la misión de los agentes de descubrir delitos y perseguir a los delincuentes.*

A nuestro juicio, sin pretensiones ni mucho menos de sentar doctrina (obiter dicta), los ***datos identificativos*** *de un titular o de un terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (art. 18-3 C.E.) sino en el marco del derecho a la* ***intimidad*** *personal (art. 18.1º C.E.) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal, L.O. 15/1999 de 13 de diciembre: art. 11.2 d. o su Reglamento, Real-Decreto 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin despreciar la Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, R.D. 424 de 15 de abril de 2005, en los que parece desprenderse que sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de inv estigación penal".*

La correcta interpretación de esta doctrina nos debe llevar a la distinción de cuándo unos datos personales pueden afectar al secreto a las comunicaciones y cuándo, conservados y tratados por las Operadoras, no se están refiriendo a comunicación alguna, es decir, datos estáticamente almacenados, conservados y tratados por operadores que se hallan obligados a la reserva frente a terceros.

Distinguimos pues dos conceptos:

a) datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el art. 18-3 C.E:

b) datos o circunstancias personales referentes a la intimidad de una persona (art. 18-1º C.E.), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o habeas data del art. 18-4 C.E. que no pueden comprometer un proceso de comunicación.

Desde esta perspectiva dicotómica la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un *auténtico desenfoque* del problema, pues incorporaría en el

ámbito de la protección constitucional del art. 18-3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la autodeterminación informática del art. 18-4 C.E. (véase por todas S.T.S. n.º 249 de 20-5-2008).

En el caso concernido es patente que los datos cuyo obtención se pretende por el Fiscal no tienen relación ni afectan ni interceptan ni descubren ni tratan de descubrir una comunicación concreta, sino que por ser preciso para la acción investigadora el conocimiento del domicilio, número de teléfono o identidad del titular del terminal informático que opera en la Red (I.P.), la solicita a la operadora, al objeto de pedir del juez un mandamiento de entrada y registro con fines indagatorios o de investigación de un posible delito, acerca del que se conocen datos indiciarios.

El M.º Fiscal se hallaba en el ejercicio de sus funciones, entre otras, promover la acción de la justicia (art. 126 C.E. y art. 3 de su Estatuto Orgánico) y también investigando los hechos delictivos, dentro del marco de unas diligencias preprocesales de naturaleza criminal (art. 773-2 L.E.Cr.).

Tal proceder del M.º Fiscal *no afecta al secreto de las comunicaciones* sino que se desenvuelve en el marco del derecho a la intimidad, más concretamente, dada la escasa intensidad en que es efectuada, la cuestión se proyectaría sobre la obligación que establece la Ley Orgánica de Protección de Datos de no publicar los datos personales de los usuarios que un servidor de Internet posee, los cuales no pueden cederse sin el consentimiento del titular, pero la ley establece diversas excepciones.

Así el art. 11.2 d) de la Ley Orgánica 15/1999 de 13 de diciembre nos dice que el consentimiento del interesado a que se refiere el párrafo anterior no será necesario.... d) *"Cuando la comunicación que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tienen atribuidas"*.

Por su parte la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones, cuyo articulado se remite al art. 12 de la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (ahora derogada por la Ley 25/2007) se establece el deber de retención de datos de tráfico relativos a las comunicaciones electrónicas en cuyo n.º 3 nos dice que los *"datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguarda de la seguridad pública y la defensa nacional, poniéndola a disposición de los jueces o tribunales o del Ministerio Fiscal que así lo requieran"*.

Finalmente la propia Agencia de Protección de Datos, órgano público de carácter autónomo que conforme al art. 37.1. a) de la L.O. 15/1999, tiene por misión *"velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos, ha dicho en sus informes 135/2003 y 297/2005 que en los supuestos a que se refiere el art. 11.2 la cesión de datos personales no está sujeta a reserva jurisdiccional"*.

Por todo ello entendemos que el Fiscal tiene facultades de investigación paralelas a las del juez de instrucción en el Procedimiento Abreviado (art. 773-2 L.E.Cr.) y salvo los actos injerenciales en los derechos fundamentales y la adopción de medidas cautelares posee las mismas atribuciones y responsabilidades que un juez. Si el juez instructor no hubiera estimado pertinente la adopción de la medida de entrada y registro los datos se archivarían, sin haber salido del ámbito de disponibilidad y reserva de la autoridad encargada de la investigación criminal (bien se trate del Fiscal o del Juez).

Pero es que la decisión de invadir el domicilio particular de una persona no provenía de haber desvelado su identidad, ya que ello era absolutamente secundario o anodino; el juez acordó la entrada y registro valorando la necesidad, utilidad y proporcionalidad de la medida de acuerdo con los datos aportados por la policía indiciarios de la comisión de un delito grave, y la medida interesada, fuera quien fuera el titular del terminal, solo tenía por objeto el desvelamiento del nombre de la persona física o jurídica que contrató con el operador de Internet y le asignó un I.P. encriptado en una clave alfanumérica

Ni que decir tiene que este régimen jurídico *sólo es aplicable antes de la ley 25/2007* de 18 de octubre; con posterioridad a su vigencia debemos estar al acuerdo del Pleno no jurisdiccional de esta Sala de 23 de febrero de 2010.

En atención a lo expuesto parece ser que la Audiencia confunde el derecho al secreto de las comunicaciones (art. 18-3 C.E.), el derecho a la intimidad (art. 18-1 C.E.) y la obligación de conservar secretos los datos informáticos personales (art. 18-4 C.E.) conforme a la Ley Orgánica de Protección de Datos de carácter personal, que excepciona la petición del Fiscal en el ejercicio de sus funciones legales de investigación de los delitos."

Redes sociales y seguridad

Ponencia de José María Blanco Navarro
Director del Centro de análisis y Prospectiva
de la Guardia civil

Es Licenciado en Ciencias Económicas y Empresariales por la Universidad Complutense de Madrid (C.E.U. San Pablo), con la especialidad de Financiación y Licenciado en Derecho por la U.N.E.D. Entre otros es Master Analista de Inteligencia. Universidad Carlos III y Rey Juan Carlos y experto en Gestión del Conocimiento y Capital Intelectual.

También es Consejero del Instituto Universitario de Investigaci n sobre Seguridad Interior (IUISI) y de la Revista Cuadernos de la Guardia Civil; Codirector del Ciclo Superior de Formación en Inteligencia del Instituto de Ciencias Forenses y de la Seguridad, de la Universidad Autónoma de Madrid y colaborador del Master de Analista de Inteligencia (Universidad Carlos III y Rey Juan Carlos).

RESUMEN

La tecnología y la sociedad van modulando las acciones de gobierno y de gestión pública, en el caso que se nos plantea a través del desarrollo de los llamados "social media" (preferiremos utilizar la denominación de Medios Sociales).

En ocasiones las organizaciones centramos la atención en los riesgos y amenazas originadas por la evolución de la tecnología o incluso las demandas ciudadanas, olvidando, de forma no intencionada, las oportunidades que también se generan.

Desde este planteamiento se percibe la necesidad desde las organizaciones de adoptar una doble política:

– Potenciar las oportunidades que ofrecen los Medios Sociales para las Fuerzas y Cuerpos de Seguridad en el ámbito de la información, la comunicación, la investigación policial, la gestión de crisis y catástrofes, la participación ciudadana, la reputación corporativa, etc.

– Minimizar los riesgos, para la seguridad personal de los miembros de las Fuerzas y Cuerpos de Seguridad, y para las propias organizaciones.

En este sentido la gratuidad, accesibilidad y sencillez de los "social media" no nos debe cegar ni llamar a engaño. Es preciso desarrollar una gestión "estratégica" y quizás abordar algunas acciones planificadas, consensuadas, como pudieran ser:

– Elaboración de unas guías para el uso de social media por miembros de los cuerpos policiales. No se trata de prohibir ni limitar, sino informar y recomendar.

– Formación específica sobre "Social Media" para cuerpos policiales, cuyo entorno podrían ser las plataformas de teleformación.

– Avanzar en lo que se viene a denominar "Open Government" o "Gobierno Abierto". Cuestión que, a falta todavía de un marco nacional general, puede ser desarrollado por los cuerpos policiales, en sus dimensiones de comunicación, compromiso y participación ciudadana.

– En materia de prospectiva desarrollar sistemas de inteligencia colectiva, que amplíen la visión de los analistas dando entrada a Universidades, académicos y expertos, y trabajando a través de sistemas en red (wikis, foros, etc.).

1. LOS MEDIOS SOCIALES.

Los profesores Kaplan y Haenlein definen medios sociales como *"un grupo de aplicaciones basadas en Internet que se desarrollan sobre los fundamentos ideológicos y tecnológicos de la Web 2.0, y que permiten la creación y el intercambio de contenidos generados por el usuario"*.

En la llamada web 1.0, el usuario de internet era un mero consumidor de información. En la web 2.0 se convierte en creador, en fuente de opinión, en usuario interactivo. Se comienza incluso a hablar de una web 3.0, que sería aquella que presentara los siguientes componentes:

– Web de bases de datos.

– Web semántica.

– Web 3D.

– Inteligencia artificial. Predicción.

Tecnología, interacción social, y comunicaciones móviles son los tres elementos que configuran los medios sociales.

Se superan ampliamente los conceptos de comunicación unidireccional y bidireccional, todos los usuarios se comunican con todos. Genera en cierto modo una democratización de las comunicaciones, siendo posible incluso el acceso y conversaciones directas, a través de redes sociales, de ciudadanos con políticos, expertos en diversas materias, o cuerpos policiales.

Una posible clasificación de dichos medios sería:

Comunicación:

- Blogs: Wordpress, Blogger.
- Localización: Foursquare, Facebook places.
- Agregadores información. Paper.li, Netvibes.
- Redes sociales. Twitter, Tuenti, Facebook, Pinterest, Instagram, Google.

Colaboración:

- Documentos: Google docs, Dropbox.
- Noticias: Digg, Reddit.
- Gráficos: Creately.
- Wikis: Wikipedia, Wikinews, 15Mpedia.
- Gestores de contenido. Wordpress, Joomla, Drupal.
- Marca social: Delicious, CiteULike, Google Reader.

Ocio:

- Juegos: Zynga, Empire Avenue.
- Mundos virtuales: Second Life.

Opinión:

- Productos: Ciao, Amazon.
- Preguntas: Ask.com, Wikianswers.

Multimedia:

- Música: Last.fm, Spotify.
- Video: Youtube, Vimeo.
- Imágenes: Instagram, Picasa, Pinterest, Flickr.
- Presentaciones: Prezi, Scribd.

Algunos datos sobre el uso de social media en España (finales de 2011):

- 5.º país uso de Redes Sociales.
- 75% internautas utilizan Redes.
- Facebook: 15 M (800 en el mundo).
- Twitter: 4,5 M (200 en el mundo).
- Tuenti: 12 M.
- Linkedin: 2M (15 en el mundo)

2. ANÁLISIS DAFO DE LOS MEDIOS SOCIALES PARA LAS FUERZAS Y CUERPOS DE SEGURIDAD.

Se ha optado por un análisis de Debilidades, Amenazas, Fortalezas y Oportunidades, con objeto de estudiar las posibilidades de los Medios Sociales para los cuerpos policiales.

Es habitual que la aproximación que se realiza desde el ámbito policial en esta materia está centrada en las amenazas para la seguridad generadas por el uso de la red. Pero no se debe olvidar todas las oportunidades que se pueden generar, adicionalmente, a través de un uso y explotación eficiente.

	INTERNO	EXTERNO
POSITIVO	**FORTALEZAS** ✓COSTE ✓INMEDIATEZ ✓SENCILLEZ ✓INTERACTIVIDAD ✓MOVILIDAD ✓DIFUSIÓN	**OPORTUNIDADES** ✓INFORMACIÓN ✓COMUNICACIÓN ✓PARTICIPACIÓN ✓DIFUSIÓN CULTURA DE SEGURIDAD ✓GESTIÓN DEL CONOCIMIENTO ✓GESTIÓN REPUTACIÓN CORPORATIVA ✓FORMACIÓN ✓COMPROMISO CON CIUDADANOS ✓COMUNICACIÓN INTERNA , INTRANETS ✓OPEN GOVERNMENT ✓MONITORIZACIÓN ✓GESTIÓN DE CRISIS Y EMERGENCIAS ✓ANÁLISIS Y ESTUDIO ✓INVESTIGACIÓN POLICIAL . PERFILES . ✓PREDICCIÓN ✓INTELIGENCIA ✓INTELIGENCIA COLECTIVA
NEGATIVO	**DEBILIDADES** ✓FALTA DE FORMACIÓN SUJETOS : o *DIRECTIVOS , EMPLEADOS* ✓FALTA DE FORMACIÓN OBJETO : o *INTERÉS , TÉCNICAS* ✓INFRAVALORACIÓN IMPORTANCIA ✓FALTA TIEMPO Y DE PERSONAL ✓PÚBLICO VS PRIVADO ✓LIBERTAD VS SEGURIDAD ✓TRANSPARENCIA VS SECRETO ✓GESTIÓN DEL ERROR ✓RUIDO	**AMENAZAS** ✓INFOXICACIÓN . EXCESO INFORMACIÓN ✓CREDIBILIDAD Y FIABILIDAD DE LA INFORMACIÓN ✓LAS PROPIAS FORTALEZAS ✓IMPOSIBILIDAD DE CONTROL ✓NUEVOS Y VIEJOS DELITOS ✓INGENIERÍA SOCIAL ✓CESIÓN DE INTIMIDAD ✓RIESGOS SEGURIDAD INFORMÁTICA ✓RIESGOS SEGURIDAD FÍSICA ✓HERRAMIENTA TERRORISTAS ✓VÍA RADICALIZACIÓN Y EXTREMISMO

Tabla 1: *Análisis DAFO de Medios Sociales para la Seguridad*.
Fuente: *Eva Moya (Analista de Inteligencia on-line) y José María Blanco*.

2.1. Fortalezas.

Atenderíamos a aquellos aspectos internos de las organizaciones que suponen una ventaja a la hora de utilizar los Medios Sociales. Dichas ventajas coinciden con las propias características generales de los mismos:

Efectivamente, el coste de presencia en las redes se puede considerar mínimo, incluso nulo. El acceso es inmediato, no se precisa una preparación especial o la espera de un momento concreto. En general su utilización es sencilla, claramente intuitiva. Su uso, a través de los dispositivos móviles (smartphones, portátiles, tablets, etc.) está ligado a la ubicación física del usuario que porta dichos medios y que por tanto puede interactuar en cualquier momento y lugar. Y finalmente cabe destacar el alto grado de difusión de una comunicación, un mensaje, debido a la alta audiencia y al carácter viral de las redes sociales.

En definitiva, unas potentísimas ventajas que como veremos posteriormente en ocasiones se tornan inconvenientes.

2.2. Debilidades.

2.2.1. *Ausencia de formación*.

La facilidad de uso y su inmediatez pueden llevar a pensar que cualquier organización puede lanzarse a tener presencia en las redes sociales. Nada más lejos de la realidad. Tener presencia en Medios Sociales supone disponer de una estrategia de comunicación, definir el mensaje a transmitir, el estilo a utilizar, el lenguaje, y disponer de una formación específica sobre su uso.

En esta línea de especialización destacamos el lanzamiento de la obra *"Escribir en internet"*, de la Fundación del Español Urgente.

Esta circunstancia es fuente habitual de errores por parte de políticos, y personajes famosos.

La adecuada formación para la utilización de Medios Sociales por cuerpos de seguridad ya comienza a ser una materia específica, como vemos en el siguiente ejemplo:

2.2.2. *Infravaloración de su importancia*.

Se trata, de la misma forma, de una consecuencia de la sencillez y facilidad de uso. Las características de los Medios Sociales pueden dañar la imagen de una institución y organización de una manera inmediata (incluso de manera injusta o premeditada). Es preciso disponer de planes para gestión de imagen y reputación corporativa en red.

2.2.3. *Falta de tiempo y de personal*.

La inmediatez de uso puede afectar a las capacidades de reflexión exigibles antes de lanzar un mensaje o comunicación que va a ser leído por multitud de personas y que ya no admite vuelta atrás.

En otras ocasiones las organizaciones no disponen de personal específico, y formado, para el desarrollo de esta función, encomendando la misma a otros trabajadores, de forma adicional a sus funciones propias.

Es clave pensar que se debe tratar como una función específica, que requiere un tiempo de diseño estratégico, de reflexión, y de valoración de los contenidos a emitir.

2.2.4. *Lo público frente a lo privado*.

El derecho a comunicarse de los ciudadanos a través de los Medios Sociales podría generar, en algunas ocasiones, problemas a las empresas u organizaciones para las que trabajan. ¿Puede limitarse una actividad privada en base a una actividad profesional? Parece

evidente que en determinados aspectos no y en otros sí, básicamente en aquellos que afecten a información o a la imagen de la organización.

Pero posiblemente, la política adecuada a adoptar por las organizaciones no iría tanto por el lado de las prohibiciones, sino por el de la concienciación, mediante guías e información a los empleados.

2.2.5. *Secreto frente a Transparencia*.

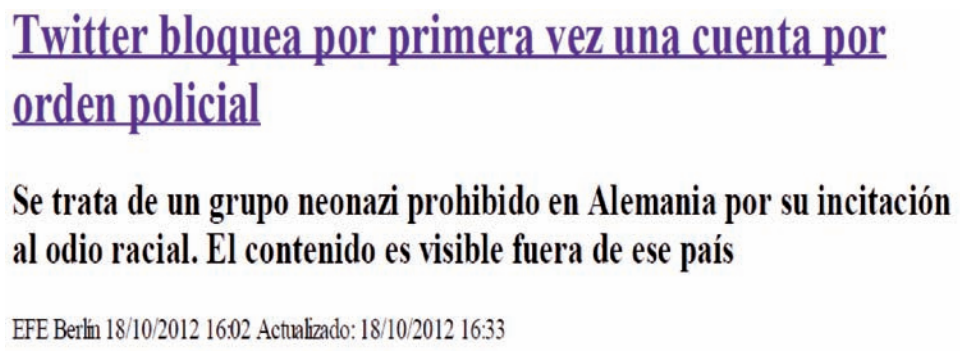
En las redes sociales se libra esta continua y habitual guerra. Se convierten en un medio para la denuncia, la protesta, las filtraciones (leaks). Esta situación tiene efectos tanto positivos como negativos. Por un lado, en ocasiones, pueden poner en peligro la seguridad de ciudadanos, policías, agentes de inteligencia. Pero por otra parte permiten que el ciudadano conozca malas prácticas que de otra forma permanecerían ocultas. En ocasiones las actividades delictivas filtradas superan en gravedad, ampliamente, la propia actividad delictiva de la filtración.

2.2.6. *Seguridad frente a Libertad*.

Este es el segundo gran debate en el ámbito de la seguridad. A lo largo de la historia, y en multitud de países (véase la mal llamada Primavera Árabe), se limita la libertad bajo la excusa de la seguridad. Los usuarios de internet consideramos, quizás de forma algo ilusoria, que la red es el último espacio de libertad existente.

Se trata de una ecuación que no por ser real hay que señalar que es equivocada. La seguridad es un presupuesto para la libertad. La seguridad garantiza a los ciudadanos el disfrute de sus derechos y libertades. La seguridad es un medio, la libertad es un fin.

Pero también se debe considerar el extremo contrario, la utilización de la inmediatez y anonimato en la red para lanzar mensajes contrarios a los sistemas democráticos, inducir discursos extremistas o racistas, etc. Se precisa un pacto de todos los actores del sistema para lograr el debido equilibrio.



Twitter bloquea por primera vez una cuenta por orden policial

Se trata de un grupo neonazi prohibido en Alemania por su incitación al odio racial. El contenido es visible fuera de ese país

EFE Berlín 18/10/2012 16:02 Actualizado: 18/10/2012 16:33

2.2.7. *Ruido*.

Denominamos ruido al exceso de información no útil que aparece en los Medios Sociales. Por un lado toda aquella información no veraz, la información que no soporta

unos niveles mínimos de fiabilidad y credibilidad. Por otra parte, al tratarse de sistemas virales, la repetición de noticias y mismos contenidos. Aspectos que complican, sin duda, el uso y explotación eficiente de los Medios Sociales.

Vemos en el siguiente ejemplo, extraído de Twitter, dicho efecto:

2.2.8. *Gestión del error.*

Los errores quedan para siempre. Se difunden de manera viral, sin dar pie a matizaciones. Se recomienda no eliminar el mensaje inapropiado, ni ofrecer excusas absurdas. La Red valora la transparencia y la honestidad. Pedir disculpas inmediatas es la mejor opción. Asistimos a diario a multitud de ejemplos de políticos y de famosos.

2.3. Amenazas.

2.3.1. *Infoxicación*.

Que cada usuario de la web se convierta en creador de contenidos ha provocado un incremento incontrolable de información. Sobre cualquier tema, hecho, o polémica, es posible encontrar grandes cantidades de información. Ello supone un problema para quie-

nes trabajan con fuentes abiertas, que deben disponer de tecnologías de apoyo, y de claros criterios para la evaluación y selección de la información.

2.3.2. *Credibilidad de la información*.

La pérdida de una clara autoría de la información, la dificultad de encontrar la fuente primaria, y la creación de contenidos en base a agregar detalles a noticias anteriores, hacen preciso que los analistas de información en las redes sociales deban extremar los criterios para poder garantizar, en cierto grado, la credibilidad y fiabilidad de la información.

Un ejemplo ya clásico es el de la presunta chica lesbiana de Siria, que cada viernes informaba sobre las manifestaciones que se producían en su ciudad:

Domingo, 21 de octubre 2012

LAVANGUARDIA.com | Internacional

La bloguera lesbiana de Damasco era él

La historia de una de las activistas más famosas de Siria ha resultado ser una mentira escrita por un hombre estadounidense

Internacional | 13/06/2011 - 07:52h

MARINA MESEGUER | Sigue a este autor en Twitter
Barcelona

Uno de los símbolos de la oposición siria, la bloguera lesbiana Amina Abdallah Araf al Omari, autora del famoso blog *A gay girl in Damascus*, ha resultado ser una farsa. Tras una semana de especulaciones sobre su existencia, el misterio se ha solucionado: Amina es en realidad un tal Tom MacMaster, un hombre estadounidense que escribe, según él, desde Estambul.

Pero, ¿Quién era Amina? Durante 106 días se suponía que era una joven de 35 años que hablaba sobre su vida como lesbiana en una ciudad como Damasco. *A gay girl in Damascus* se convirtió en un blog donde esta *mujer*, que decía tener doble nacionalidad siria y estadounidense, escribía de forma apasionada sobre su sexualidad y su activismo político en una Siria inmersa en un proceso revolucionario.

2.3.3. *Los riesgos derivados de las propias fortalezas de los Medios Sociales*.

Su inmediatez y gran capacidad de difusión en ocasiones puede generar incluso problemas de orden público. Mediante movilizaciones espontáneas se ha llegado a intentar obstaculizar la labor policial de identificación de ciudadanos. En otras ocasiones, la convocatoria de una fiesta "doméstica" a través de estos medios, ha derivado en una asistencia masiva, generando problemas de seguridad.

2.3.4. *La imposibilidad de control*.

Dado que cada ciudadano se puede convertir en creador de contenidos, en ocasiones dicha información puede poner en riesgo la seguridad de los Estados, o generar problemas diplomáticos. Una caricatura religiosa, por ejemplo, puede generar un importante número de víctimas en otro extremo del mundo.

Esta circunstancia está muy bien tratada en un artículo del Instituto Español de Estudios Estratégicos (IEEE), denominado "El ciudadano estratégico".

EL CIUDADANO ESTRATÉGICO

Resumen:

La acción o el documento producido de modo privado por un ciudadano y exhibida en internet tiene la capacidad de comprometer la estrategia y a la diplomacia de su país de modo creciente e irreversible. Especialmente en lo que respecta a las relaciones entre el mundo occidental y el musulmán, especialmente sensible a los contenidos de tipo religioso.

2.3.5. *Nuevos y viejos delitos*.

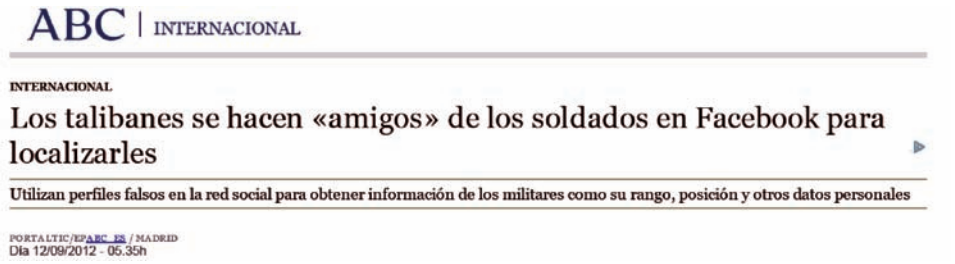
Los Medios Sociales son vías para la actividad delictiva, aunque se debe señalar que no siempre son nuevas tipologías. En muchas ocasiones se trata de los delitos de siempre que encuentran un nuevo medio o espacio. Un claro ejemplo es el ciberacoso, una figura clásica que a través de la red, y en base al anonimato y el uso tecnológico, agrava el grado de amenaza y genera dramáticos efectos, como venimos viendo en los medios de comunicación casi a diario.

2.3.6. *Riesgos para la seguridad informática*.

Virus, Malware, Spyware, etc. La Red es una vía de infección, que precisa la adopción de todos los medios de protección precisos.

2.3.7. *Riesgos para la seguridad física*.

Las redes sociales se han llegado a convertir en una doble vida para muchos ciudadanos. Virtual, pero tan real, y con tantos efectos tangibles, como la vida física. En ocasiones se comparte información sobre hábitos, sobre desplazamientos y viajes, o se actúa en las redes con los sistemas de geolocalización de los dispositivos móviles activados.



ABC | INTERNACIONAL

INTERNACIONAL

Los talibanes se hacen «amigos» de los soldados en Facebook para localizarles

Utilizan perfiles falsos en la red social para obtener información de los militares como su rango, posición y otros datos personales

PORTALTIC/EP ABC.ES / MADRID
Día 12/09/2012 - 05.35h

Según el informe, una de las estrategias empleadas por los terroristas es **hacerse pasar por «atractivas mujeres»** que, una vez han conseguido hacerse amigas de los militares a través de la red social, pueden **rastrear el paradero de los soldados** a través de las opciones de etiquetado geográfico de Facebook.

«La mayoría no reconoce que las personas que utilizan perfiles falsos, quizá haciéndose pasar por un antiguo amigo de la escuela, podrían capturar su información y movimientos», indica el informe. **«Pocos consideran las posibilidades de extraer datos y cómo los patrones de comportamiento** pueden ser identificados con el tiempo», remarca.

Según indica el sitio web Mashable, el estudio del gobierno de Australia también señala que la familia y los amigos de los militares pueden poner en peligro las misiones de los soldados mediante el **intercambio de datos confidenciales a través de los medios sociales**.

2.3.8. *Ingeniería social*.

En el ámbito de la seguridad informática se suele señalar que en muchas ocasiones el factor humano es el eslabón más débil de la cadena. La Ingeniería Social o "Human Hacking" se basa en la manipulación inteligente de la tendencia de las personas a confiar.

Mediante definidas técnicas de comunicación, conversación, simulando roles o situaciones, es posible extraer de personas sus números de tarjeta de crédito o cualquier otro tipo de dato de interés.

2.3.9. *Seguridad de la información*.

Más bien como consecuencia de los factores que hemos señalado en los tres puntos anteriores, se produce un efecto de pérdida de información, o descontrol de la misma, de carácter inicial, que puede ser la entrada no sólo a riesgos físicos, sino a pérdidas de información posteriores y continuadas (virus, robo de claves, etc.).

2.3.10. *Pérdida de intimidad*.

Todo el uso de la Red y de los Medios Sociales produce la elaboración de patrones de conducta, de hábitos, de consumo. Cada pequeño detalle de información es susceptible de ser transformado en un análisis, con fines de investigación o comerciales sólo en el mejor de los casos:

2.3.11. *Jihad 2.0*.

Internet y las redes sociales se han convertido en una vía para los grupos yihadistas, con objeto de informar y comunicar, adoctrinar, reclutar, obtener financiación, planificar acciones, etc.

2.3.12. *Radicalización y extremismo violento*.

De la misma forma, la red sirve para difundir mensajes extremistas que puedan incitar a la violencia. Hay que tener en cuenta que estos movimientos desarrollan potentes narrativas y doctrina, que en la red encuentra una magnífica vía de difusión. Y no únicamente el mensaje inicial, sino toda la acción que forma parte de un proceso de radicalización (victimización, búsqueda de un enemigo común, socialización con el objetivo ofreciendo atención o comprensión, puesta en contacto con círculos radicales, intercambio de materiales, etc.).

2.4. Oportunidades.

2.4.1 *Información*.

Un uso básico de los Medios Sociales es informar, y por tanto es también extrapolable al ámbito de la seguridad.

2.4.2. *Comunicación*.

El segundo aspecto básico es la capacidad de interacción. Comunicación ya no sólo bidireccional, sino entre todos aquellos interesados en sumarse a una temática o hilo de debate.

2.4.3. *Participación*.

Los Medios Sociales generan oportunidades para la participación ciudadana, también en temas de seguridad. Un ejemplo lo tendríamos en el Grupo de Delitos Telemáticos, a través de cuyas aplicaciones un ciudadano puede convertirse en patrullero de la seguridad en la Red, o denunciar situaciones a través de redes sociales.

2.4.4. *Cultura de seguridad*.

Los Medios Sociales son una magnífica vía para la difusión de la cultura de seguridad. En el ámbito de la Guardia Civil destacamos el Instituto Universitario de Investigación en Seguridad Interior (IUISI), a través de su web (www.iuisi.es) o de sus cuentas en redes sociales (@iuisi).

2.4.5. *Gestión del conocimiento*.

Absolutamente relacionado con el aspecto anterior, la red (interconexión más tecnología) permite la utilización de aplicaciones que permiten la estructuración, difusión y visua-

lización de conocimiento. Siguiendo el mismo ejemplo destacamos el "diario" del IUISI *http://paper.li/iuisi/1336729098*

2.4.6. *Formación*.

Las Fuerzas y Cuerpos de Seguridad también pueden beneficiarse, en sus actividades formativas, de la utilización de plataformas on-line. Quizás Moodle sea una de las más conocidas, pero las posibilidades pueden ser extensibles a la utilización de una cuenta en Twitter, o la creación de grupos en Linkedin.

En todo caso no se deben olvidar y determinar todas aquellas cuestiones que puedan afectar a la seguridad, motivo por el cual las redes sociales pueden ser limitadas, por ejemplo, a una vía de comunicación abierta para acciones formativas o de difusión de Cultura de Seguridad, como jornadas, seminarios, etc.

2.4.7. *Compromiso con los ciudadanos*.

Uno de los objetivos máximos de cualquier cuerpo policial debería ser lograr el compromiso de los ciudadanos en las cuestiones de la seguridad. Este principio es de fácil declaración, pero de difícil ejecución. Conseguir un "compromiso" está mucho más allá de la comunicación, la colaboración, o la participación. Supone la asunción de un compromiso, un "contrato psicológico" que no se puede exigir de manera coercitiva. Este tipo de contratos se forjan en base a la transparencia y la confianza, y exigen al menos una percepción de equilibrio entre las prestaciones de un ciudadano a este bien común, y las contraprestaciones que recibe a cambio.

En momentos de crisis económica, con una preocupante pérdida de crédito institucional, son precisamente las organizaciones que prestan servicios a los ciudadanos las que lideran todas las encuestas de confianza. Cuerpos policiales, sanidad, servicio sociales, etc. encabezan los barómetros, como el de confianza institucional que cada verano publica Metroscopia.

2.4.8. *Reputación corporativa*.

Los Medios Sociales facilitan a los cuerpos policiales información sobre su "marca", sobre la percepción social de su organización. Existen herramientas gratuitas en la red que posibilitan análisis de carácter básico, como Google Trenes, Icerocket, Social Mention, etc.

Vigilar qué se dice en la red sobre una organización se ha convertido en una necesidad, que obliga a una gestión estratégica de comunicación.

2.4.9. *Comunicación interna*.

La proliferación de la presencia en los Medios Sociales no debe hacer descuidar a los cuerpos policiales la atención a la comunicación interna. Las intranets son una de las herramientas, y sus funcionalidades deben ser similares a las de los Medios Sociales abiertas. Las intranets modernas deben permitir la interconexión, la movilidad, la agilidad, aunque siempre condicionadas por las cuestiones de seguridad.

En determinadas empresas se empieza a generar la Intranet como widget o app, portable en dispositivos móviles, y con integración de agendas (tipo Google), notas (tipo Evernote), creación de grupos y comunidades, gestor de contenidos, servicios al empleado, foros, blogs, wiki, etc.

Consideramos que una buena práctica es Goblonet, desarrollada por la Federación Española de Municipios y Provincias:

2.4.10. *Gobierno Abierto (Open Government)*.

Se puede definir como una doctrina política que trata de crear espacios de participación ciudadana en la gestión pública, con la transparencia como un valor fundamental.

Las redes sociales e Internet en general, sin duda, son un elemento de valor para el desarrollo del Gobierno Abierto. Webs, administración electrónica, sistemas de participación, fórmulas para facilitar las denuncias, etc. son algunas de las fórmulas aplicadas por las Fuerzas y Cuerpos de Seguridad, pero no las únicas.

En el ámbito de la Seguridad, citamos como buena práctica el caso del Departamento de Seguridad Interior de Estados Unidos, que directamente, en su propia web, especifica su proyecto de Gobierno Abierto:

2.4.11. *Monitorización de contenidos en la Red*.

Advertíamos de la utilización de la Red, y de los Medios Sociales, para el adoctrinamiento y la radicalización. La parte positiva es que todos los contenidos en Red quedan en la misma, en muchos casos con carácter abierto. Por tanto es posible rastrear información, monitorizar webs, palabras clave, entidades, de interés para los servicios de seguridad de los Estados, respetando la legalidad y la privacidad en base a las normativas de cada uno de ellos.

2.4.12. *Investigación policial*.

En parte consecuencia del apartado anterior, la investigación en redes sociales posibilita ampliar la información disponible, en temas como contactos, aficiones, actividades, etc.

2.4.13. *Gestión de emergencias*.

Las redes sociales se han mostrado útiles a la hora de facilitar información en situaciones de catástrofes o emergencias. Tsunami de Japón, terremoto de Lorca (mensajes con

consejos y recomendaciones desde la Administración Pública), los incendios de verano de 2012 en Valencia (con solicitudes de medios a través de Twitter), o recientemente el huracán Sandy en Estados Unidos, son algunos de los ejemplos.

Se vienen desarrollando proyectos en este sentido (Twitter, Topsy), y también a nivel de la Unión Europea (la Guardia Civil participa en un consorcio que ha presentado una propuesta a la Comisión, en el área de seguridad del 7.ª Programa Marco).

2.4.14. *Análisis y estudio*.

No toda la acción policial va encaminada a la investigación. Determinadas unidades pueden tener en sus competencias el análisis de tendencias, factores sociales, prospectiva, etc. Un ejemplo sería el Centro de Análisis y Prospectiva. A título de ejemplo, si se quiere intentar entender algo sobre los nuevos movimientos sociales, el ciberactivismo, el 15M, es obligatorio estar o seguir los Medios Sociales. Y no con objetivo punitivo, sino con la única pretensión de intentar entender el mundo en que vivimos, muy complejo, muy acelerado, y con multitud de variables que obligan a evitar explicaciones simplistas o con una única base ideológica.

2.4.15. *Predicción*.

Las técnicas predictivas avanzan a pasos agigantados. Sin duda, el futuro no es predecible, pero desde el campo de la psicología sí es posible determinar la propensión a la comisión de determinados delitos. Estudios intentan incluso sacar conclusiones a través del lenguaje que se utiliza en las redes sociales.

Otra vía es la generación de sistemas inteligentes, que partiendo del análisis de grandes cantidades de datos, generan algoritmos que se van corrigiendo a medida que se incorporan nuevos datos.

2.4.16. *Inteligencia*.

Los Medios Sociales se convierten en una de las fuentes de información para la Inteligencia, algo que se podría englobar en lo que denominamos Inteligencia de Fuentes Abiertas (OSINT), En todo caso, las redes sociales, por su funcionamiento, tienen un componente OSINT pero también de Inteligencia de Fuentes Humanas (HUMINT). A título de ejemplo, una información en Twitter se puede considerar OSINT, pero un mensaje privado en esa misma red sería más bien HUMINT.

2.4.17. *Inteligencia colectiva*.

Los Medios Sociales posibilitan la creación de inteligencia colectiva, sistema de cocreación conjunta de conocimiento. Un concepto similar, pero no exacto, es de la sabiduría de las multitudes, acuñado por Surowiecki en su obra "The wisdom of the crowds" (en su versión en castellano se tradujo como "100 mejor que 1").

Un caso de ejemplo, como posible buena práctica, sería Wikistrat, sobre cuyo objetivo y funcionamiento es posible encontrar completa información en su web (www.wikistrat.com).

3. CONCLUSIONES.

Siguiendo la metodología DAFO, se podrían establecer diferentes estrategias de acción, que pasan por atacar las debilidades, reducir las amenazas, y aprovechar al máximo las oportunidades que los Medios Sociales ofrecen a las Fuerzas y Cuerpos de Seguridad.

Pero no debemos quedarnos en este nivel de generalización, sino generar propuestas concretas, de sencilla y no costosa materialización. De esta forma, las propuestas que se realizan desde este Centro de Análisis y Prospectiva se orientan a:

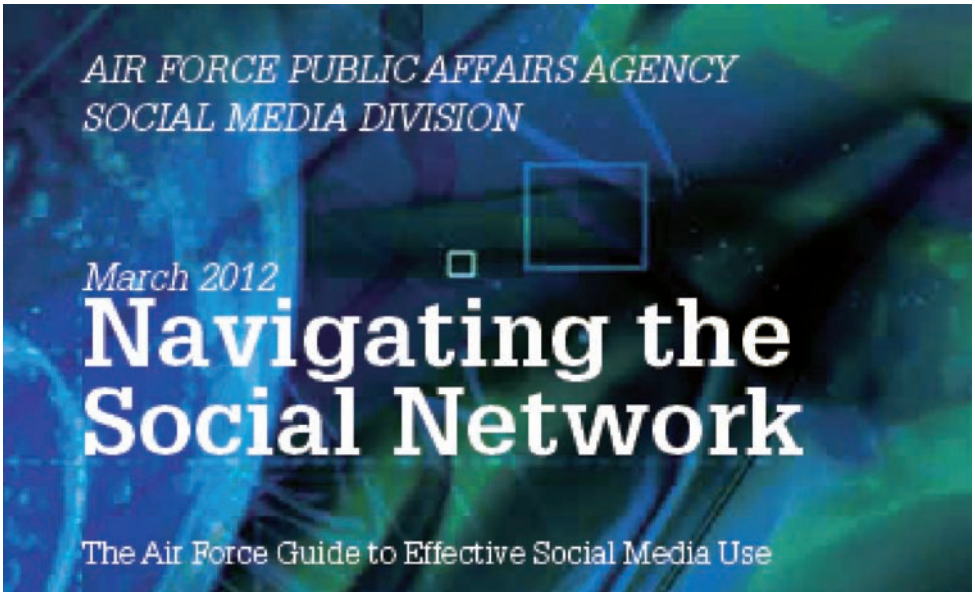
3.1. *Potenciar la información y la formación sobre la materia*.

Consideramos que la prohibición no es la vía, que la forma debe ser la concienciación de los empleados de la responsabilidad del uso de los Medios Sociales. Cuestión fácilmente abordable por dos vías:

– Elaboración de un guía sobre el uso de redes sociales, y su difusión masiva a todos los miembros de la organización.

– Diseño de una formación especializada que podría ser implementada mediante sistemas de teleformación, con objeto de reducir costes y aumentar el número de destinatarios., Una formación permanentemente abierta, y accesible.

Como buena práctica citamos la guía de la Air Force Public Affaire Agency:



3.2. *Sistemas colaborativos internos*.

Incorporación de tecnología estilo Medios Sociales en el seno de las organizaciones con objeto de hacer explícito y compartido el conocimiento existente, que se pierde con la

marcha de muchos profesionales. Sistemas de trabajo colaborativo, gestores de documentación, agendas compartidas, creación de grupos y comunidades informales, etc.

3.3. *Análisis y Prospectiva*.

Como Director de un Centro con dicha denominación no pretendo defender esa función, pero sí señalar que esta función de análisis y prospectiva, en materia de seguridad, es extensible a cómo evoluciona la sociedad y la tecnología, ofreciendo de esta manera a los cuerpos policiales nuevas amenazas, pero también nuevas oportunidades.

3.4. *Inteligencia colectiva*.

El grado de especialización de la sociedad actual ha llevado a compartimentar el saber, lo que produce grandes y evidentes sesgos en nuestra visión del mundo. Cada persona y organización percibe esa realidad desde su punto de vista. No es un error, pero sí una visión sólo parcial y muy limitada. Multienfoque, diversidad, e integración de expertos de diferentes áreas, son las salidas a esta situación.

3.5. *Gobierno Abierto*.

Es preciso avanzar en transparencia y potenciar las vías de participación ciudadana en seguridad. Si queremos ciudadanos comprometidos con la seguridad, que se conviertan en ojos y oídos de los cuerpos policiales, no en nuestro beneficio sino en el de toda la comunidad, es preciso disponer de ciudadanos formados e informados en seguridad, sin medias tintas, con claridad, con objeto de forjar una sociedad resiliente.

Se señala que la seguridad es subjetiva, y que la seguridad absoluta es una utopía. Los ciudadanos deben conocer las amenazas a las que nos enfrentamos, sin que con ello se genere alarma social. Una sociedad que sepa que, a pesar de los enormes esfuerzos de sus servidores públicos, puede ser golpeada por la barbarie, el fanatismo y la sinrazón de grupos de cobardes asesinos. Pero una sociedad lo suficientemente fuerte para levantarse al día siguiente, ponerse en pie, reanudar su funcionamiento y vencer a quienes tratan y seguirán tratando de perturbar nuestra paz, y de impedir el libre ejercicio de nuestros derechos y libertades.

"Los peligros están ahí, no los disminuyo, pero las oportunidades también, y estas, las oportunidades que tenemos, hay que magnificarlas con toda la fuerza de nuestra voluntad y de nuestra imaginación, transformando nuestra experiencia en un destino mejor, más democrático y más libre".
(Carlos Fuentes)

Delincuencia en redes sociales

Ponencia de D. scar de la Cruz Yagüe
Jefe del Grupo de Delitos Telemáticos
Unidad Central Operativa de la Guardia Civil

Internet se ha convertido en pocos años, en una revolución tecnológica de la cual nadie duda de las ventajas que nos aporta como forma de comunicación global. Las posibilidades que la red nos ofrece son ilimitadas, de tal forma que han cambiado nuestra forma de relacionarnos, de trabajar y de pasar nuestro tiempo de ocio.

Probablemente a nadie de las últimas y no tan últimas generaciones se le ocurra escribir una carta en lugar de enviar un correo electrónico; esperar la cola de una taquilla en lugar de hacer una reserva online; tener que ir al banco a pedir un extracto o realizar una transferencia; y un largo etcétera de actividades cotidianas que gracias a la red realizamos desde cualquier lugar de manera cómoda, ágil y sin esperas.

Es necesario comprender que estas nuevas tecnologías no constituyen un apartado más de nuestra vida, al que podamos dar cabida o no, sino que se conforma como una capa más que cubre el resto de actividades de realizábamos antes de forma habitual, es decir, es un elemento transversal que afecta a todos los ámbitos de nuestra vida.

Sin embargo, y a pesar de que las nuevas tecnologías nos presentan grandes beneficios de forma mayoritaria, algunas personas han encontrado en ellas una vía novedosa y eficaz para la comisión de nuevas conductas delictivas, aprovechándose de los vacíos legislativos que existen al respecto debido a su continua transformación y a la falta de conocimiento sobre los peligros que entraña su uso. De esta manera se generan los delitos tecnológicos o ciberdelitos, denominados como las actividades ilícitas o abusivas relacionadas con los sistemas y las redes de comunicaciones, bien porque sean el objetivo del delito en sí mismos, o se trate de la herramienta y el medio para su comisión.

En las siguientes páginas, vamos a dar una visión general sobre la delincuencia que de forma específica se mueve alrededor de las redes sociales. A modo de introducción y de forma breve, se expondrá cómo la Guardia Civil estructura sus Unidades relacionadas con la investigación tecnológica, así como unos conceptos generales y cifras relacionadas con

el uso de la red. Posteriormente, una relación genérica de los delitos que tienen mayor incidencia en este contexto, sin olvidarnos de otras conductas, que aunque no son perseguibles penalmente, sí que constituyen unos contenidos nocivos, a los cuales puede acceder cualquiera, incluidos por supuesto los menores de edad. Finalmente a modo de resumen, se citará el decálogo de navegación segura, elaborado por el Grupo de Delitos Telemáticos.

LA GUARDIA CIVIL Y LOS DELITOS TECNOLÓGICOS

Para la lucha contra lo que se conocen como ciberamenazas, la Guardia Civil ubica sus Unidades especializadas en investigación tecnológica en dos Jefaturas, la de Policía Judicial y la de Información. Esto responde al tratamiento diferencial que históricamente se ha dado a la delincuencia organizada y al terrorismo, y sus evoluciones tecnológicas que son la ciberdelincuencia y el ciberterrorismo.

En este ámbito ciber, es más patente si cabe la aproximación de ambas formas, en las que unas se sirven de otras para lograr sus objetivos, y donde más claras se ven sus conexiones, en el blanqueo de capitales y financiación del terrorismo. Si bien la finalidad del cibercrimen y el ciberterrorismo es diferente, el medio para conseguirlo es idéntico, y como prueba puede servir un ejemplo de una intrusión a una infraestructura crítica. Una organización que consiga el acceso a los sistemas SCADA de control industrial de una infraestructura de este tipo (central eléctrica, industrial, transporte...) en un primer momento se tratará como posible acto terrorista por el ataque a un sector que se considera básico para la población y que puede generar graves daños o estragos. Sin embargo dicho acceso ha podido ser realizado por un grupo organizado que sólo pretenda extorsionar con un pago económico sin que nunca exista la voluntad de generar ese perjuicio, lo cual haría tratar el hecho desde la perspectiva de la ciberdelincuencia.

Estructura

Para la persecución del ciberdelito, la Guardia Civil enmarca dentro de su estructura periférica a los Especialistas de Investigación Tecnológica (EDITEs), dentro de las Unidades Orgánicas de Policía Judicial que residen en cada Comandancia a nivel provincial. Dichos Especialistas están suficientemente capacitados y formados (a través de los cursos básicos de investigación tecnológica CBIT) como para llevar de forma independiente las investigaciones relativas a ciberdelitos en su ámbito territorial.

Para realizar la correcta coordinación de estos Especialistas, realizar tareas de elaboración de inteligencia y posterior difusión a las Unidades afectadas, homogeneización de procedimientos e impulso de actividades de formación, así como canalizar comunicaciones con otros organismos nacionales e internacionales, la Unidad Técnica de Policía Judicial (UTPJ) dispone de su sección de Delitos Tecnológicos.

Puesto que la delincuencia se ha vuelto transnacional y ya no entiende de fronteras, más aun si hablamos de ciberdelincuencia, los criterios territoriales que determinaban la investigación han quedado totalmente obsoletos. La determinación del *itercriminis* resulta compleja, más aun en los primeros momentos de las indagaciones. Por todo lo anterior, se crearon las Unidades Centrales, capaces de dar una respuesta global a la delincuencia en todo

el territorio nacional. Es pues en el seno de la Unidad Central Operativa, donde se incardina el Grupo de Delitos Telemáticos, con las misiones que se expondrán a continuación.

Dependiente del Servicio de Criminalística, el Departamento de Ingeniería se encarga de apoyar las investigaciones que realizan el resto de Unidades de la Guardia Civil, realizando los análisis forenses de los equipos informáticos y dispositivos que les sean requeridos, ya se trate de discos duros, tablets, smartphones, pendrives, etc... El estudio forense de dichos dispositivos se plasmará en un informe pericial, con validez plena para el proceso penal, debido a la cualificación como peritos que tienen los miembros del SECRIM.

En lo que respecta a la Jefatura de Información, recientemente reestructurada, el Área Técnica se encarga de aglutinar a sus Unidades con competencias en estos aspectos tecnológicos que requieren especiales dotaciones tanto en medios humanos como materiales. Destacar la labor que desarrolla la Unidad de Ciberterrorismo, encargada de dar el apoyo técnico tan necesario hoy en día en la investigación a través de internet y redes sociales para la lucha contra el terrorismo nacional e internacional.

Composición y estructura del Grupo de Delitos Telemáticos (GDT)

Dentro del Grupo de Delitos Telemáticos se ha adoptado el esquema de trabajo que se puede derivar del Convenio sobre ciberdelincuencia del Consejo de Europa, firmado en Budapest en 2001 y el protocolo adicional firmado dos años después para incluir los delitos de apología del racismo y la xenofobia. Por lo tanto, para categorizar y estructurar el tipo de delincuencia que investiga el GDT, se han establecido cuatro grandes áreas:

– Relacionados con el contenido y menores, como son la pornografía infantil, abusos sexuales a menores y grooming, ciberbullying, ...

– Delitos de fraude y falsificación informática, en sus distintas versiones como fraudes bancarios y phishing, y fraudes en el comercio electrónico.

– Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas, más conocidos como hacking.

– Delitos contra la propiedad intelectual y derechos afines.

De acuerdo con la división de delitos realizada por este convenio, la estructura del GDT se articula en el Mando y PLM, tres secciones de investigación y una sección de I+D.

Misiones

Las misiones específicas del Grupo del Grupo de Delitos Telemáticos son las siguientes:

– Desarrollo de investigaciones relacionadas con la delincuencia informática, especialmente de aquellas que por su complejidad técnica, ámbito territorial o novedad en su modus operandi requieran un tratamiento especial en lo que respecta a capacitación técnica.

– Apoyo en aspectos técnicos del resto de investigaciones de la UCO, tanto en el volcado y clonado de equipos informáticos intervenidos, como cualquier otro apoyo de carácter técnico que se pueda requerir en el desarrollo del resto de operaciones de la Unidad o del resto de Unidades Orgánicas de Policía Judicial.

– Colaboración de forma muy significativa en la formación del personal de los especialistas EDITEs de las Unidades Orgánicas. De igual modo el GDT constituye el apoyo técnico de dichos equipos. Además de estos cursos, el GDT participa en cursos organizados por órganos judiciales, fiscalía, etc.

– Por último, representar y promover la participación del Cuerpo en foros y encuentros internacionales sobre cibercrimen y actuar como punto de contacto internacional en este ámbito a través de organismos como Europol, Interpol, Eurojust, G8, etc...).

ALGUNAS CIFRAS RELACIONADAS CON LA RED

Para ayudar a comprender parte de la problemática que supone la investigación de este tipo de delincuencia, es interesante aportar algunas cifras, para contextualizar el fenómeno. En tan sólo 1 minuto circulan por la red unos 200 millones de correos electrónicos (de los que casi el 80% se trata de spam o correo no deseado), se suben más 30 horas de vídeo a Youtube o se realizan más de 2 millones de búsquedas en Google. Igualmente, la red social Facebook ya ha superado los 1.000 millones de usuarios, con lo que si fuera un país, sería ya el tercero más poblado del mundo por detrás de China e India.

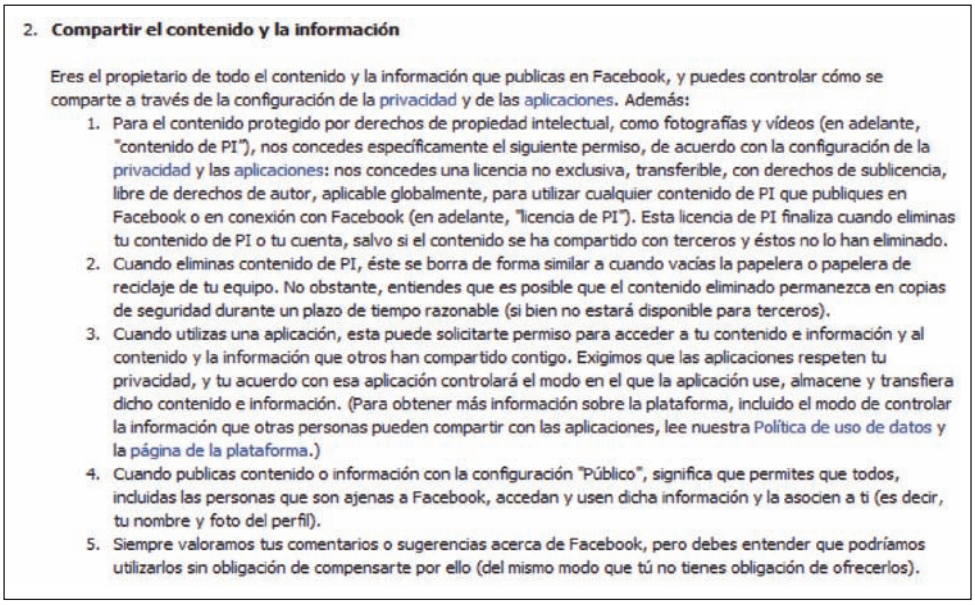
Según cifras del Instituto Nacional de Estadística, 1 de cada 3 jóvenes españoles hace algún tipo de uso de redes sociales; en concreto, el porcentaje de jóvenes entre 15 y 24 años sobre el total de la población respecto a este uso es del 29%. De hecho, otro tipo de estudios, consideran este rango de edad como los usuarios mayoritarios de redes sociales.

Otro dato a tener en cuenta, es el volumen de información que tratamos, lo que se conoce actualmente como “big data”, que mal gestionado puede dificultarnos nuestras tareas en lugar de ayudar. Como curiosidad, se hizo una estimación da la cantidad de información que había generado el ser humano desde su creación hasta el año 2.003, se cuantificó y dio como resultado 5 exabytes (1 exabyte = 1.000 millones de gigabytes), pues bien, actualmente esa información se genera cada dos días, y en 2015 se espera que sea generada cada diez minutos.Todo esto hace que el flujo de información sea difícilmente controlable, en lo que respecta a extensión e inmediatez.

PRIVACIDAD EN REDES SOCIALES

Uno de los aspectos genéricos importantes a tratar respecto al uso de redes sociales, es el relativo a la privacidad. En primer lugar, pocos usuarios han leído las condiciones de uso al darse de alta, porque la navegación en internet requiere inmediatez, y queremos disponer del acceso y del contenido de forma instantánea, sin perder tiempo leyendo varias páginas en las que además hay que prestar atención. Es aconsejable conocer qué derechos esta-

mos otorgando de forma implícita a la red social cada vez que subimos un contenido más o menos personal a la misma, como muestra el ejemplo:



2. Compartir el contenido y la información

Eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte a través de la configuración de la privacidad y de las aplicaciones. Además:

1. Para el contenido protegido por derechos de propiedad intelectual, como fotografías y vídeos (en adelante, "contenido de PI"), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de la privacidad y las aplicaciones: nos concedes una licencia no exclusiva, transferible, con derechos de sublicencia, libre de derechos de autor, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (en adelante, "licencia de PI"). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido con terceros y éstos no lo han eliminado.
2. Cuando eliminas contenido de PI, éste se borra de forma similar a cuando vacías la papelera o papelera de reciclaje de tu equipo. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros).
3. Cuando utilizas una aplicación, esta puede solicitarte permiso para acceder a tu contenido e información y al contenido y la información que otros han compartido contigo. Exigimos que las aplicaciones respeten tu privacidad, y tu acuerdo con esa aplicación controlará el modo en el que la aplicación use, almacene y transfiera dicho contenido e información. (Para obtener más información sobre la plataforma, incluido el modo de controlar la información que otras personas pueden compartir con las aplicaciones, lee nuestra Política de uso de datos y la página de la plataforma.)
4. Cuando publicas contenido o información con la configuración "Público", significa que permites que todos, incluidas las personas que son ajenas a Facebook, accedan y usen dicha información y la asocien a ti (es decir, tu nombre y foto del perfil).
5. Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos).

Otro de los aspectos a tratar, es la configuración de la privacidad, es decir, el nivel de acceso o restricción que imponemos a según qué personas sobre nuestros contenidos. Conviene invertir tiempo en configurar de forma correcta estos parámetros, para evitar que personas que no pertenecen a nuestro entorno puedan acceder a nuestra información más confidencial. Toda estos datos acerca de nuestra vida privada que estamos facilitando, en forma de imágenes, vídeos, geolocalizaciones, tienen consecuencias que debemos meditar, según quién vaya a hacer uso de los mismos. Actualmente, cualquier departamento de recursos humanos realiza una pequeña "investigación" sobre nosotros como complemento al curriculum vitae y la entrevista personal, por lo que en un futuro podemos pagar nuestros excesos del pasado. Igualmente, la delincuencia se sirve de nuestra información para saber si estamos en casa o fuera, qué nivel de vida tenemos, conocer nuestro entorno y familiares, aficiones... Un caso real se produjo en Australia, donde una joven publicó una foto en Facebook donde aparecía contando una gran cantidad de dinero que le había tocado a su abuela en un sorteo. A las dos horas estaban dos individuos encapuchados llamando a la puerta de su casa preguntando por ella.

Resulta llamativo ver cómo se enfoca la privacidad según la red social de que hablemos y el país en que radique, ya que cada una de ellas está sujeta a la legislación del país donde se ubique su razón social. Por lo tanto, en el caso de redes sociales españolas, se someten estrictamente a nuestra legislación tanto de tipo penal como de protección de datos de carácter personal, y la configuración de privacidad es cerrada y limitada por defecto. Al contrario, podemos ver en otras redes sociales que la configuración inicial es

VIDA DIGITAL

Publica en Facebook una foto con fajos de billetes y asaltan su casa

El suceso ocurrió en Australia. Una joven colgó una imagen con su abuela y mucho dinero

DPA
28 de mayo de 2012 11:54

25 votos

Una australiana de 17 años desató un asalto a la casa de su madre al colgar en facebook una fotografía en la que aparecía junto a fajos de dinero.

Según informó hoy la policía, la joven había ayudado a su abuela a contar el dinero y se había fotografiado junto a él y subido la imagen a la red social.

Pocas horas después, dos hombres armados se presentaron en casa de su madre y preguntaron por el dinero y la joven. Lo que no sabían es que los billetes no se encontraban en la casa en Bundanoon, sino en la de la abuela en Sídney, a 150 kilómetros de allí.

La madre dijo a los ladrones que su hija ya no vivía con ella. Los hombres registraron entonces la casa y se llevaron consigo algunos objetos de valor y una cantidad reducida de dinero en efectivo.

SABER MÁS...

Facebook

abierta totalmente, y todos los contenidos que subamos son compartidos con todos los usuarios, por lo que para poner límites y restringir accesos debemos acceder a nuestra configuración personal y modificar los accesos para cada tipo de entorno.

Aunque queda mucho trabajo por hacer, los usuarios cada vez están más concienciados con el uso o mal uso de su privacidad. Sirva como ejemplo reciente el caso de Instagram, red social creada para compartir fotografías. Ante el anuncio del cambio de sus políticas de uso, por la que podría hacer uso comercial de todas las fotos subidas por sus usuarios, ha perdido el 50% de los mismos que se han dado de baja en el servicio, haciendo dar marcha atrás en sus intenciones de cambio.

Otro aspecto a tener en cuenta respecto a la subida de contenidos a la red, es la imposibilidad material de retirar un contenido (texto, imagen, vídeo) de la red. Actualmente la legislación sólo faculta a la Autoridad Judicial para instar la retirada de contenidos, lo cual se traduce en un proceso poco ágil. Debido a la posibilidad de replicación masiva y viral que ofrece la red, en el tiempo que se tarda en retirar de un sitio web, es posible que se haya colgado en otros tantos, por lo que la limpieza total, añadiendo la función que hacen los buscadores en este sentido, resulta como hemos dicho tarea imposible. En EEUU hace unos años realizaron una campaña hace unos años llamada “Thinkbeforeyou post (piensa antes de publicar) para concienciar al ciudadano, especialmente a los más jóvenes, de los problemas que puede acarrear el publicar contenidos de carácter personal en la red.

TIPOLOGÍA DELICTIVA

El uso de redes sociales, como forma de interacción humana, ha supuesto una prolongación de actividades delictivas que en la mayoría de los casos ya existían, pero en su variante digital, amplificadas por las peculiaridades de las comunicaciones a través de la red, como son la sencillez para conseguir anonimato, o el hecho de poder suplantar fácilmente cualquier dato que vincule a una identidad, ya sea perfil, dirección de correo, imagen, etc.

A continuación, se hará un repaso sobre los delitos más comunes cometidos a través de las comunicaciones en redes sociales.

GROOMING

Desde el nacimiento del Grupo de Delitos Telemáticos en el año 1996, uno de sus cometidos principales y en los que se vuelcan más esfuerzos, es la protección de los colectivos más vulnerables, como es el caso de los menores. La "brecha digital que separa algunas generaciones, ha hecho que algunos padres sean incapaces de aconsejar a sus hijos acerca de las precauciones que deben tomar en la red, y que éstos no sean capaces de identificar y reconocer los potenciales peligros que les acechan. La clave para reducir estas formas delincuenciales es la prevención, en forma de educación y concienciación. La cuestión es si el resto de la sociedad está preparada y capacitada para asumir esta importante función.

El grooming (del verbo inglés groom) consiste en el progresivo acercamiento que realiza un adulto hacia un menor, ocultando su verdadera identidad y edad, para ganarse su confianza. En este contexto, y mediante su posición de superioridad psicológica sobre el menor, tratará de conseguir que éste le envíe alguna imagen o video con contenido sexual explícito. El problema resulta cuando el menor accede a esos deseos, que lejos de quedar satisfecho con esas imágenes, el problema se agrava ya que utilizará las mismas para amenazarlo con la difusión en su entorno familiar o escolar si no accede a proporcionarle nuevo material. A partir de este punto, si la víctima no denuncia los hechos a su familia o autoridades, entra en una espiral de coacciones que pueden acabar en el peor de los casos en forzar un encuentro físico y realizar abusos sobre la víctima.

En el grooming se pueden diferenciar varios elementos o fases del acoso:

1. Inicio de la fase de acercamiento. En ella se hace referencia a la primera toma de contacto con el menor de edad para conocer gustos y preferencias y poder crear una vinculación especial de amistad con el objeto de alcanzar la confianza de la víctima.

2. Inicio de la fase de relación. En esta fase se va afianzando la relación en la que se incluye con frecuencia confesiones personales e íntimas entre el menor y el acosador. De esta forma, se consolida la confianza obtenida del menor y se profundiza en información sobre su vida, gustos y costumbres.

3. Componente sexual. Con frecuencia incluye la descripción de términos específicamente sexuales y la petición a los menores de su participación en actos de naturaleza sexual, grabación de imágenes o toma de fotografías.

Para evitarlo, es necesario advertir a los jóvenes sobre este tipo de conductas, para que sólo admitan en redes sociales y chats a personas que conozcan en la vida real, teniendo en cuenta como ya hemos comentado que es posible la suplantación de todos los datos en un perfil.

CIBERBULLYING

Se trata del fenómeno conocido como ciberacoso. Lamentablemente en los últimos tiempos han salido a la luz varios casos de suicidios de menores por sufrir acoso por parte de sus compañeros. Si bien es cierto que siempre han existido casos de acoso escolar en las aulas, el ciberacoso resulta más complejo de atajar, ya que sus efectos tienen más amplitud temporal y son más difíciles de detectar si no es denunciado por la propia víctima.

Esta conducta se define como el acoso entre iguales en el entorno de las nuevas tecnologías, e incluye actuaciones de chantaje, vejaciones e insultos entre menores. En una definición más exhaustiva, se podría decir que el ciberbullying supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos.

La clave, en cualquier caso, es que se trata de una situación en que acosador y víctima son menores: compañeros de colegio o instituto y personas con las que se relacionan en la vida física.

El ciberbullying se caracteriza por los siguientes aspectos:

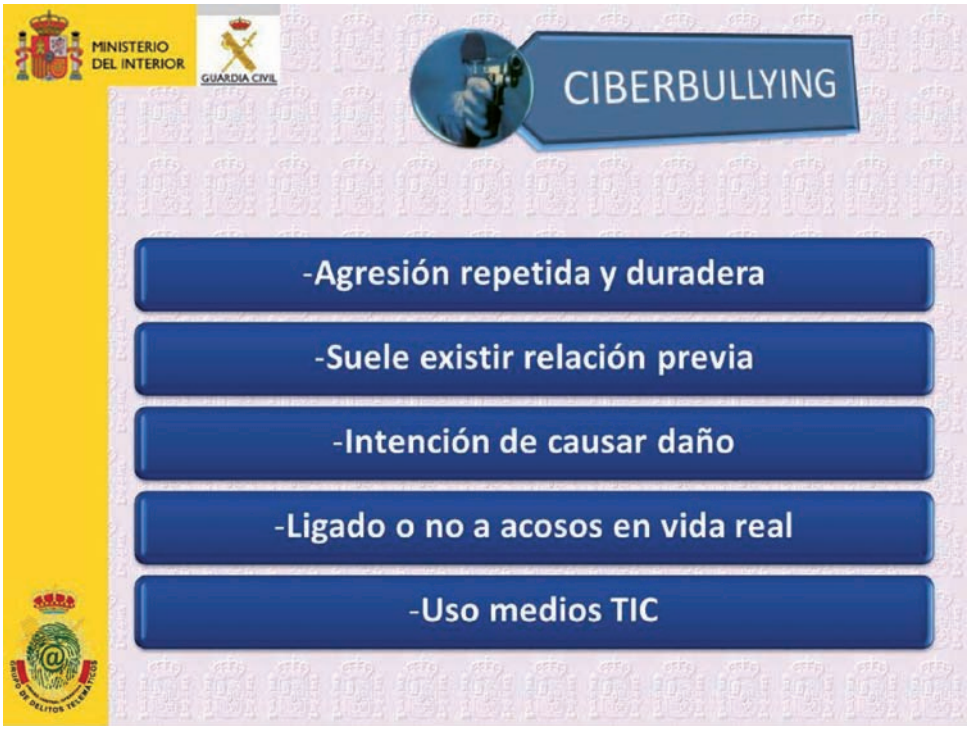
1. Que la situación de acoso sea dilatada en el tiempo. Por lo tanto quedan excluidas las acciones puntuales. Obviamente no con el fin de restar importancia a estos sucesos, los cuales pueden tener serios efectos para el afectado y constituir un grave delito, sino que al tratarse de hechos aislados no sería ciberbullying.

2. Víctimas y acosadores sean de rangos de edades similares.

3. Que la situación de acoso no cuente con elementos de índole sexual. En caso de que la situación de acoso cuente con elementos y connotaciones de carácter sexual, la situación se consideraría grooming.

4. Las víctimas y acosadores tengan previa relación o contacto en el mundo físico. Es necesario que ambas partes tengan algún tipo de relación previa al inicio del acoso electrónico. Con frecuencia, la situación de acoso comienza en el mundo real, siendo el medio electrónico una segunda fase de la situación de acoso.

5. Que el medio utilizado para llevar a cabo el acoso sea tecnológico. En este sentido, puede tratarse de Internet y cualquiera de los servicios asociados a ésta; teléfono móvil, redes sociales, plataformas de difusión de contenidos, etc...



SEXTING

El Sexting, es un término que proviene de la contracción de sex y texting, como anglicismo de nuevo cuño, y hace referencia al envío de contenidos eróticos o pornográficos a través de las nuevas tecnologías, especialmente telefonía móvil. La evolución de éstas ha propiciado nuevos canales de difusión, y se ha pasado de difundir sólo texto a través de SMS (que da origen al término), a difundir imágenes a través de mensajes multimedia MMS, y actualmente tanto foto como vídeo a través de nuevas aplicaciones de mensajería que utilizan internet, como WhatsApp.

De hecho, recientes estudios afirman que en España 2 de cada 3 menores de 10 a 16 años posee un teléfono móvil (65%), y ya en franjas de edad entre 15 y 16 años pasamos a un 89%. Casi el mismo porcentaje utiliza su teléfono para realizar fotografías, el 49% las envía a otras personas, y el 21% las publica en Internet.

Esta actividad que siempre se ha relacionado con un entorno adolescente o juvenil, la realidad ha demostrado que es realizada por personas de cualquier edad, atendiendo a los últimos casos ocurridos en España, los cuales han tenido una excesiva repercusión mediática.

Por lo tanto, la clave vuelve a ser la concienciación y educación respecto a los problemas que esta conducta puede generar, y que son los siguientes:

– Difusión del contenido sin consentimiento del afectado, vulnerando el derecho al honor y a la propia imagen, teniendo en cuenta el potencial que tiene la red para poder replicar y difundir estos contenidos de forma viral.

– Si la persona afectada es menor de edad, la persona que difunda este material estaría cometiendo un delito de tenencia y distribución de pornografía infantil, castigado en nuestro Código Penal.

– La entrega consentida de este tipo de imágenes/vídeos que suele realizarse en un entorno de máxima confianza o de pareja, se vuelve en contra con la ruptura de ésta, por lo que se contabilizan en miles los casos de exparejas que cuelgan en foros y páginas web estos contenidos como venganza.

– El fenómeno de la "sextorsión", en el cual se amenaza y coacciona con difundir estos contenidos, exigiendo en su contra el pago de una cantidad económica, o lo que es más graves, por mantener relaciones sexuales.

SUPLANTACIONES Y ROBOS DE IDENTIDAD

La facilidad que permite Internet para realizar navegación anónima y la complejidad para implementar un sistema de autenticación sencillo, confiable, robusto y económico, hacen que en numerosas ocasiones detrás de una identidad digital (perfil de red social, correo electrónico) no se encuentre la identidad real que dice ser. A todo este fenómeno que popularmente se conoce como suplantaciones o robos de identidad, nuestra legislación todavía no le da un trato diferenciado acorde con la evolución que ha tenido con el uso de las nuevas tecnologías, por lo que en la práctica, se encajan estas conductas en los tipos que ya existían con anterioridad.

Por simplificar y esquematizar la casuística, se van a exponer las posibles situaciones y el tratamiento legal que se da a cada una, por orden creciente de gravedad:

– Perfil inventado.

  En el caso de crear un perfil en una red social con datos totalmente inventados, no existe ningún tipo de reproche penal por dicha conducta. Otra cuestión diferente, es qué calificación se le otorga al formulario de registro por el que nos damos de alta en la red social, en el que se recogen los derechos y obligaciones de ambas partes, y aunque no medie precio, supone un contrato, en el cual la información aportada debe ser verídica.

– Perfil suplantado (Parodia o incompleto).

  Estos son los casos en los que se crean perfiles suplantados, generalmente a personajes públicos, con cierta notoriedad. Si de forma expresa se hace constar, o por la evidencia de los comentarios, que se trata de una parodia, tampoco encaja en el tipo penal contemplado para estos casos, que es la usurpación de estado civil recogida en el art. 401 "El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años".

Para arrojar algo más de claridad a tan escueta relación, y por qué no encajan los perfiles paródicos o incompletos en el tipo, es necesario hacer alusión a la STS 635/2009, en la que parte dice: *"Usurpar el estado civil de otro lleva siempre consigo el uso del nombre y apellidos de ese otro, pero evidentemente requiere algo más, sin que sea bastante la continuidad o la repetición en el tiempo de ese uso indebido para integrar la mencionada usurpación.*

Usurpar equivale a atribuirse algo ajeno. En la segunda acepción de nuestro diccionario oficial se dice que es "arrogarse la dignidad, empleo u oficio de otro, y usarlos como si fueran propios".

Trasladado esto al tema que nos ocupa, quiere decir que para usurpar no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden; como puede ser el obrar como si uno fuera otro para cobrar un dinero que es de este, o actuar en una reclamación judicial haciéndose pasar por otra persona, o simular ser la viuda de alguien para ejercitar un derecho en tal condición, o por aproximarnos al caso presente, hacerse pasar por un determinado periodista para publicar algún artículo o intervenir en un medio de comunicación."

– Perfil suplantado completo.

En estos casos sí que se da la tipicidad relatada en el apartado anterior. La finalidad de la misma suele ser crear un descrédito y daño en el honor e imagen de la persona suplantada, por lo que en los comentarios realizados a través del perfil suplantador suele ser habitual la relación con otras formas de delito como injurias, calumnias o amenazas.

Independientemente de los hechos en vía penal que se deriven de estas conductas, otra vía para atajar esta problemática, que se puede seguir de forma paralela ya que pertenece al ámbito administrativo, es la vulneración a la Ley Orgánica de protección de datos de carácter personal, y que se puede denunciar a la Agencia Española de Protección de Datos (AEPD) el uso y utilización de nuestros datos personales en los perfiles públicos sin nuestro consentimiento.

– Perfil robado.

Por último, en este apartado se recogen aquellas conductas en las que el perfil original de la víctima ha sido vulnerado y comprometido, por la obtención ilegítima de sus credenciales de acceso (generalmente a través de páginas de phishing o la infección con troyanos que trataremos posteriormente). En estas situaciones, si se utiliza el mismo para suplantar al propietario original concurriría el apartado anterior del delito de usurpación de estado civil, con otro de descubrimiento y revelación de secretos, por el acceso no autorizado a la información que contiene el usuario en su perfil de forma privada.

DISTRIBUCIÓN DE MALWARE

Igual que ha ocurrido con el correo electrónico tradicional, las redes sociales se han erigido como una fuente fundamental de difusión y propagación de malware y spam.

Dicho malware se suele vincular a contenidos de foto/vídeo atractivos, o a los llamados "hoax" (bulos en la red), sabedores que así tendrán una rápida y viral propagación.

Mención especial merecen las direcciones acortadas, que se utilizan masivamente en la red Twitter para ahorrar espacio de caracteres, comot.coo bit.ly, que se utilizan en forma de hipervínculo a la url final, sin que previamente podamos tener idea sobre qué dirección están apuntando, por lo que hacer click en una de estas direcciones sin conocer la confiabilidad de la persona que ha puesto el enlace es potencialmente peligroso.

Una vez infectado nuestro equipo, el atacante pasará a tener el control total del mismo, sin que nosotros percibamos ningún efecto adverso en el mismo. El principal uso que se da a los troyanos es el robo de nuestra información personal, especialmente la relacionada con datos bancarios. Se han creado varias familias de troyanos que se denominan bancarios, como *Zeus y SpyEye* para recuperar información sobre credenciales bancarios y tarjetas de crédito y enviarlos a un repositorio controlado por los delincuentes. Estos troyanos también sirven para vulnerar nuestra intimidad, ya que incorporan módulos para almacenar pulsaciones del teclado (keylogger), generar capturas de pantalla, abrir el micro o incluso activar nuestra webcam de forma remota.

Si el troyano con el que hemos sido infectados está diseñado para que constituyamos parte de una red de ordenadores zombies, llamada botnet, a partir de ese momento nuestro equipo pasará a ser parte de un ejército de miles o millones de máquinas que el atacante tiene a su disposición para realizar actividades ilícitas. Las órdenes son transmitidas a través de un panel de control (C&C) y a parte de recopilar información personal, se utilizan estas botnets para realizar denegaciones de servicio distribuidas (DDOS), envío de spam, clickfraud, etc.

Para evitar ser infectado, es fundamental tener el sistema y las aplicaciones convenientemente actualizadas y parcheadas, un buen antivirus y cortafuegos, y no abrir archivos adjuntos ni pinchar enlaces que nos infundan desconfianza. Igualmente debemos evitar instalar aplicaciones "piratas", *cracks, keygens,* ya que la mayoría vienen con un regalo no deseado.

FRAUDES Y ESTAFAS

Al igual que como he visto en la distribución de malware, las redes sociales se han constituido como un nuevo canal de difusión para que los ciberdelincuentes puedan hacer llegar a sus potenciales víctimas sus tentativas de estafa y engaños. No son formas nuevas, ya que la mayoría de los modus operandi ya existían, pero sí se utilizan estos canales acompañados de una gran carga de ingeniería social.

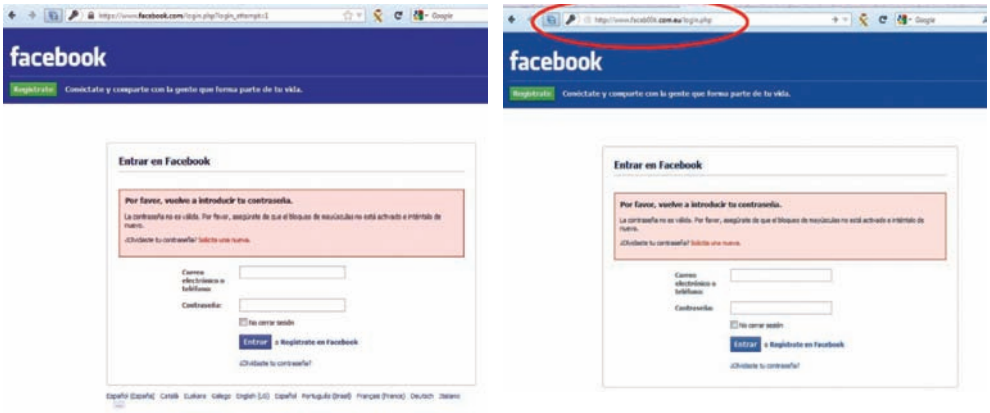
Sin abandonar los ya de sobra conocidos "fraudes nigerianos" (gracias a los cuales supuestamente hemos ganado un gran premio en un sorteo o lotería, un pariente desconocido nos deja una suculenta herencia o nos ofrecen una gran inversión) están incrementando los asociados a números de tarificación adicional y SMS Premium, así como aquellos relacionados con las aplicaciones de juegos en redes sociales en los que se pueden obtener mejoras a cambio del pago de una cantidad de dinero.

PHISHING

El phishing, básicamente consiste en conseguir redirigir al usuario a una página copia que suplanta la real, para que introduzca su usuario y contraseña. Todos estos datos son alojados en el servidor a disposición del ciberdelincuente, que los utilizará para enviar spam, extraer nuestra información personal, e incluso chantajearnos por devolvernos el perfil o por no difundir el contenido privado que tengamos alojado en el mismo.

El phishing de páginas de acceso a correo webmail y redes sociales, está proliferando por la sencillez en su elaboración y menores precauciones que toman los usuarios al introducir sus datos respecto a las tradiciones de phishing de entidades bancarias. En la propia red podemos encontrar tutoriales e incluso "kits" con las páginas ya prediseñadas para realizarlo.

Como medida de seguridad básica, consiste en verificar la url en el navegador del portal de acceso en que vamos a introducir nuestra contraseña, sobre todo si hemos sido redirigidos desde otra página, generalmente de escasa reputación.



Hay que prestar especial atención a los caracteres, ya que una técnica especialmente utilizada consiste en sustituir algunos de ellos por símbolos muy similares, como la O por el 0 de este ejemplo real.

CONTENIDOS NOCIVOS

Dentro de este apartado, es necesario incluir las conductas y contenidos que circulan por la red, que si bien no están tipificados en el Código Penal y por lo tanto no son perseguibles, sí que tienen un reproche social y debería haber cierto control sobre los mismos para que no pudieran acceder los menores de edad a ellos de forma sencilla.

La mayoría de las veces se antepone el derecho a la libertad de expresión sobre todo, sin tener en cuenta que estos contenidos pueden perjudicar el desarrollo de los menores. El concepto nocivo puede variar en función de las diferencias culturales y las diferencias individuales de los usuarios (edad, madurez intelectual, cultura, ideología, creencia religiosa, etc.).

Entre los mismos, podríamos hacer un catálogo interminable de situaciones en los que se publican imágenes y vídeos de situaciones de violencia extrema, homicidios y asesinatos, automutilación, maltrato animal, pornografía adulta como banners de publicidad en páginas comunes, apologías, etc.

Especial atención merece las conductas calificadas como apología de la anorexia y bulimia (ProAna y ProMía) por varios motivos. En primer lugar, la creación de páginas web, foros y perfiles en RR.SS. constituyen un punto de encuentro que no hace más que reforzar la conducta de forma negativa, de tal forma que los afectados por la enfermedad piensan que no es tan malo lo que hacen si hay tantas personas que se encuentran en su misma situación y les dan apoyo moral. En segundo lugar, recopilan listas de consejos o "tips" para evitar que los familiares puedan detectar la enfermedad a tiempo, así como para minimizar los efectos de la comida.

Este caso constituye un claro ejemplo de por qué es tan necesario homogeneizar y armonizar legislaciones internacionalmente en los aspectos relacionados con la red. Si en España se incluyera en el Código Penal esta apología como delito, y por lo tanto se pudie-

ran retirar y cancelar estos contenidos de la red, de poco serviría si nuestros adolescentes pueden seguir accediendo a las páginas y perfiles de usuarios de Latinoamérica que publican lo mismo en su mismo idioma.

De momento, y mientras los legisladores se siguen poniendo de acuerdo para perfilar ésta y otras muchas más situaciones que no tienen un tratamiento legal adecuado, hay que seguir apelando a la autorregulación los prestadores de servicios en Internet, los cuales en muchos casos y por cuestiones de responsabilidad corporativa, acceden de forma voluntaria a retirar contenidos a petición de Fuerzas y Cuerpos de Seguridad.

Otro de los aspectos negativos, es lo que se conoce como "Internet Use Disorder", y es un trastorno de conducta, por el uso excesivo de Internet en general o redes sociales en particular, que puede desembocar en una dependencia y adicción a las TIC. Estas conductas han resultado catalizadas por la masiva implantación de tablets y smartphones, que permiten disponer de conectividad en cualquier momento y situación, por lo que cada vez resulta más complicado desconectar de la red.

Estas situaciones afectan cada vez más a los jóvenes, también llamados "nativos digitales", que han crecido y evolucionado con estas tecnologías, y que no sólo utilizan la red, sino que viven en ella. Para reconducir estos trastornos, es fundamental el papel que desempeñan padres y educadores, para mostrarles otras vías de ocio y socialización, que eviten el paso de tantas horas frente al ordenador o dispositivo móvil.

DECÁLOGO DE NAVEGACIÓN SEGURA

1. Actualice de forma regular el sistema operativo y las aplicaciones que utilice más a menudo, especialmente las de las familias Java, Adobe, y Office.

2. Utilice un navegador actualizado y considere el empleo de extensiones que bloqueen la ejecución de Scripts automáticos. Además evite cualquier enlace que pudiera parecer sospechoso, sobre todo aquellos cuyo certificado digital no es correcto.

3. Elija diferentes contraseñas seguras (largas y alfanuméricas) para cada servicio de Internet. O al menos una distinta para los diferentes ámbitos de su actividad en Internet (una para las cuentas de correo personal, otra para actividades económicas, otra para las Redes sociales,...etc.) De esta forma le será más sencilla que recordar decenas de contraseñas diferentes y evitar reutilizar la misma contraseña para todo.

4. Verifique regularmente los movimientos de su cuenta bancaria y sus tarjetas de crédito, de esta forma detectará rápidamente los fraudes y podrá bloquearlos. Si su entidad lo permite, establezca alertas de aviso a su móvil de transacciones extrañas o cuantiosas.

5. Utilice un antivirus con licencia y actualizado (existen varios que son gratuitos), e Instale un firewall en su equipo (muchos SO´ s lo traen por defecto) para evitar accesos no autorizados. Aun así, no los remplace por su sentido común y no ejecute archivos sospechosos.

6. Considere la posibilidad de utilizar un único dispositivo para las transacciones de banca y comercio electrónicos (PC, Smartphone, Tablet,...etc.). Así podrá saber rápidamente cómo han robado sus credenciales.

7. Desconfíe de los mensajes cortos y extraños que pueda recibir por redes sociales, o correos electrónicos de desconocidos, sobre todo si éstos incluyen un enlace para acceder a otro contenido. Incluso si provienen de contactos conocidos pueden resultar peligrosos. Compruebe que sus contactos son los auténticos remitentes del mensaje, y no introduzca sus datos personales en formularios dudosos o sospechosos.

8. No piense que es inmune al software malicioso porque utilice un determinado sistema operativo o un dispositivo portátil. Las aplicaciones de Smartphone se han convertido en un objetivo para lo desarrolladores de virus y troyanos. Los proveedores están constantemente revisando sus "markets" para limpiarlos de aplicaciones maliciosas.

9. No confíe ciegamente en las aplicaciones de seguridad instaladas, éstas no remplazan a la navegación responsable ni a la prudencia del usuario.

10. Si dispone de un router inalámbrico para conectarse a internet, cambie las contraseñas por defecto y establezca una más segura. No utilice el cifrado WEP, e incluso configure el router para que solo se puedan conectar al mismo determinados ordenadores.

EN DEFINITIVA, UTILICE EL SENTIDO COMÚN COMO MEJOR ANTIVIRUS Y NO CONFÍE CIEGAMENTE EN LOS SISTEMAS Y SUS APLICACIONES

Ciberseguridad-Ciberamenazas

PONENCIA DE D. JUAN ANTONIO GÓMEZ BULE
LICENCIADO EN CIENCIAS POLÍTICAS Y SOCIOLOGÍA POR LA
UNIVERSIDAD COMPLUTENSE DE MADRID
PRESIDENTE DEL CONSEJO ASESOR

PARTICIPA DIRECTAMENTE EN EL CONSEJO DE ADMINISTRACI N DE LA COMPAÑ A. ADICIONALMENTE, ES RESPONSABLE DE LA UNIDAD DE NEGOCIO S21SEC E-CRIME DEDICADA A LA PREVENCIÓN DEL FRAUDE EN INTERNET, LA VIGILANCIA DIGITAL DE LAS ORGANIZACIONES Y LAS PERSONAS Y LA INTELIGENCIA EN SEGURIDAD DONDE COLABORA EN LA CONSOLIDACIÓN DE SU ESTRATEGIA, DESARROLLO Y CRECIMIENTO.

APORTA MÁS DE 25 AÑOS DE EXPERIENCIA PROFESIONAL COMO EMPRESARIO Y DIRECTIVO EN EL ÁMBITO DEL ÁREA DE LA SEGURIDAD Y DE LAS TECNOLOGÍAS DE LAS COMUNICACIONES QUE LE HAN LLEVADO A OCUPAR EL CARGO DE DIRECTOR GENERAL DE LAS EMPRESAS DEL SECTOR DE SEGURIDAD Y LA VICEPRESIDENCIA DE LA MULTINACIONAL SUIZA ASCOM.

MIEMBRO DEL CLUB DE ROMA, CONSEJERO DEL INSTITUTO CHOISEUL EN ESPAÑA, MIEMBRO DE LA CÁTEDRA DE SERVICIOS DE INTELIGENCIA EN LA URJC, MIEMBRO DEL INSTITUTO DE CIENCIAS FORENSES Y DE LA SEGURIDAD (ICFS) DE LA UAM, ENTRE OTROS.

ASESOR DEL MADOC Y PRESIDENTE DEL GRUPO DE TRABAJO EN EL CESEDEN "NECESIDAD DE UNA CONCIENCIA NACIONAL SOBRE CIBERSEGURIDAD. LA CIBERDEFENSA, UN RETO PRIORITARIO."

RECIENTEMENTE ES NOMBRADO PRESIDENTE, DENTRO DEL CESEDEN, DEL GRUPO DE "CONCIENCIACIÓN SOBRE LA NECESIDAD DE UNA ESTRATEGIA DE CIBERSEGURIDAD Y CIBERDEFENSA PARA ESPAÑA".

BINOMIO CIBERSEGURIDAD Y CIBERAMENAZAS

Bajo este binomio desarrollaré cómo estos dos conceptos han transformado nuestra vida y nuestra percepción de la realidad. Primero, es preciso, determinar cuál es su significado. De esta forma entendemos Ciberseguridad según la expresa en la Recomendación UIT-T X.1205:

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

En cuanto a la definición de Ciberamenaza podríamos definirla como la adaptación de la definición de la amenaza realizada a través de internet:

" El mal ha de ser posible, en el sentido de que el destinatario puede tener motivos para creer en su verosimilitud. Que el mal sea impuesto significa que el amenazado no tiene control sobre los hechos que lo desencadenarán, por tanto, su culminación depende exclusivamente del sujeto activo. El hecho previsto ha de tener una clara repulsa social. Finalmente la determinación viene dada por la expresión cierta de un hecho. La ***amenaza*** *tiene la finalidad de causar inquietud en el amenazado produciéndole un estado o un ánimo de miedo."*

Podemos identificar cuatro grandes grupos de ciberamenazas: ciberespionaje, ciberdelitos, ciberactivismo y ciberterrorismo. Para prevenir, mitigar y reaccionar frente a estas amenazas es preciso investigar esta nueva forma de interrelación social. Entender esta realidad implica un esfuerzo cognitivo e interpretativo que va más allá de los aspectos evidentes. Internet es el vehículo de una sociedad hiperconectada donde hemos modificado nuestros hábitos de vida, de relación y de desarrollo personal.

El cambio social que estamos experimentando permite estudiar, no sólo a los investigadores sociales, sino a profesionales de cualquier disciplina, identificar y vislumbrar modelos nuevos de integración y desintegración social. Pero también los modelos tradicionales de comportamientos adoptan los nuevos vehículos para permanecer vivos en la sociedad. Sirva de ejemplo para este último caso la adopción por parte del crimen organizado del uso intensivo de herramientas tecnológicas para expandir su acción a través de este nuevo medio. Medio que ya hemos categorizado como "el quinto espacio", adoptando y adaptando la terminología militar de los espacios a defender, a saber: tierra, mar, aire, espacio y ciberespacio.

Este Ciberespacio donde no hay regulación, ni límites geográficos genera un problema de interpretación de los conflictos según los paradigmas históricos. Las capacidades de defensa ante incidentes por parte del Estado, están en jaque. Hemos de entender que las organizaciones burocráticas como el Estado, tiene mecanismos de supervivencia frente a cambios de modelo, como podría decir Max Weber, y se encuentran "incómodas" frente a revoluciones como la que estamos experimentando. El Estado ha de dar cumplida respuesta a una de las necesidades básicas de los ciudadanos, sean entidades físicas o jurídicas, y una de ellas es la Seguridad. Y estamos hablando de proporcionar a la ciudadanía una satisfacción a su "Percepción de Seguridad".

Según el Libro Blanco francés de 2008:"La globalización está transformando profundamente los cimientos mismos del sistema internacional. La tipología de amenazas y los riesgos en el siglo XXI requieren una redefinición de los términos de seguridad nacional e internacional donde la complejidad y la incertidumbre emergen como las principales características del nuevo entorno... Peligros de naturaleza más volátil y menos predecible, incluyendo los atentados terroristas, la proliferación nuclear y de otras armas de tecnologías avanzadas, ciberataques."

El concepto "Ciberseguridad" se ha integrado en nuestra vida diaria, la adopción de medidas frente a los riesgos inherentes a la exposición a las redes sociales de nuestros hijos, la vulneración de identidades en internet, la suplantación de éstas, el robo, la estafa, el ataque a la reputación, el ataque a infraestructuras críticas, el espionaje ... hace que los destinatarios de las ciberamenazas sean el global de la sociedad y se haya "democratizado" el destinatario, ya que a todos nos ha colocado el riesgo en plano de igualdad, siendo categorizados en función del interés del atacante .

Estados, empresas, universidades, ciudadanos en general estamos ante este radar. Para gestionar este tipo de riesgos es preciso una serie de elementos como la formación permanente, la concienciación de ciudadanos y del Estado, el desarrollo de tecnologías fiables y generar un espacio de colaboración donde lo público y lo privado puedan desarrollar espacios que den cumplida respuesta a lo que es un objetivo común: la Seguridad, un objetivo de todos.

España está desarrollando la Estrategia Española de Ciberseguridad, enmarcada en la Estrategia Nacional de Seguridad para España. El papel de las Fuerzas y cuerpos de Seguridad del Estado y, en concreto de la Guardia Civil, frente a estas amenazas, muchas de ellas no recogidas en nuestro ordenamiento jurídico, hace que su formación y desarrollo de competencias en estas materias tenga una importancia fundamental.

Se ha convertido en imprescindible el entendimiento de estas necesidades como dice la Estrategia de Seguridad de Estados Unidos: "la infraestructura digital es un recurso nacional estratégico y su protección una prioridad de seguridad nacional. Disuadiremos, prevendremos, detectaremos, nos defenderemos contra y nos recobraremos rápidamente de las ciberintrusiones y ataques: invirtiendo tanto en personal (campaña de concienciación sobre cibersegurdiad) como en tecnología para mejorar la protección y aumentar la "resiliencia" de los sistemas y redes gubernamentales y empresariales. Reforzando la cooperación entre el sector privado y el Gobierno y a nivel internacional (normas, leyes, protección de datos, defensa de redes y respuesta a ciberataques".

"Las amenazas a la ciberseguridad representan uno de los retos más graves relacionados con la seguridad nacional, la seguridad pública y los retos a los que se enfrenta la nación. Nuestra vida diaria depende de la energía y de las redes eléctricas, pero adversarios potenciales podrían usar nuestras ciber-vulneralbilidades para interrumpir el suministro a escala masiva. Las amenazas a las que nos enfrentamos van desde hackers individuales a grupos de delincuencia organizada, desde redes terroristas a avanzados estados-nación.

Estamos asistiendo a conflictos entre Estados distintos a los históricamente estudiados, donde la interconexión entre elementos en apariencia inconexos y las diferencias en

el modelo de acción se han puesto de manifiesto. Términos como asimetría y globalización se ha convertido en elementos fundamentales para entender este tipo de fenómenos.

La soberanía nacional, considerada como la salvaguarda de la soberanía e integridad del territorio nacional y sus habitantes permitiendo el desarrollo de su libertad, de su actividad personal, económica y social que, a su vez, limita sustancialmente o evita, los efectos de riesgos internos y externos. Siguiendo estas líneas de actuación, la salvaguarda por parte del Estado de estas libertades hace que se tengan que tomar todo tipo de medidas para hacer frente a esta situación, considerando que no es únicamente tarea del entorno público sino también del entorno privado, es decir, que para la salvaguarda de la Seguridad del país hay que considerar que esta tarea es una tarea de todos.

La seguridad de las infraestructuras críticas frente a las ciberamenazas

Ponencia de D. Fernando Sánchez Gómez
Director del Centro Nacional de Protección de Infraestructuras Críticas
Oficial de la Guardia Civil
Diplomado de Estado Mayor

Ha desarrollado sus funciones en los últimos años en el campo de la seguridad de infraestructuras e instalaciones de car cter estratégico en la Direcci n General de la Policía y la Guardia Civil, Dirección Adjunta Operativa (Estado Mayor).

En su cargo actual ejerce como coordinador en la elaboración y desarrollo de la normativa española sobre protección de infraestructuras críticas (Ley 8/2011, Real Decreto 704/2011 y sus planes derivados). De la misma manera ha participado en representación española en las discusiones en el seno de la Comisión Europea para la redacción de la Directiva 114/2008 sobre protección de las infraestructuras críticas europeas.

Es el Punto de Contacto del Estado Español con la Unión Europea en materia de protección de infraestructuras críticas, y participa habitualmente en diversos grupos de trabajo, nacionales e internacionales, en dicho campo.

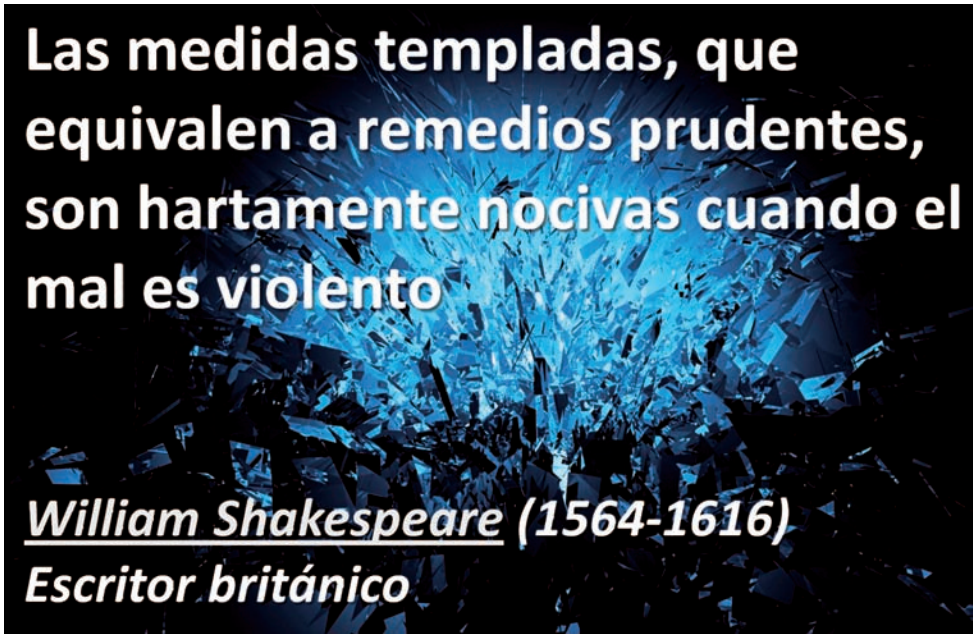
Colabora asiduamente en la impartición de diferentes cursos y masters relacionados con defensa y seguridad, organizados por la UNED, la Universidad politécnica de Madrid, la Universidad Camilo José Cela, la Universidad Europea de Madrid, la Universidad Carlos III, el Instituto Universitario de Investigación Ortega y Gasset o el Centro Superior de Estudios de la Defensa Nacional, entre otros.

GENERALIDADES

Nos enfrentamos a un cambio de época. Un cambio de época que supone un salto cualitativo en nuestra manera de ver y enfrentarnos al mundo; un cambio de paradigmas en el que los avances que experimentamos son tan rápidos y profundos que están transformando nuestro mundo en tan sólo unos pocos años... para bien, y también para mal...

Los avances tecnológicos que están propulsando a la sociedad postindustrial a situaciones más propias de ciencia ficción, donde el control absoluto de los procesos y sistemas se pueden conseguir con tan sólo pulsar un botón, comienzan ya a ser una realidad tangible; pero también se empiezan a manifestar unas amenazas que, a caballo de las nuevas tecnologías, están haciendo acto de presencia en las sociedades avanzadas.

La interacción entre los conceptos de protección de infraestructuras críticas y ciberseguridad hace que nos planteemos escenarios en los que las probabilidades de que se produzcan daños a gran escala que afecten, no sólo a las instituciones de gobierno y a la economía global de un país, sino a todos y cada uno de sus ciudadanos, son cada vez más altas. Todo análisis de riesgos que se efectúe al respecto debe considerar todas las hipótesis, tanto las más probables como también las más peligrosas, y dado que las potenciales consecuencias en el ámbito que nos ocupa pueden llegar a ser catastróficas, es preciso abordar la situación de forma decidida y poniendo los recursos necesarios.



En palabras del célebre William Shakespeare, *"las medidas templadas, que equivalen a remedios prudentes, son hartamente nocivas cuando el mal es violento"*. Dicho de una manera más castiza y actual, yo convendría en acordar con el gran escritor inglés que, cuando las consecuencias a las que nos enfrentamos pueden ser graves (y éstas lo son), es preciso "coger el toro por los cuernos" y aportar cuanto antes soluciones prácticas y estrategias firmes que nos permitan enfrentarnos al problema con la seriedad que éste demanda. Veremos a continuación el por qué de todo ello.

Para hacernos una idea cabal del escenario en el cual nos debemos desenvolver quisiera recurrir a un símil que nos va a trasladar a la antigua Grecia y a su mitología: Según

la leyenda, al principio de los tiempos, una vez que el gran Zeus, padre de los dioses, hubo creado el Universo y la Tierra, éste se encontraba tan cansado que decidió delegar la creación del Reino Animal en dos de sus Titanes, unos seres poderosos que descendían de Urano (el Cielo) y de Gea (la Tierra).

Nuestros protagonistas, que a la sazón eran hermanos, se llamaban Prometeo y Epimeteo. Y así ambos comenzaron su titánica labor de tal manera que, mientras que Prometeo moldeaba al animal en cuestión y lo dotaba de vida mediante un leve soplo, Epimeteo completaba el trabajo otorgándole una serie de dones que aplicadamente iba sacando de un gran cofre del cual era único custodio. A las aves les concedió la capacidad de volar, a los peces la de nadar y poblar los océanos, a los felinos astucia y fiereza...

Pasaron los días y la labor estaba casi completada, pero les faltaba algo... y ese algo tenía que ser especial. Entonces, a Prometeo se le ocurrió la brillante idea de crear a un ser que fuera a imagen y semejanza de los mismísimos dioses; ya está: ¡le llamarían Hombre!

Sin embargo, cuando llegó el momento de dotar al Hombre de sus cualidades, Epimeteo se encontró con que el cofre de los dones se encontraba ya casi vacío... no había nada especial con lo que igualar tan magnífica apariencia, puesto que los principales regalos ya los había repartido.

Fue Prometeo, el más avispado de ambos hermanos, el que encontró una vez más la solución: en una osada acción, subió al monte Olimpo y, mientras Zeus y el resto de dioses dormían, aprovechó para robar el Fuego del carro de Helios. ¡Ya tenía el Hombre su

don especial! De esta manera, el ser humano se convirtió en el rey de la Creación y es, hasta hoy, el dominador absoluto del resto de las especies...

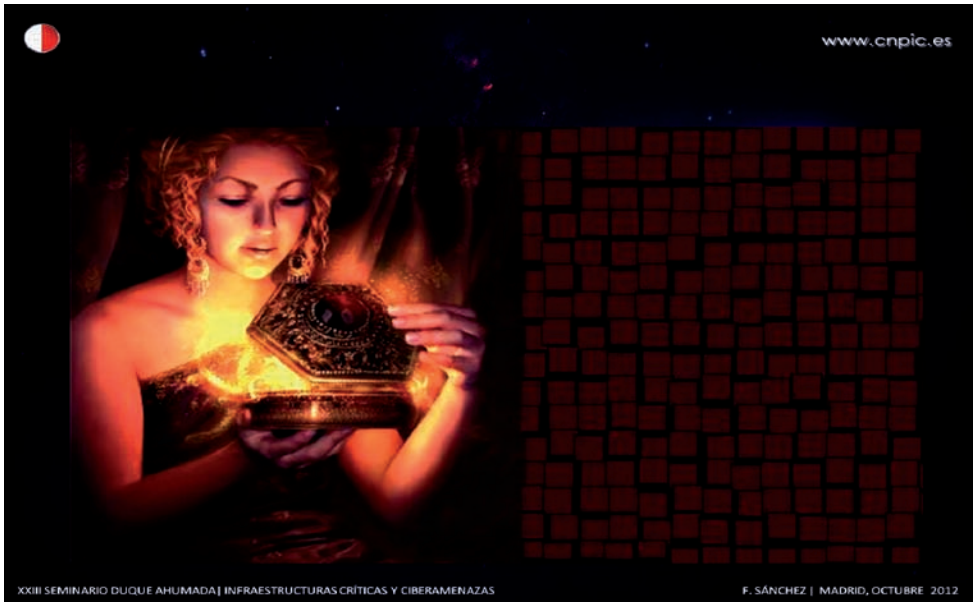
Cuando Zeus descubrió la añagaza, montó en cólera. No podía ya deshacer el entuerto, pero sí que podía tomar cumplida venganza, ¡y vaya si lo hizo!: Prometeo, como instigador principal, fue inmediatamente encadenado de por vida (y, teniendo en cuenta que los Titanes eran inmortales, eso era toda una eternidad) a una montaña en el lejano Cáucaso, donde un águila le devoraba el hígado por la mañana, hígado que volvía a regenerarse durante la noche, y así día tras día. Pero esa es otra historia...

El castigo para Epimeteo fue mucho más sutil. Dice la leyenda, que Zeus decidió pagar con la misma moneda y así creó, moldeado por Atenea y Hefesto y con la ayuda de todos los dioses, a un nuevo ser, más bello y perfecto por supuesto que el propio Hombre: así nació la Mujer, a la que se puso por nombre *Pandora*.

Y a Pandora la envió Zeus a la Tierra con una nueva caja de dones bajo el brazo para que se la entregara a Epimeteo, ya que los dones, como sabemos, se le habían acabado.

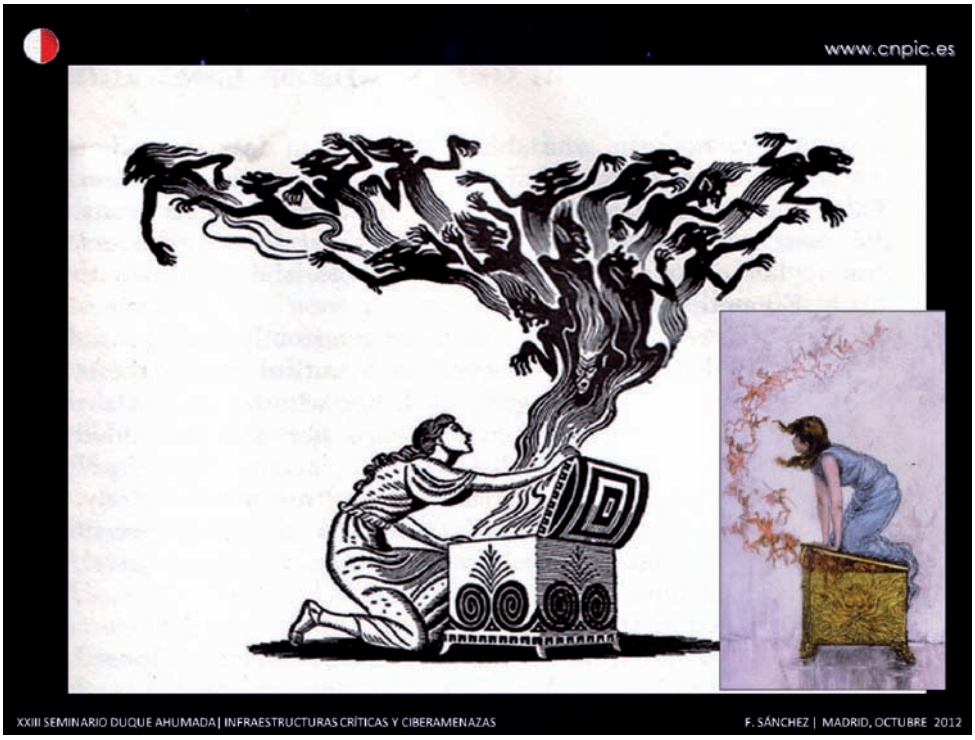
A pesar de que el desdichado Prometeo le había aconsejado a su hermano, mientras partía a su destierro, que no aceptara regalos de Zeus, Epimeteo pronto sucumbió a los encantos de Pandora y la hizo su esposa, recibiendo de paso la misteriosa cajita, que el Padre de los dioses ya le había categóricamente indicado a aquélla que jamás abriera, puesto que sólo Epimeteo estaba capacitado para ello.

Al principio todo fue bien, pero a pesar de las advertencias de Zeus o, tal vez, precisamente por ello, Pandora no se pudo resistir a echar una miradita al interior de la caja y, un día que Epimeteo se encontraba fuera, la mujer levantó con precaución la tapadera y empezó a mirar por la rendija que se abría...



¡Ante ella comenzaron a desfilar toda una suerte de magníficos dones, los bienes divinos, ligeros y efímeros, que se fueron filtrando al exterior y elevándose por el aire: el amor, la paz, la salud, la nobleza, la juventud, la belleza...!

Tan emocionada se hallaba Pandora ante tantos y tan bellos dones, que abrió sin darse cuenta la caja de golpe y sin tomar las precauciones adecuadas, y entonces comenzaron a salir con fuerza otras cualidades mucho más maléficas que, al ser más pesadas que las anteriores, se habían quedado más atrás, pero que inmediatamente empezaron a arrastrarse a ras del suelo: el odio, la enfermedad, la guerra, la injusticia, la envidia, la codicia, la muerte... Pandora intentó con todas sus fuerzas cerrar la caja, pero ya era tarde: las plagas y desventuras se habían propagado ya por toda la Tierra, y desde entonces continúan asolándola.



Por ello, y desde aquel momento, el género humano, se ve obligado a convivir con el Bien y con el Mal, que son las dos caras de una misma moneda. Desde entonces, también, el mito de la *Caja de Pandora* permanece entre nosotros como testimonio vivo de la dualidad de todos nuestros actos.

A lo largo de la historia de la Humanidad han existido muchas otras cajas de Pandora: unas se abrieron, otras no... Si tuviéramos que establecer unos rasgos comunes entre todas ellas, podríamos reconocer que, mientras que le han proporcionado, o proporcionan aún, grandes avances y beneficios para el ser humano, por contra son también responsables de

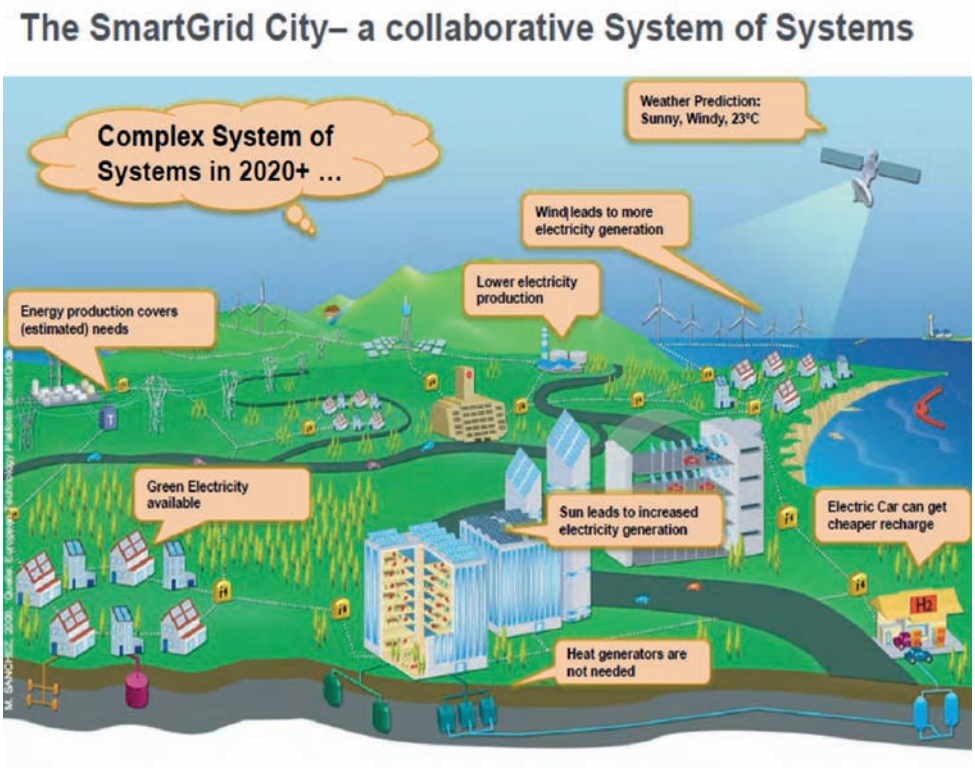
no pocos graves perjuicios con los que debemos coexistir por no haber utilizado correctamente las nuevas herramientas, los nuevos "dones" puestos a nuestra disposición. Piénsese si no, por ejemplo, en la industrialización y en sus consecuencias... ¡quién le iba a decir a James Watt, allá por el s. XVIII, que su máquina de vapor iba a traer consigo muchos años después, el Progreso (con mayúsculas)... y la destrucción de la capa de ozono, y de millones de kilómetros cuadrados de masa forestal, también!

Pero, sin duda, *nuestra actual Caja de Pandora son las Tecnologías de la Información y las Comunicaciones, más conocidas como TIC*. Los avances experimentados en los últimos años por nuestra sociedad postindustrial no tienen parangón en la historia de la humanidad. Nos han permitido tener acceso a una vida mucho más cómoda y gestionar mejor nuestros negocios y nuestro ocio; somos capaces de acceder a una enorme cantidad de información en tiempo real a cualquier hora del día, podemos comunicarnos con amigos o familiares y hacer negocios con lugares situados en el otro lado del globo... En definitiva, hemos conseguido una calidad de vida impensable hace unos años y no digamos por nuestros antepasados. Y aún existe mucho potencial por delante que explotar, estamos ante lo que se suele denominar "la punta del iceberg".

Uno de los ejemplos de hacia dónde nos podríamos encaminar con la implantación generalizada de las TIC es la *ciudad del futuro, o Smart City* (Ciudad Inteligente), cuyo horizonte puede ser de tan sólo unos años desde este momento. Una *Ciudad Inteligente* del

futuro estará gestionada por un complejo sistema de sistemas informatizado, que dirigirá también sus procesos energéticos a través de lo que ya se conoce como *Smart Grids* (Redes Inteligentes).

Las *Smart Grids* ya son un hecho, se encuentran en pleno proceso de implantación en muchos países, entre ellos España, y no son sino una nueva red de energía que se está construyendo sobre las instalaciones existentes, a base de implantar dispositivos de información y comunicaciones; es decir, se trata del proceso mediante el cual las redes de energía se proveen de elementos capaces de monitorizar, controlar y gestionar los procesos relativos a la generación, transmisión, distribución y consumo de energía eléctrica.



La *Ciudad Inteligente* del futuro podría ser, por tanto, algo parecido a la imagen en pantalla: eficiente energéticamente, compatible y respetuosa del Medio Ambiente al integrar energías verdes, económica y limpia... siempre y cuando seamos capaces de implantarla salvaguardando su propia seguridad, porque...

... otro escenario plausible, de no abrir correctamente nuestra particular Caja de Pandora, bien podría ser aquel que se nos ofrece en películas futuristas apocalípticas al estilo de Mad Max. Y esto nos lleva, por cierto, al concepto de *infraestructura crítica:*

Desde siempre han existido determinadas instalaciones o infraestructuras cuya protección ha sido necesario asegurar, ya que su pérdida o destrucción podría suponer un quebranto de gravísimas consecuencias para las sociedades a las que servían. Estas instalaciones han sido objetivo preferente de organizaciones terroristas al ofrecer, en muchas ocasiones, un blanco fácil y de gran rentabilidad.

La expansión del Estado del Bienestar en los países desarrollados y la revolución que ha supuesto el nacimiento de las nuevas tecnologías desde los años ochenta ha ido creando unas sociedades acostumbradas a un alto y cómodo nivel de vida, con múltiples e inmediatos servicios a su disposición, derivados de unos elevados índices de producción que descansan sobre unas sólidas infraestructuras.

Para el *Centro Nacional para la Protección de las Infraestructuras Críticas de España (CNPIC)* el concepto primario, el aspecto clave desde el que hay que partir, no es tanto la infraestructura en sí, sino la función que ésta desempeña o el servicio que presta.

Es decir, son determinadas funciones (los servicios esenciales) las que, a nuestro juicio, merecen el calificativo de críticas y a partir de ahí, mediante el estudio de las instalaciones, las redes y los procesos de trabajo por los que se desarrollan estas funciones, podremos determinar si alguna de las infraestructuras sobre las que operan reúne las características precisas para ser considerada de una manera especial.

Estos *servicios esenciales* están estructurados en nuestro país en *12 grandes sectores estratégicos,* desde la energía o el agua, hasta la salud, el transporte y, por supuesto las telecomunicaciones.

Sobre todo ello, me atrevería a hacer tres reflexiones fundamentales:

1. Nuestro país, nuestra sociedad hipertecnificada, es *extremadamente dependiente* de esto que denominamos infraestructuras críticas o, mejor, de los servicios esenciales que éstas proporcionan. No hay actividad de gobierno, económica, social o humana, que no se encuentre vinculada o dependa, de una u otra forma, de alguno de estos servicios.

Esto nos hace enormemente *vulnerables,* ya que estamos acostumbrados a, con un simple "click", obtener de forma automática, agua, luz, calor, información, imágenes, sonido... Es impensable que todo esto pudiera desaparecer de la noche a la mañana, ¿verdad? Reflexionen tan sólo qué sucedería si, de golpe y porrazo retrocediéramos, ya no a la Edad Media, sino a principios del s. XX... sin teléfono, sin ordenador, sin televisión, sin radio, sin tarjetas de crédito no cajeros automáticos...¡¡¡sin electricidad ni agua corriente!!! ¿Sería esto posible alguna vez?

Y las perspectivas de futuro son que *las infraestructuras críticas serán cada vez más críticas* porque, además, cada vez seremos más dependientes de ellas.

2. Los servicios esenciales y las infraestructuras críticas que los soportan son dependientes entre sí. Es el concepto de *interdependencia:* el correcto funcionamiento de un determinado servicio condiciona la prestación de otro(s), desarrollándose una cadena cuya protección global tiene la protección del eslabón más débil. Así, la inhabilitación de un determinado servicio o infraestructura podría provocar la caída en cadena de otros, pudiendo originar, en un caso extremo, un efecto dominó de imprevisibles consecuencias.

Y las perspectivas de futuro nos indican que las *interdependencias serán cada vez más fuertes,* porque la conexión entre servicios es cada vez mayor.

3. Por último, horizontal a todo esto, y *como nexo de unión cada vez más importante, se encuentran las TIC,* a través de las que se dirigen, gestionan y explotan la mayoría de las infraestructuras críticas y sus procesos productivos.

Y las perspectivas de futuro, como ya hemos podido apreciar, son que las TIC serán responsables, en un horizonte ya muy próximo, del funcionamiento global de una sociedad en la que la conectividad de sistemas y elementos se contará por billones.

El ciberespacio es peligroso: el potencial que ofrece para mejorar nuestra vida puede ser también aprovechado para hacer el mal. Y las fuentes desde donde puede provenir este mal son múltiples y muy variadas, así como sus modalidades, sus motivaciones y la información y los recursos con los que pueden contar estos potenciales *depredadores de la Red*.

No obstante, a grandes rasgos, y sin tener en cuenta la infinidad de factores y matices que intervienen en su parametrización, podrían esbozarse, grosso modo, tres grandes bloques de amenazas para y desde el ciberespacio, encarnadas por:

– **Delincuentes:** Que actúan con un móvil fundamentalmente económico y que ocupan en cuanto a número de actividades el primer puesto entre todos los agentes de la amenaza. Su impacto sobre la sociedad es muy heterogéneo, abarcando desde delincuentes individuales y pequeños fraudes hasta delitos a gran escala realizados por grandes redes criminales (en relación con el robo de información de tarjetas de crédito o de certificados digitales, con el fraude telemático sobre operaciones bancarias o transacciones desde Internet, con el blanqueo de dinero y con el robo de identidades asociado a inmigración ilegal, por citar tan sólo algunos ejemplos).

– **Hacktivistas:** De carácter preferentemente ideológico/antisistema, organizados en torno a pensamientos o ideas más o menos radicales, generalmente poco estructurados y con conocimientos técnicos de carácter muy dispar, lo que no impide que lleguen a poseer la capacidad de llevar a cabo acciones potencialmente muy dañinas.

Sus acciones incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollos de software, entre otras. El año 2011 ha puesto de manifiesto la importancia de la interacción entre los activistas del mundo físico y los hackers del mundo electrónico. Así, el pasado año, en determinadas campañas centradas en los acontecimientos políticos y sociales se ha evidenciado la coordinación cada vez mayor entre ambos sectores, lo que ha tenido como consecuencia un mayor impacto en el resultado de las acciones.

– **Estados/Gobiernos:** Cuya motivación es de carácter político/estratégico. El ciberespionaje es posiblemente la actividad más desarrollada a día de hoy, tanto contra la información sensible de los gobiernos como aquella referente a desarrollos tecnológicos o industriales, con un componente esencialmente económico; pero tampoco son infrecuentes las acciones de sabotaje que podrían conducir incluso, en casos extremos, a la ciberguerra (ciberguerra que, en opinión de algunos expertos, ya se está desarrollando encubiertamente en algunos teatros de operaciones). La participación de los servicios de inteligencia de los Estados, de las unidades cibernéticas de sus Fuerzas Armadas y de grandes compañías multinacionales confiere a todo ello una especial gradación, al estar dotados de grandes medios y recursos técnicos y de una gran capacidad de acción. Sus actividades son muy prolongadas en el tiempo y el tipo de herramientas que utilizan normalmente muestran unos niveles muy bajos de detección en los sistemas de seguridad de los objetivos.

De forma transversal a todo ello, y con posibilidades de ser realizadas por cualquiera de estos grupos, de una u otra manera, y con una u otra motivación, están las *posibilidades de ataques terroristas valiéndose de la Red: Y la peor de las hipótesis es, precisamente, un ataque contra nuestras infraestructuras críticas*.

Las posibles víctimas de las ciberamenazas son, evidentemente, las mismas que se benefician de los avances de las TIC: todos nosotros o, al menos, todos aquellos que hacen uso de la Red para la administración y la gestión pública, para los negocios y los procesos de trabajo y, en fin, para el desarrollo de su vida diaria.

Cada día, millones de *ciudadanos* en España utilizan las Tecnologías de la Información y las Comunicaciones en su actividad diaria (búsqueda y envío de información, compra y venta de bienes y servicios, formación, participación en redes sociales, banca electrónica...). De igual forma, las *Administraciones Públicas* dependen de estas tecnologías, tanto como base de su funcionamiento interno como de los servicios que prestan a los ciudadanos (el 95% de los servicios públicos ya están operativos a través de Internet). Por su parte, las *empresas* mantienen un uso intensivo de las TIC como soporte de su negocio y como motor de crecimiento y creación de nuevas oportunidades.

Por todo ello, estos *tres tipos de actores hemos de tener nuestra cuota de responsabilidad,* cada cual a su nivel y en su ámbito de actuación. Porque por nosotros, y porque a través de nosotros, la sociedad se puede poner en riesgo.

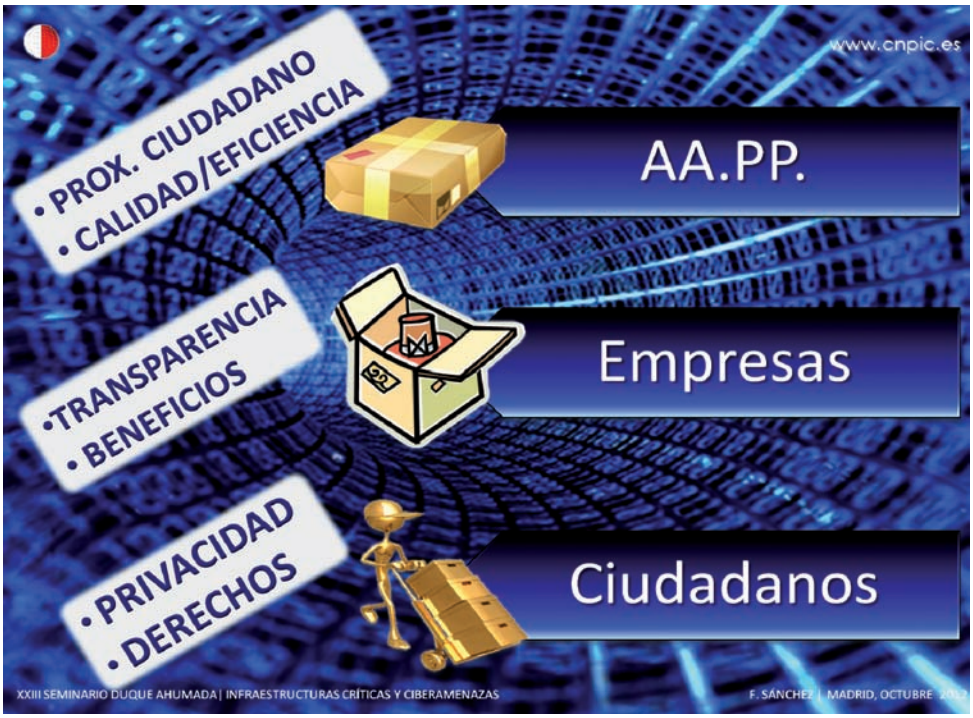
Además, es preciso resaltar que cada uno de estos grupos tenemos nuestras propias *Cajas de Pandora,* entendidas éstas como algo que, siendo intrínsecamente bueno y beneficioso, pueden suponer, si no se utilizan de forma racional y adecuada, una vulnerabilidad, una posible vía de ataque contra nuestros propios intereses.

Ejemplos de estas virtudes cuyo mal empleo puede ser contraproducente podemos encontrarlos en las Administraciones Públicas y en muchas empresas, donde se proporciona en ocasiones un *exceso de información accesoria o innecesaria* que, bajo el paraguas de los principios de transparencia o de cercanía al ciudadano, pone al alcance de cualquiera datos sensibles para la propia organización, que bien pudieran emplearse en su contra.

Es frecuente encontrar, en las páginas corporativas de Internet de muchas organizaciones, referencias a su estructuración interna, activos, contratos y licitaciones, fotografías y hasta planimetría, fruto de una falta de rigor a la hora de cribar aquella información que es sensible de la que no lo es.

Lo mismo se podría decir respecto al *componente económico*. La obtención de beneficios a toda costa, o el manido recurso en tiempos de crisis como el actual de la contención del gasto son, en otras tantas ocasiones, una muestra de mala gestión dado que, tanto una cosa como la otra, se pueden llevar a cabo con una adecuada planificación, con organización y con análisis de riesgos adecuados. Lo que sí es evidente es que la seguridad cibernética de los activos de una organización debe ser considerada como un valor añadido, en lugar de cómo una rémora económica... y, en algunos casos, aún no se ha llegado a ese convencimiento.

Y respecto a nosotros mismos, los ciudadanos, otro tanto se podría decir; ¿quién, entre nosotros, no dispone de uno o varios ordenadores, smart phones, u otros dispositivos electrónicos? El consabido recurso a *"hago lo que quiero con él, porque es mío",* aún siendo un derecho más que legítimo, no debería ser una excusa para descargar aplicaciones en *páginas piratas,* emplear productos de cuestionable seguridad y no llevar a cabo unas mínimas medidas de seguridad sobre nuestros equipos informáticos.



Como base de todas estas conductas se puede identificar un problema, más cultural y social que otra cosa: Tenemos, como sociedad una grave carencia de conocimiento de la realidad a la que nos enfrentamos y, por lo tanto, adolecemos de una terrible *falta de conciencia* sobre las consecuencias que nuestra conducta puede arrostrar y, por supuesto, de la responsabilidad que tenemos, como gestores públicos, como empresarios y, por supuesto, también como ciudadanos.

CIBERTERRORISMO E INFRAESTRUCTURAS CRÍTICAS

En cualquiera de los casos, y poniendo ahora el acento, como no puede ser de otra forma dentro del foro en el que nos encontramos, en la *cibercriminalidad* (entendida ésta, en sentido amplio, como la realización de actividades delictivas y/o terroristas utilizando o teniendo como fin las nuevas tecnologías), podríamos establecer una serie de parámetros y características diferenciales en comparación con la criminalidad "clásica" o "tradicional", que nos puede llevar a entender más fácilmente la razón por la cual su proliferación está siendo tan elevada:

Así, como ventajas para el ciberdelincuente frente al delincuente "físico", podríamos encontrar:

– La mayor seguridad, en general, para cometer sus actividades, debido al escudo que en la mayoría de los casos se crea con el anonimato que ofrece estar cómodamente sentado tras un ordenador, careciendo por ello de un riesgo personal inminente.

– La posibilidad de actuar en cualquier parte del mundo, con un ámbito geográfico prácticamente ilimitado.

– La mayor repercusión mediática en cuanto a la propaganda de sus acciones (si le conviene) y, en todo caso, la facilidad de utilizar la Red para actividades de información, proselitismo y comunicación.

Por lo tanto, si tradujéramos estos datos a un idioma púramente comercial, podríamos convenir en que la *relación coste (riesgo) - beneficio* es, simplemente, *óptima*.

Ahora bien, no todo va a ser ventajas para el ciberdelincuente en relación con su competidor "tradicional". Como inconvenientes podemos apuntar:

– La falta de dramatismo de sus acciones, dramatismo que perjudica fundamentalmente a aquellos que buscan en la repercusión mediática una caja de resonancia para conseguir sus objetivos (terroristas, por ejemplo).

– La falta de control de los resultados dado que, una vez que se lanza un ataque, no en todos casos se puede dirigir y encaminar por los delincuentes.

– La necesidad de amplios conocimientos técnicos, lo cual hace que esta modalidad delincuencial necesite de un grado de preparación y tecnificación que no está al alcance de cualquiera. Pero, dicho esto, es preciso reconocer que las nuevas generaciones que se van incorporando a nuestra sociedad tienen un grado de especialización informática que, poco a poco, va a ir convirtiendo este hecho en una "ventaja", ya que la mayor parte de los delincuentes contará, en los próximos años con una formación mucho más exhaustiva en la materia. Además, se va extendiendo la modalidad de "comprar servicios ciberdelincuenciales", lo que se conoce como *Malware As A Service,* o MAAS, que no es sino una forma de alquilar a expertos informáticos para realizar actividades delictivas.

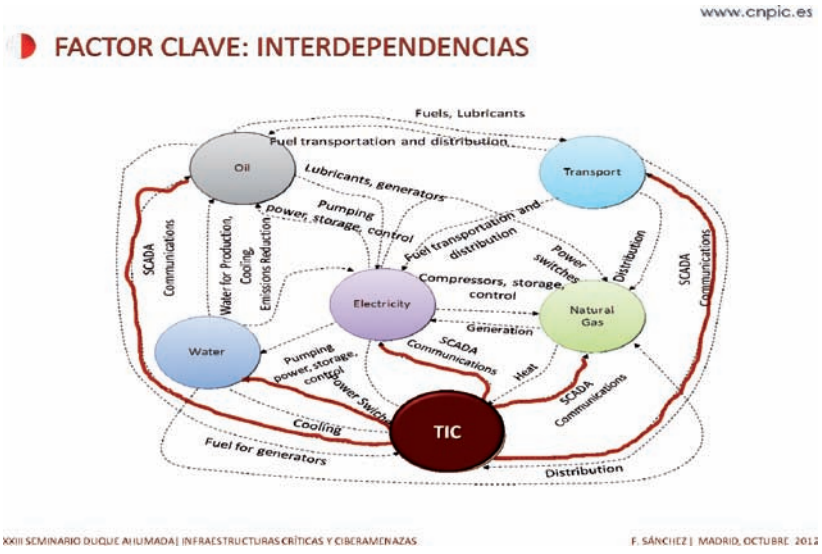
Si enlazamos, por tanto, las características de la cibercriminalidad, en su sentido más amplio y, fundamentalmente, del ciberterrorismo, con las circunstancias especiales en las que se desarrollan nuestras infraestructuras críticas, podemos identificar en éstas una serie de *debilidades intrínsecas que pueden contribuir a hacerlas más vulnerables* ante eventuales ataques cibernéticos realizados contra ellas:

– La amplia interconexión entre ellas, o interdependencia, y la posibilidad de causar efectos en cascada.

– La cada vez mayor dependencia tecnológica, en todos los aspectos, pero fundamentalmente en aquellos elementos que dirigen sus operaciones (los *SCADA*, de los que hablaremos más tarde).

– La posibilidad de crear efectos psicológicos amplificadores. La caída en cascada de sistemas, la sensación de que "las cosas no funcionan" puede ser una herramienta de primer orden para causar el pánico y la desconfianza de la población hacia el sistema político y los gobiernos. La hipótesis más peligrosa en lo que se refiere a los efectos de una acción terrorista consistiría precisamente en la realización de ataques concertados convencionales con los de carácter cibernético.

– Por último, hay que destacar la terrible vulnerabilidad en la que nos puede introducir el concepto, cada vez más desterrado, pero existente a día de hoy entre algunos responsables de seguridad del concepto de *"seguridad por oscuridad":* Hasta hace poco, muchos operadores "suponían" que el desconocimiento de las tecnologías que operaban un sistema industrial era un factor suficiente como para minimizar el riesgo (técnica del avestruz). Actualmente, la convergencia hacia una tecnología abierta y estandarizada hace que este comportamiento ya no sea sólo eficaz sino peligroso. Y esto afecta fundamentalmente aquellos sistemas e infraestructuras con una edad media/avanzada.



Hace unos minutos me refería a los *SCADA* como aquellos elementos especialmente sensibles en la mayoría de infraestructuras críticas a la hora de ser sometidos a un hipotético ataque cibernético; abundaré un poco más en ello.

Los SCADA (acrónimo en inglés de *Sistemas de Control y Adquisición de Datos*) son una aplicación de software especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos) y controlando el proceso de forma automática desde la pantalla del ordenador. Los SCADA se componen normalmente de una serie de elementos:

– El *Controlador de Sistemas,* o *PLC (Programmable Logic Controller):* El principal elemento de todos ellos. Es un sistema encargado de gestionar las lecturas de los dispositivos de campo agrupados en una cierta área concreta, *"traducir"* las medidas (pasando, por ejemplo, de una medida analógica a información digital) y, en su caso, de *"ordenar"* a los dispositivos de campo que lleven a cabo alguna acción.

– Los RTU (Remote Terminal Unit), o dispositivos de campo, que actúan como sensores encargados de obtener mediciones sobre un elemento industrial.

– El MTU (Master Terminal Unit): Un sistema central encargado de centralizar y analizar la información proveniente de los sistemas anteriores, con capacidad de ver todo el mapa de la infraestructura, y de determinar acciones a más alto nivel.

En el ámbito que nos ocupa, la peor de las hipótesis se daría en el caso de que un supuesto atacante tuviera la capacidad de simular las órdenes de los PLC hacia los dispositivos de campo y, dado que estos últimos no tienen capacidad de "pensar" lo que están haciendo, lo hicieran sin más. En este escenario, se podría llegar a alterar gravemente los procesos llevados a cabo por el sistema, llegando incluso a ocasionar la *destrucción física del mismo y a la paralización de los servicios esenciales* que proporciona la infraestructura en sí.

1945 está ampliamente reconocido como el año en el que la *Industria Nuclear "perdió su inocencia"*. Hasta ese momento, aunque su capacidad destructiva era sobradamente conocida, la tecnología nuclear era una novedad, una promesa que ofrecía un potencial prácticamente ilimitado para obtener energía no contaminante, a bajo precio y mucho más eficiente que los métodos existentes hasta ese momento. Con el lanzamiento de *Little Boy* sobre Hiroshima, y de *Fat Man,* sobre Nagasaki, en los últimos estertores de la II GM, el mundo entero quedó horrorizado con el potencial aniquilador nuclear.

2010 es el año en el que muchos expertos y analistas del ciberespacio convienen en señalar como el de la *"pérdida de la inocencia" de las TIC,* debido al potencial destructivo que el *"malware"* diseñado y extendido causó en millones de equipos, sistemas e infraestructuras. Y, desde entonces, la naturaleza de los ciberataques ha evolucionado de forma dramática, tanto en términos de frecuencia como en su sofisticación y agresividad. Por aportar tan sólo algunos ejemplos:

– **OPERACIÓN AURORA (enero 2010):** además de Google, otras 34 empresas multinacionales sufrieron robo de información a través de un "malware". El link al que muchos empleados dieron *click* provocó que dentro de sus computadoras se instalara un "troyano", es decir, un software malicioso que se instaló en la máquina del usuario casi en secreto, y que sin avisar, instaló un programa que permitió el acceso remoto de un usuario no autorizado para copiar la información contenida en su ordenador.

– **WIKILEAKS (a partir de abril de 2010):** La organización se ofrece a recibir filtraciones que desvelen comportamientos no éticos por parte de gobiernos, con énfasis en los países que considera tienen regímenes totalitarios, pero también de religiones y empresas de todo el mundo. Las actividades más destacadas de WikiLeaks se centraron en la actividad exterior de los Estados Unidos, especialmente en relación con las guerras de Irak y de Afganistán.

– **STUXNET (junio 2010):** Fue el primer rootkit (un programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones) para sistemas *SCADA*. Su vía de infección principal fueron las llaves USB, en lugar de la infección "tradicional" por Internet. Explotaba hasta 4 vulnerabilidades "día-0", para sistemas Microsoft / Windows y utilizó múltiples contramedidas para evitar su detección. Por su sofisticado diseño, parece haber sido desarrollado por un equipo profesional experto durante un largo período de tiempo. Afectó fundamentalmente a Irán y a su programa nuclear.

– **NIGHT DRAGON (febrero 2011):** Destinado a la explotación de vulnerabilidades de Microsoft Windows, que empieza a aprovechar debilidades de la red externa (extranet) y a través de un sostenido proceso de ataques que involucra distintos programas chinos orientados al hackeo que están disponibles en la Dragón Nocturno logró invadir distintos servidores de petróleo, gas y petroquímica, comprometiendo a empresas y ejecutivos de Holanda, Estados Unidos, Kazajistán, Taiwán y Grecia.

– **ZeuS (abril 2011):** Malware bancario que se extiende rápidamente por Internet a través de plataformas de intercambio de archivos o ciertas páginas web. La liberación de su código fuente ha convertido al troyano ZeuS en lo que podría denominarse un "kit de cibercrimen de código abierto". Sus versiones derivadas y mejoradas han seguido siendo fuente de problemas en 2012.

– **DUQU (octubre 2011):** El objetivo de Duqu, con numerosas similitudes con el troyano Stuxnet, era reunir datos sensibles de algunas organizaciones -tales como fabricantes de componentes- del sector del control industrial. Los autores de Duqu buscaban información relativa a documentos de diseño para ayudarlos a organizar un futuro ataque a una planta de control industrial.

Como colofón, por tanto, de esta segunda parte, me aventuro a concluir que:

– Las nuevas tecnologías, las TIC, son un *fenómeno constante y creciente en el entorno terrorista*.

– *Internet es vulnerable,* y permite la navegación de depredadores que están al acecho para causar daño, con una y otra motivación, y de maneras muy diversas.

– Internet, como *instrumento terrorista* es una realidad contrastada; como *medio terrorista* es una herramienta de primer orden; y, como *objetivo terrorista,* está en sus inicios, involucrando de lleno a las infraestructuras críticas.

– Por lo tanto, el riesgo cibernético sobre nuestras infraestructuras críticas y los servicios esenciales para la población es *real,* aunque se trate aún de un escenario emergente pero creciente en agresividad y tipología.

Estamos cerca de ese momento en el que los entornos hacker y los grupos terroristas pueden cruzar sus caminos. *Dejaremos entonces de hablar de amenazas para hablar ya de realidades*.

ACCIONES EN CURSO

El abordaje de esta problemática es, como se puede ver, de carácter complejo y multidisciplinar, con un cierto parecido a la resolución de un rompecabezas:

Es necesario llevar a cabo medidas, no sólo de clases completamente diferentes y a niveles distintos (normativo, estratégico, operativo, formativo...), sino por parte de actores distintos, aquéllos que de una u otra forma tienen un grado de responsabilidad y conocimiento en la materia, y en la medida que le corresponda.

El Gobierno y las Administraciones públicas deben promover las medidas legislativas que favorezcan la seguridad de nuestro ciberespacio, e impulsar estrategias que fijen las líneas maestras del uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar a nuestro país su seguridad y progreso, a través de la adecuada coordinación de todas las Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos, canalizando las iniciativas y los esfuerzos internacionales en defensa del ciberespacio.

Se trata de implantar, en fin, una *conciencia de responsabilidad compartida y de coordinación* que haga encajar todas las piezas sin dejar espacios de vulnerabilidad.

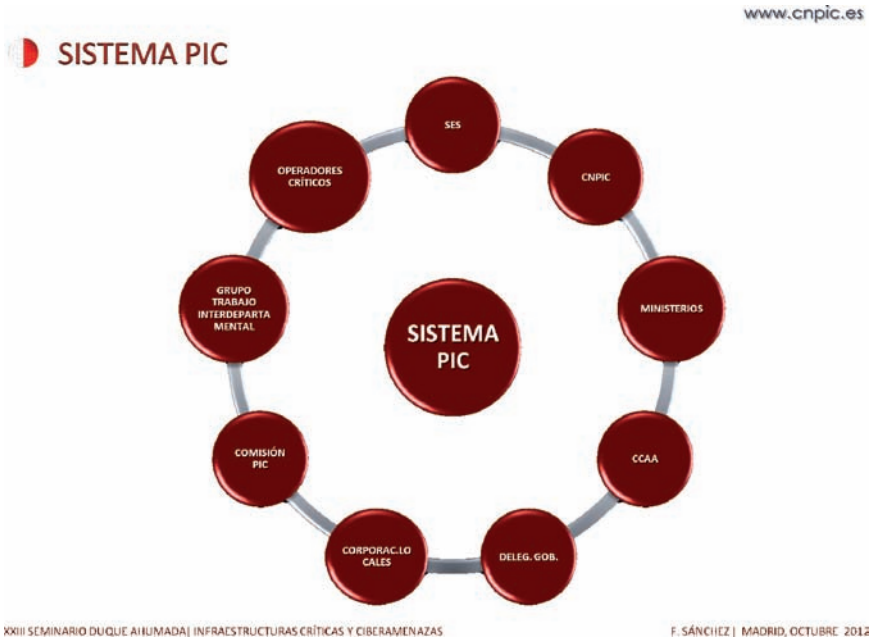
Precisamente es la *concienciación la pieza esencial* de todo el entramado, y la piedra angular sobre la que se debe construir este edificio. Una concienciación que estamos todos obligados a impulsar en una doble dirección: Por un lado, los *Altos Cuadros de Mando,* entendiendo éstos como las Autoridades y dirigentes políticos en la Administración, y los Consejos de dirección, Presidentes y altos directivos en las empresas; por otro, los propios *individuos,* de manera que cale en la ciudadanía una conciencia de seguridad en los productos, contenidos y actividades que llevan a cabo en su vida cotidiana.

Es una tarea ingente intentar proteger a la sociedad contra tantas posibles amenazas, imprevisibles e inimaginables. Para ello se requiere cooperar, compartir información, evaluar riesgos potenciales y asignar y priorizar los recursos humanos, materiales y económicos racionalmente. Nuestro reto consiste en proteger a la sociedad de riesgos y amenazas potencialmente ilimitados, pero con recursos materiales, humanos y económicos limitados, y esto sólo es posible mediante la coordinación de esfuerzos entre todos los agentes implicados. Este es precisamente el fundamento y el impulso que pretende la *Ley de Protección de Infraestructuras Críticas 8/2011,* y el sistema que promueve desde el Ministerio del Interior.

El *Sistema Nacional de Protección de Infraestructuras Críticas,* pionero en España y en la vanguardia de las tendencias existentes a nivel internacional, contiene aquellas instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. Es de destacar dentro de este *Sistema PIC* el papel que juegan los operadores críticos, es decir, aquellos que gestionan al menos una infraestructura crítica. El Sistema Nacional debe definir el conjunto de estrategias y de iniciativas necesarias para dirigir y coordinar las actuaciones de los distintos órganos responsables. A tal fin, el Sistema impulsará la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras con el fin de optimizar su grado de protección y de contribuir a la seguridad de la población.

Obviamente, este sistema debe descansar sobre el establecimiento de lazos sólidos de cooperación entre los operadores de nuestras infraestructuras y los órganos dedicados a la protección y a la seguridad de los ciudadanos. Sólo sobre esta base de confianza mutua podremos edificar una adecuada estructura de seguridad.

De la misma manera, el Gobierno publicó en junio de 2011 la *Estrategia Española de Seguridad,* actualmente en revisión, donde se identifican las amenazas y riesgos contra la seguridad de nuestro país sobre *6 ámbitos diferentes:* Terrestre, marítimo, aéreo, espacial, *ciberespacio* e informativo. La Estrategia Española de Seguridad detecta 10 amenazas principales, para las cuales establece una serie de *líneas de acción,* así como las organizaciones responsables de llevarlas a cabo. Desde el punto de vista del Centro Nacional para



la Protección de las Infraestructuras Críticas, aquellas relacionadas con el terrorismo, las ciberamenazas y las infraestructuras críticas son las más relevantes, y se está trabajando intensamente sobre las mismas.

De la misma manera, y con el fin de dar respuesta al gran desafío que supone preservar el ciberespacio de todo tipo de riesgos y ataques, defendiendo los intereses nacionales y contribuyendo al desarrollo de la Sociedad Digital, el Gobierno de España está impulsando la elaboración de una *Estrategia Española de Ciberseguridad* que, partiendo de la Estrategia General, sirva como marco de referencia de un modelo integrado que garantice a nuestro país su seguridad y progreso. El Ministerio del Interior forma parte del grupo de trabajo al que se ha encomendado su redacción.

La Estrategia Española de Ciberseguridad deberá asentarse sobre unos principios básicos que permitan un crecimiento ordenado, coherente y cohesionado de las acciones que sea necesario desarrollar para la mejora de la ciberseguridad y la ciberdefensa, que deberá contemplar, entre otros, los siguientes:

1. Seguridad Integral.

A pesar de que el entorno tecnológico se ve afectado por una serie de amenazas propias de su naturaleza, no se debe olvidar que al fin y al cabo siguen siendo vulnerables frente a las amenazas más comunes provenientes del entorno físico tradicional. Por lo tanto, para una adecuada mejora de la ciberseguridad se debe fomentar y asegurar el trabajo conjunto de los responsables en ambos campos de acción, siempre que dichas responsabilidades estuviesen divididas.

2. Responsabilidad compartida.

Teniendo en cuenta que la seguridad es una necesidad básica del ser humano, y que la seguridad pública es competencia primordial del Estado, en el caso de la ciberseguridad se imponen una serie de restricciones que hacen necesaria la implicación de terceros, de modo que únicamente se podrá garantizar una adecuada ciberseguridad si todos los agentes aceptan su responsabilidad en la materia y se trabaja de forma conjunta y cohesionada.

Para ello es necesario el establecimiento de tres vías de coordinación: Entre las Administraciones Públicas, entre los sectores público y privado, y a nivel internacional.

3. Respuesta Coordinada.

Contar con el establecimiento de mecanismos que aseguren la implicación de los agentes oportunos, y que faciliten una respuesta coordinada con el objetivo de que las acciones que se lleven a cabo sean totalmente efectivas. Del mismo modo, esta respuesta coordinada debe ser extensible a las relaciones que se establezcan en el ámbito internacional.

4. Proporcionalidad.

Las acciones que se deban llevar a cabo en caso de un incidente cibernético se basarán en el criterio de proporcionalidad, garantizando en todo caso los derechos fundamentales de los ciudadanos.

5. Educación y Concienciación.

Teniendo en cuenta que cada vez es más elevado el empleo de tecnologías de la información y comunicaciones por parte de los ciudadanos, es fundamental que éstos cuenten con unos conocimientos básicos sobre ciberseguridad que redunden en una mejora en el

uso de este tipo de sistemas. Fomento de campañas de concienciación dirigidas a aquellos usuarios de sistemas tecnológicos relacionados con las infraestructuras críticas, adecuadas al grado de responsabilidad que tengan en su uso u operación.

6. Desarrollo de la Industria.

Es fundamental para una mejora de la seguridad nacional fomentar el desarrollo de productos donde la seguridad sea un aspecto esencial desde las primeras fases de diseño. Para ello se fomentará la aplicación de los estándares oportunos en cada caso.

7. I+D.

Es necesario fomentar la Investigación y el Desarrollo en materia de ciberseguridad, con el fin de realizar una tarea proactiva que permita adelantarse a posibles eventos que puedan poner en riesgo la seguridad nacional, y para proteger de forma adecuada las infraestructuras críticas.

Termino ya. Y lo hago tal y como empecé, volviendo a la historia de *Pandora y su Caja:* Dice la leyenda que, cuando Pandora pudo por fin cerrar el cofre de donde se habían escapado todos los dones y las plagas que contenía, hubo tan sólo una cosa que quedo en el fondo, y se mantuvo (y aún se mantiene) durante la eternidad. ¡Ese algo no era otra cosa que la *Esperanza*!

Por eso, se dice que lo último que se pierde es siempre la esperanza, que se mantiene

como apoyo y sustento del ser humano, y que le evita caer en el fatalismo de un sino contra el que hay que luchar. Por eso se dice también que, mientras hay vida, hay esperanza.

Creo sinceramente que aún no hemos llegado a abrir completamente nuestra Caja de las TIC, y que estamos aún a tiempo para ser capaces de explotar los extraordinarios beneficios que nos ofrecen las nuevas tecnologías sin recibir a cambio las plagas que pueden traer asociadas. Pero para esto es preciso actuar ya, y actuar todos, cada cual a su nivel, y sin egoísmos, intereses ni protagonismos indeseables, siendo conscientes que sólo desde la responsabilidad compartida y la sinergia de todos podemos alcanzar nuestros objetivos.

Al menos, yo mantengo la esperanza en todo esto.

Retos presentes y futuros en materia de ciberseguridad

Ponencia de D.ª María José Caro Bejarano
Licenciada en Informática

Analista del IEEE (Instituto Español de estudios Estratégicos). Fue responsable de la Unidad de Documentación Técnica y Métodos de Ensayo del Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI) del Instituto Nacional de Técnica Aerospacial (INTA).

Ha participado en las primeras evaluaciones de la seguridad de las tecnologías de la información realizadas en España, tanto con los criterios ITSEC como con los Common Criteria, contribuyendo a la acreditación del CESTI como laboratorio de evaluación.

Tiene experiencia en la evaluación de sistemas para Defensa, cifradores, dispositivos seguros de creación de firma y productos para la creación de infraestructuras de clave pública y en la empresa privada como Ingeniero de Software en diversos proyectos espaciales y de defensa.

El *ciberespacio* se considera ya un nuevo ámbito junto con los tradicionales ámbitos de tierra, mar, aire y espacio, donde pueden presentarse amenazas a la seguridad.

El avance de la tecnología y en particular la relacionada con la información y las comunicaciones, las TIC, nos ha permitido avanzar hacia una conectividad global. Ya nos resulta imposible imaginar un mundo sin conectividad.

Las TICs ejercen una creciente influencia en la economía, en los servicios públicos y en la vida de todos los ciudadanos, la estabilidad y prosperidad de un país dependen de la seguridad y confiabilidad del ciberespacio, por ello, debe evitarse su compromiso por agresiones deliberadas.

Las nuevas tecnologías e Internet son motores de competitividad y prosperidad, pero al tiempo que crece nuestra dependencia de la tecnología, aumenta también nuestra vulne-

rabilidad ante la creciente amenaza en el mundo digital, ante el uso o ausencia de esa tecnología.

La Estrategia Española de Seguridad aprobada en junio de 2011, considera precisamente los peligros tecnológicos como uno de los potenciadores de riesgo, que son factores que "propician la propagación o transformación de las amenazas y riesgos e incrementan nuestra vulnerabilidad . Y una de esas amenazas identificadas en la estrategia es la ciberamenaza.

Las ciberamenazas pueden materializarse debido a un uso malintencionado o incorrecto de las incesantes innovaciones que se producen en el terreno de las TIC, tecnologías de la información y la comunicación.

Existen factores legales y tecnológicos que aumentan las posibilidades de que las *ciberamenazas* se materialicen. Entre los legales, destaca la ausencia de una legislación común o de seguridad global que permita una lucha más efectiva contra ellas. El factor tecnológico permite una interconexión creciente de redes, sin embargo, Internet, que se creó para ser útil y sencillo, adolece de seguridad. En esta red de redes los ataques se escudan tras el anonimato y la dificultad de atribución, lo que dificulta su neutralización.

Las amenazas tradicionales parecen haber acuñado el prefijo ciber y así se habla de nuevos términos como ciberterrorismo, ciberdelincuencia, ciberespionaje, cibersabotaje, ciberguerra o ciberconflicto. También la seguridad ha recibido el prefijo ciber para referirnos a la ciberseguridad como la seguridad en el ciberespacio.

Los agentes o actores que están detrás de estas ciberamenazas son diversos: Estados, actores no estatales, grupos de crimen organizado, individuos aislados, individuos organizados, "hacktivistas", es decir, activistas ideológicos o políticos por Internet, etc.

Además de la diversidad de los atacantes son también variadas las motivaciones de los ataques: espionaje industrial y económico, sabotaje, terrorismo, robo de datos, suplantación de identidad, motivación económica, contrainteligencia, etc.

Las víctimas u objetivos también han ido variando pero se ven afectados todos los sectores de la sociedad: servicios públicos y privados, empresas y ciudadanos, pero en especial, últimamente los más atacados son las infraestructuras críticas y sectores estratégicos, es decir, el objetivo último de los ataques vienen siendo las empresas, su patrimonio tecnológico y de conocimiento.

El impacto económico es considerable, aunque no existen datos fiables y comparables, se puede mencionar como ejemplo, una estimación realizada por el Reino Unido que cifra la pérdida económica anual en 27.000 millones de libras esterlinas como consecuencia de los diferentes ataques a la ciudadanía, compañías y entidades gubernamentales, o el último estudio del Instituto Ponemon y HP que estima en 3,2 millones de dólares las pérdidas por el cibercrimen en ese mismo país.

La sofisticación de los ataques ha crecido, de modo que se ha evolucionado de los iniciales virus, troyanos y gusanos que simplemente accedían a cualquier sistema o red sin

mayor objetivo que demostrar su vulnerabilidad haciéndose visibles. Desde hace unos años nos enfrentamos a amenazas más sofisticadas y complejas, las conocidas APT o amenazas persistentes avanzadas, que son ataques dirigidos a un objetivo específico con una motivación concreta y que presentan incluso una arquitectura modular para adaptarse al tipo de objetivo y de ataque.

Ejemplo de estas amenazas más sofisticadas son el gusano Stuxnet que en 2010 afectó a los sistemas de control de una central nuclear iraní; en 2011 evolucionó hacia el gusano Duqu cuyo objetivo era conseguir datos de las empresas; en mayo de este año 2012 se alertó sobre Flame, una herramienta de espionaje cibernético altamente sofisticada detectada (contra objetivos de Oriente Próximo y Europa del Este); en agosto se detectaba el virus Gauss, capaz de espiar las transacciones bancarias y robar información de acceso a redes sociales, correo electrónico y mensajería instantánea; en este mes se ha informado (por el laboratorio de la empresa Karpesky) de miniFlame, una herramienta de ataque de gran precisión, que realizaría una investigación y ciberespionaje en profundidad sobre un objetivo potencial previamente infectado por alguno de los gusanos anteriores (Flame o Gauss).

La mayor dependencia y vulnerabilidad ante las ciberamenazas ha empujado a numerosos países de nuestro entorno a avanzar, entre otras cuestiones, en la legislación para incluir la ciberseguridad como uno de los aspectos cruciales a considerar. Muchos de estos países han elaborado incluso una estrategia específica de ciberseguridad, este es el caso ya de EEUU, Reino Unido, Francia, Alemania, Holanda, y organizaciones internacionales como la OTAN y la UE, etc.

Todas estas estrategias enfatizan la coordinación y cooperación de todos los sectores: público, académico y privado. En estas ciberestrategias se plantea un enfoque reactivo, con la defensa de las redes y comunicaciones y la vigilancia o monitorización de los eventos de seguridad de las redes pero, además se plantea un enfoque proactivo para anticiparse frente al posible atacante, cuyo objetivo final es conseguir una capacidad de resistencia y recuperación ante los ataques de los sistemas atacados, la llamada resiliencia.

En el caso de España, la estrategia nacional de seguridad plantea una iniciativa para contrarrestar las ciberamenazas mediante la gestión integral de la ciberseguridad. Esta iniciativa será recogida en uno de los documentos de segundo nivel a desarrollar, la Estrategia Española de Ciberseguridad.

Incluso la recientemente aprobada en julio Directiva de Defensa Nacional alude a esta ciberestrategia y aboga por abordar un enfoque integral en el que “deberían participar los centros de alerta temprana nacionales junto con los sectores de telecomunicaciones y los proveedores de servicios de telecomunicaciones”.

Además se debería avanzar en la regulación normativa, elaboración de un código de buenas prácticas en el ciberespacio y apoyar la colaboración entre países para perseguir los ataques. Una de las iniciativas de normalización internacionales ha presentado recientemente una nueva norma de ciberseguridad, la Norma ISO/IEC 27032.

Otro ejemplo de colaboración es el reciente acuerdo firmado entre el Ministerio del Interior y el Ministerio de Industria, Energía y Turismo para luchar contra la ciberdelincuencia en España, que recoge además mejoras en la protección de las infraestructuras críticas a través del Centro Nacional de Protección de estas infraestructuras, las Fuerzas y Cuerpos de Seguridad del Estado e INTECO.

Retos presentes y futuros en materia de ciberseguridad

Ponencia de D. lvaro Ortigosa Juárez
Profesor del Departamento de Ingenieria Informática
de la Universidad Autónoma de Madrid

Director de la Agencia de Certificaciones de Ciberseguridad y director del Centro Nacional de Excelencia en Ciberseguridad, ambos dependientes del Instituto de Ciencias Forenses y de la Seguridad, Universidad Autónoma de Madrid.

Sus principales áreas de interés son la Ciberseguridad, el uso de técnicas de inteligencia artificial en la lucha contra el crimen, y la construcción de perfiles de usuario a partir del análisis de su comportamiento en redes sociales y textos escritos.

Ha colaborado y colabora actualmente con el Ministerio de Interior (Guardia Civil y Cuerpo Nacional de Policía) en diversos proyectos de investigación y formación.

Ya hemos sido todos hackeados, ¿y ahora qué?

1. El fenómeno del cibercrimen

Día a día las empresas y organizaciones se ven más expuestas a ataques informáticos perpetrados a través de Internet, normalmente conocidos como ciberataques. La amenaza cibernética no es una posibilidad que haya que discutir. El fenómeno de la cibercriminalidad es un hecho, una realidad que ya está con nosotros y ha venido para quedarse.

En Estados Unidos, los incidentes de seguridad informática se han incrementado un 650% en los últimos cinco años [1], poniendo en peligro la confidencialidad e integridad de información sensible del gobierno. El 1 de marzo de 2011 el director del FBI Robert

Mueller mostró su profundo convencimiento de que en muy corto plazo la amenaza de ciberataques será la mayor amenaza para el país, mayor aún que la de un ataque terrorista tradicional. La misma afirmación había sido realizada en enero por Mueller ante el Comité de Inteligencia del Senado Americano [2]. En estos momentos ya existen suficiente cantidad de incidentes que justifican los temores del FBI (4).

El mayor problema relacionado con este fenómeno es lo vulnerable que son los sistemas informáticos antes los ciberataques. La percepción general de los profesionales de la seguridad informática es que *un atacante suficientemente motivado siempre podrá encontrar la forma de acceder a un sistema,* por más medidas de seguridad que se hayan adoptado.

Diversos son los factores que provocan esta situación. Entre ellos podemos mencionar la profesionalidad de los atacantes: ya no estamos hablando de hackers solitarios, encerrados en un sótano oscuro y desafiando la seguridad de los sistemas informáticos por el simple hecho de demostrar que pueden. Detrás de la mayoría de los ciberataques hoy en día se encuentran verdaderas organizaciones mafiosas de alcance internacional. En 2010 ya se consideraba el cibercrimen más rentable que el tráfico de heroína [3]. Incluso es ampliamente aceptado, aunque de difícil demostración, que detrás de muchos de estos ataques hay gobiernos de estados nacionales. La organización de los atacantes, incluida una adecuada división del trabajo, promueve, entre otras cosas, el descubrimiento y la utilización de vulnerabilidades del software muy poco conocidas y ante las que todavía no se han tomado medidas de protección (llamadas vulnerabilidades día cero). La explotación de este tipo de vulnerabilidades puede provocar, por ejemplo, que un usuario vea infectado su ordenador por el simple hecho de visitar una página web, sin que ejecute intencionalmente ningún programa y aunque tenga instalado un antivirus actualizado.

Un segundo factor que aumenta la vulnerabilidad de los sistemas informáticos es el robo de identidades, normalmente conocido como *Phishing*. El *phishing* es el proceso de robar,a través de algún tipo de engaño, credenciales o información que permitan acceder a un sistema (cuentas bancarias, cuentas de correo electrónico, acceso a servidores, etc.). Aunque el *phishing* es un fenómeno conocido y que en su versión más simple difícilmente engañe a un usuario estándar de Internet, actualmente se están desarrollando un tipo de ataque de *phishing* más peligroso, conocido como spear *phishing*. Este tipo de *phishing* hace uso intensivo de la llamada ingeniería social para recabar información de la potencial

---

(4) En 2010 un gusano informático extremadamente sofisticado llamado Stuxnet atacó equipamiento de las centrales nucleares en Irán, destruyendo físicamente un número no determinado de centrífugas (informes de inteligencia dicen que serían unas 1000 las centrífugas que tuvieron que ser reemplazadas). Dada su sofisticación, se cree que un gobierno debe estar detrás de su desarrollo. De hecho, un artículo del New York Times confirmó implícitamente esta sospecha [11].

Una variante de este gusano, llamado Duqu, fue descubierto en el año 2011 en ordenadores de Europa; el objetivo de esta variante era robar información para futuros ataques. Se ha descubierto que deben existir al menos otras tres variantes, listas para ser utilizadas. Para complicar más aún la situación, la organización hacktivista Anonymous consiguió el código fuente del gusano y lo publicó en Internet.

Respecto de esta organización, en marzo de 2012 se informó que atacó y puso fuera de servicio un servidor de la empresa española Panda Security, una de las empresas más importantes a nivelmundial en seguridad informática. Y hace algunos meses, la mismaorganización robó (a través de Internet) documentos privados del Instituto de Seguridad Stratfor, contratado entre otros por las FF.AA. de EE.UU. y American Express.

víctima y elaborar un engaño mucho más creíble. Aunque este tipo de ataque requiere más esfuerzo y tiempo de parte de los delincuentes, las probabilidades de éxito son mucho mayores. Si el objetivo vale la pena (normalmente desde un punto de vista económico), los atacantes estarán dispuestos a realizar este esfuerzo adicional. Utilizando *spear phishing* se puede lograr, por ejemplo, que un usuario revele sus credenciales de acceso a un sistema o visite una página web diseñada para explotar una vulnerabilidad día cero, entre otras cosas.

Finalmente, otros dos factores que están cambiado y mucho la forma de utilizar sistemas informáticos, con importantes consecuencias en su seguridad, son los llamados fenómenos del *cloud computing* y BYOD *(Bring your own device)*. El cloud computing (computación en la nube) se refiere a la creciente tendencia de las organizaciones a utilizar servidores externos para almacenar la información. Esta solución ofrece ventajas desde el punto de vista económico y organizativo; sin embargo presenta nuevos desafíos desde el punto de vista de la seguridad, al estar la información fuera de la organización y casi siempre accesible a través de redes públicas. El fenómeno BYOD (literalmente, traiga su propio dispositivo) describe otra tendencia creciente: la de que los miembros de una organización utilicen dispositivos propios, comprados de forma privada, para acceder a los recursos informáticos de la empresa. Normalmente estos dispositivos son teléfonos inteligentes y tabletas que poseen las mismas facilidades para conectarse a Internet que sus hermanos mayores los ordenadores portátiles y de sobremesa, y por lo tanto con las mismas vulnerabilidades. Lo que incrementa la inseguridad es que estos dispositivos no están controlados por el servicio de tecnologías de la información de la correspondiente organización y, por ejemplo, es muy posible que no tengan instalado ningún antivirus. Al respecto, El INTECO afirmó que "El uso indebido de las infraestructuras TIC en las empresas se ha convertido en una de las amenazas más importantes de seguridad para su actividad."[4] , y en cuanto a los particulares, afirmó [5] que "un 64,2%, de los internautas ha vivido una situación de intento o culminación de fraude en los últimos tres meses [...]".

Por tanto, la ciberseguridad supone un problema real y actual que afecta a la seguridad nacional y su proyección internacional, tanto en el sector público como en el privado. Este problema no solo requiere organismos dedicados a enfrentarlo, sino también personas que lleven acabo labores de ciberseguridad desde el nivel más básico, llevando acabo buenas prácticas de seguridad y un uso adecuado de las TICs, hasta el nivel más alto, gestionando y resolviendo incidentes de ciberseguridad.

En este sentido, es importante destacar que normalmente se considera al ser humano como el eslabón débil del sistema de defensa. Como decía una de los personajes de la saga Juego de Tronos, de XX [6]: "Ningún muro es más fuerte que los hombres que lo defienden". Hoy en día se considera un ataque de phishing como el método más probable para que ciberdelincuentes obtengan acceso ilícito a un sistema.

2. El contexto

Ante este panorama, el conocimiento en ciberseguridad es uno de los valores más apreciados hoy en día no solo por organizaciones públicas, o privadas, sino por la socie-

dad en general (5). Una persona bien formada en ciberseguridad es un valor en alza y, pese a los tiempos de crisis, con realidades y perspectivas de empleo cada vez mayores, como así lo afirman las valoraciones sobre empleabilidad en este sector [8]. Contar con un número suficiente de personas formadas en ciberseguridad es ya una necesidad.

Este hecho hace de la Ciberseguridad un campo altamente rentable para productos de formación. La oferta formativa realizada por instituciones u organizaciones públicas (las menos) o privadas (la gran mayoría) no solo ha proliferado sino que es cada vez mayor; el modo de obtenerla, diverso (presencial, semipresencial, online) y la gama de titulaciones que se otorgan cada vez más amplia.

3. El problema

Pese a la ventaja que supone esta amplia oferta formativa por la facilidad y posibilidad de acceso a la misma que ofrece, existe una problemática derivada justo de la proliferación, amplitud y variedad de la oferta y sus titulaciones: Esta oferta se ha hecho sin control, garantías o rigor.

La mala noticia es que esta falta de rigor y control ha desembocado en una manifiesta escasez de confianza en las titulaciones y el conocimiento o pericia que éstos reflejan, lo que comienza a retraer la contratación de personas y servicios. Como consecuencia lógica, esta desconfianza se extiende sobre la capacidad de una organización para hacer frente a problemas de ciberseguridad, ya que dicha capacidad se basa, en gran parte, en la de su personal.

Las razones para dicha desconfianza son múltiples, pero las más relevantes son:

a) Lejanía de la formación de las demandas de conocimientos que tienen instituciones y empresas.

b) Formación que, en no pocas ocasiones, se muestra demasiado dependiente de las herramientas (6) de seguridad informática, de marcas más o menos conocidas (Microsoft, CISCO, etc.), sobre las que se realiza.

c) Variabilidad en los criterios y exigencias (7) de evaluación para obtener titulaciones.

d) Nula garantía de mantenimiento y actualización de conocimientos (8) que requiere un campo en continua evolución como es el de la ciberseguridad.

En el informe de la CIS (Commision on Cybersegurity) “Human Capital Crisis in Cybersecurity” presentado en 2010 al presidente Obama se señalaba que el problema crí-

(5) El informe del año 2012 de la Fundación ESYS sobre seguridad (SICUR, febrero de 2012) [7] señala que, por primera vez, la preocupación de la población por la seguridad informática supera a la de la seguridad física.

(6) Estos productos son ofrecidos para la formación por las empresas con el objetivo de fidelizar su uso.

(7) Las necesidades económicas de las instituciones hacen que no pocas veces se otorguen titulaciones con un pobre nivel de exigencia para su obtención.

(8) Un título garantiza, en el mejor de los casos y en mayor o menor medida, que se ha obtenido un conocimiento, pero no prevé mecanismos que garanticen su mantenimiento o actualización.

tico no está tanto en la tecnología disponible (9) como en la posibilidad de contar con recursos humanos a) bien formados (10) en ciberseguridad, b) con certificaciones que garanticen su formación y den confianza en su competencia (11), y c) y personas en número suficiente, para dar respuesta a las demandas (12) de ciberseguridad. El mismo problema ha sido detectado tanto en la UE (13), como en nuestro país [7, 10].

4. Las vías de solución

Diversos informes tanto internacionales [8], como nacionales [7, 10] señalan, entre otras, seis vías fundamentales de solución; a) dos orientadas a mejorar las condiciones de formación, y b) cuatro destinadas a incrementar la confianza en la contratación y prestación de servicios.

Mejora de la formación:

– Mayor implicación y liderazgo de entidades oficiales, sobre todo las universidades, en la formación de ciberseguridad, creando titulaciones de grado y posgrado, así como cursos de actualización o formación específica, abiertos a los profesionales del sector.

– Mayor participación de empresas y profesionales expertos del sector en el proceso de formación, tanto en la planificación como en la organización e impartición de la formación, de forma que ayuden a las entidades oficiales a acercar los planes de formación y prácticas educativas a los problemas reales.

Incremento de garantías y confianza:

– Implantación de CERTIFICACIONES DE CIBERSEGURIDAD como sistemas rigurosos y fiables de evaluación de conocimientos, que sean a) independientes de las titulaciones y formación adquirida, así como de los productos sobre los que se realiza la formación, y b) que incorporen mecanismos que garanticen la continúa actualización de conocimientos y destrezas.

– Que dichos sistemas de evaluación sean extensibles a organizaciones que prestan servicios de ciberseguridad, bien como instituciones o empresas del sector, bien

(9) Aunque también es un problema, el desarrollo tecnológico pierde eficacia si no se dispone de personal que opere con los productos.

(10) "We need to promote the development of more rigorous curricula in our schools and universities" [9, página 7].

(11) "We need to promote the creation and adoption of rigorous professional certifications" [9, página 7], "We fully concur that certifications and licensing regime are essential element form informing and protecting those who buy professional services on Cybersecurity that buyers are often unable to evaluate" [9, página 1].

(12) "A critical element of a robust cyberspace strategy is having the right people, in an enough number, at every level. And this is, by many accounts, the area where we are the weakest.[-] In our Agency there are about 1.000 security people who have the specialized security skills to operate effectively in cyberspace. We need 10.000 to 30.000" [9, página 1].

(13) "[-] the EU need certifications and 60-80% of increasing in cyber security jobs only for the next two years. Fact: we do not have enough people to accomplish such a demand" [8, página 21]

como garantes de la seguridad electrónica de datos en algunas de sus áreas, secciones, o departamentos (lo que afecta a cualquier organismo, desde empresas de distribución eléctrica hasta centros educativos.). Esto es; las ACREDITACIONES DE CIBERSEGURIDAD (Una acreditación es una certificación aplicada a una organización. Se certifican personas, se acreditan organismos).

– Que entidades oficiales, sobre todo las universidades, tomen un papel mucho más protagonista en dicha creación, aportando su prestigio y excelencia al proceso de certificación y generando así confianza.

– Que dichas entidades impliquen a empresas y personal experto líderes del sector para hacer las certificaciones y acreditaciones creíbles para el sector contratante de personas y servicios.

5. Importancia de la creación de las Certificaciones de Ciberseguridad de la ACC

La creación de las Certificaciones de Ciberseguridad del ICFS de la UAM supone un acontecimiento sin precedentes en el campo de la Ciberseguridad en España ya que estas certificaciones:

– Son las primeras surgidas de una institución pública española (14).

– Son en español, lo que permite satisfacer la demanda no solo española, sino Latinoamericana.

– Surgen de una universidad de prestigio como es la Universidad Autónoma de Madrid (Campus Internacional de Excelencia).

– Sus programas de certificaciones se acoplan a las necesidades de la sociedad al haber sido elaborados en asociación con expertos provenientes tanto de empresas del sector de la ciberseguridad (en concreto, con personal de S21sec), como de entidades gubernativas (p.ej. Ministerio del Interior).

– Permiten certificar no solo a particulares (CCS), sino a organismos tanto públicos como privados (ACS) en su totalidad, o a secciones o departamentos.

– Permiten certificar competencias de ciberseguridad independientemente de la formación de referencia, provenga de donde provenga, de la titulación obtenida, y del modo de adquisición de la formación. Al no requerir titulación, incrementa la empleabilidad de personas que hayan obtenido conocimientos y destrezas por propia experiencia.

– Sus evaluaciones son independientes del producto de seguridad informática sobre el que pueda haberse adquirido dicha formación (Microsoft, CISCO, etc.), evitando los potenciales sesgos que pueda introducir tanto la institución formadora, como la distribuidora.

---

(14) Aunque existen múltiples agencias internacionales (alguna de ellas operando en España), solo estas certificaciones ofrecen las garantías ya mencionadas.

– Son las únicas en español que garantizan, mediante su normativa disciplinaria, la actualización constante de conocimientos.

Además, la *Agencia de Certificaciones de Ciberseguridad* (ACC) es la primera agencia española y una de las primeras en Europa orientada a la certificación y acreditación de conocimientos en ciberseguridad. Esto supone para España situarse entre los líderes en este sector.

6. Beneficios que se obtienen

La persona certificada:

– Reconocimiento oficial de conocimientos, habilidades, y compromiso ético y profesional.
– Reconocimiento de su capacidad para realizar trabajos de alta calidad.
– Credibilidad y prestigio ante los clientes.
– Incremento de su capacidad de contratación frente a profesionales no certificados.
– Incremento de su potencial de ganancia económica.

La organización acreditada:

– Reconocimiento oficial de su capacidad para ofrecer servicios de calidad.
– Fiabilidad de compromiso ético y profesional.
– Fidelización de clientes
– Incremento de credibilidad ante los clientes.
– Prestigio y publicidad frente a los demás.
– Incremento de su potencial de contratación.
– Ventaja competitiva frente a otras organizaciones no certificadas.

El cliente o entidad contratante:

Contratar personas u organizaciones certificadas o acreditadas:

– Proporciona confianza al reducir el riesgo en la contratación.
– Simplifica el proceso de selección de personal.
– Garantiza la actualización de avances e innovaciones en ciberseguridad.
– Incrementa el potencial de ganancia económica por valor añadido al producto.
– Reduce la probabilidad de pérdida económica o prestigio frente al riesgo de la contratación de personas u organizaciones no certificadas.

7. Las certificaciones de Ciberseguridad de la ACC

Fruto de este trabajo continuado, llevado a cabo desde 2009 hasta el momento actual por personal del ICFS, S21sec, y de la Secretaría de Estado de Seguridad del MIR es la creación de las Certificaciones de Ciberseguridad del ICFS de la UAM y de la Agencia de Certificaciones de Ciberseguridad del ICFS, garante de las certificaciones.

El sistema de certificaciones de la ACC del ICFS tiene sus propias reglas (equiparables a las contempladas por las mejores certificaciones internacionales) procedimientos y forma de administración para llevar a cabo una certificación, que han sido convenientemente inscritas en el Registro Territorial de la Propiedad Intelectual. Dicho sistema, cumple los requisitos de ser objetivo, riguroso, fiable, eficaz, operativo, y estar administrado de manera imparcial y honesta.

Las certificaciones de la ACC son entendidas tanto como un producto y como un proceso (ver figura 1) de garantías que comienza por a) la *adquisición* de la certificación, en el programa deseado (ver apéndice II), al nivel de exigencia de conocimientos, habilidades y experiencia elegido (Nivel Base, y Profesional), y continúa con b) su *mantenimiento* -anual- y c) *renovación* periódica -trianual-, lo que garantiza la actualización y puesta al día de dichos conocimientos y habilidades.

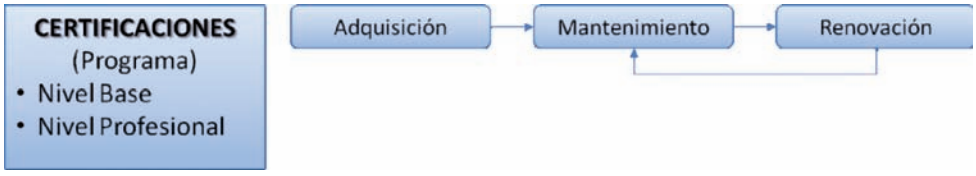


Figura 1: *La certificación entendida como un proceso*

Cuando este proceso se orienta a evaluar la competencia de la plantilla de una organización (empresa o centro educativo) en materia de Ciberseguridad, toma la forma de *Acreditación de Ciberseguridad* o ACS.

Su objetivo

Garantizar a la sociedad, que una persona u organización: a) ha superado las evaluaciones, demostrado su competencia, mantiene actualizados sus conocimientos de ciberseguridad, y se han comprometido específicamente b) a seguir la normativa ética de conducta profesional, y c) a acatar los deberes y obligaciones establecidos por la normativa reguladora de la certificación, asumiendo en ambos casos el régimen de sanciones previsto.

A quién se dirige las Certificaciones

– **Particulares:** Con diferentes niveles de formación.

– **Organismos:** Empresas y centros educativos.

Niveles de certificación acreditación

Particulares: 2 niveles de certificación:

1. *Nivel de Base:* Superación de examen.

2. *Nivel Profesional:* Resolución de casos prácticos de incidentes de seguridad.

Organismos: 2 niveles de acreditación:

1. *Nivel de Base:* Mínimo 70 por ciento de la plantilla certificada.

2. *Nivel de Excelencia:* Resolución de casos prácticos de incidentes de ciberseguridad.

Sellos de certificación y/o acreditación

Al igual que los tenedores en los restaurantes o las estrellas en un hotel, los sellos de certificación son un método visual que permite:

a) distinguir la *situación privilegiada* de la persona u organización que lo ostenta frente a aquellas que han preferido mantenerse al margen de los esquemas de reconocimiento de la excelencia,

b) reflejar el nivel de certificación alcanzado y facilitar la elección de personas certificadas u organismos acreditados que más encajen con las necesidades y posibilidades de contratación, y

c) motivar tanto a los candidatos al mismo como a los miembros certificados, lo que redunda en el reconocimiento y prestigio de los mismos.

La ACC otorga los siguientes distintivos de calidad en función de los niveles de certificación:

Figura 2: *Tipos de certificaciones y acreditaciones ofrecidas*

8. Catálogo de Certificaciones Ofrecidas

La complejidad de la seguridad de la información es directamente proporcional al hecho de que las tecnologías de la información están implantadas en todas las capas socia-

les; profesionales y personales. Por este motivo, el abordaje de la gestión integral de la información, y por ende, de la seguridad, debe entenderse como un conjunto en el que las diferentes áreas de la seguridad se relacionan inevitablemente, unas con otras.

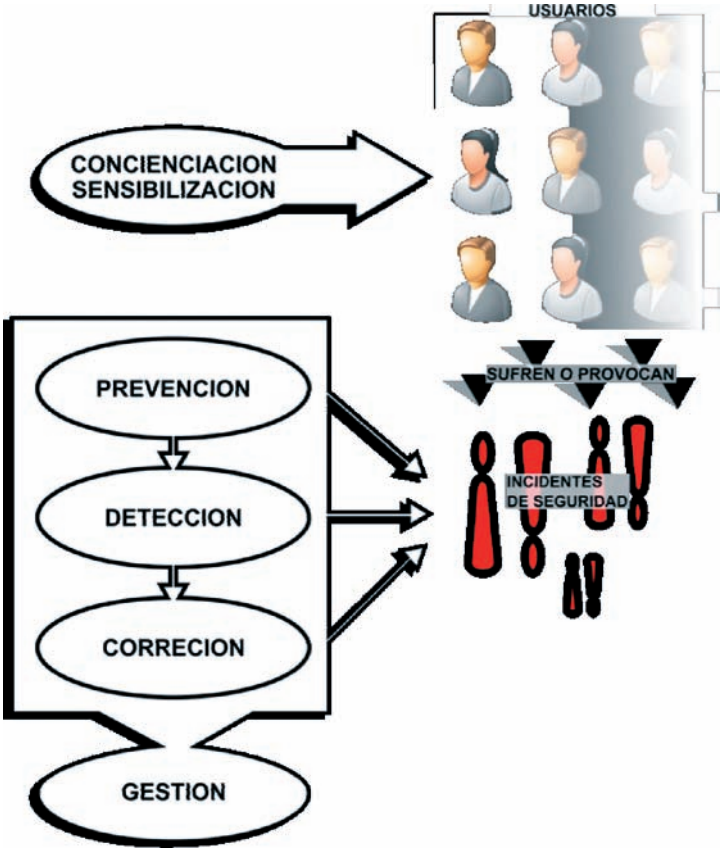


Figura 3: *La seguridad de la información: un proceso multinivel*

Desde la ACC se trata de abordar la seguridad cubriendo todos los posibles ámbitos en los que las TI son aplicables, abordando la sensibilización en seguridad en los menores, los centros educativos y los lugares de trabajo.

En las áreas "profesionales", se detallan cada una de las áreas específicas en las que interviene la seguridad: sistemas, desarrollo, prevención, detección y gestión, de este modo se obtiene una visión integral y especializada de la seguridad de la información.

Existe una fuerte interdependencia en las diferentes áreas de conocimiento que presentamos, de esta manera, el *desarrollo* implica la *gestión* de redes en las que se tienen que *detectar* y *resolver* los incidentes de seguridad y todo esto realizando una gestión acorde a las diferentes normativas, estándares y legislación.

9. Centro Nacional de Excelencia en Ciberseguridad

Sin embargo, desde el ICFS reconocemos que esto es sólo parte del problema. La lucha contra el cibercrimen exige sobre todo la participación de los Cuerpos y Fuerzas de Seguridad del Estado (CCFFSE). Y por supuesto, el problema de la necesidad de formación no les es ajeno. Todo lo contrario: su posición en primera línea de esa lucha les exige una formación continua y sumamente especializada. Además, la facilidad del cibercrimen para cruzar fronteras provoca que resulte de vital importancia la coordinación y mutuo entendimiento entre los cuerpos policiales de distintos países.

En este sentido, en Europa existen diversas iniciativas destinadas a fomentar y facilitar tanto la formación como la cooperación entre las distintas policías europeas. Una de estas iniciativas es la creación de una red de centros de excelencia aglutinados en torno al 2CENTRE (Cybercrime Centres of Excellence Network for Training, Research and Education).

Es en este contexto que la Universidad Autónoma de Madrid, a través del ICFS, la empresa S21sec, el Cuerpo Nacional de Policía y la Guardia Civil se unen para crear el Centro Nacional de Excelencia en Ciberseguridad (CNEC). El CNEC es un proyecto cofinanciado por el programa ISEC de la Comisión Europea, e integrado en la red Europea de Centros de Excelencia en Ciberseguridad 2CENTRE.

El CNEC está situado en la Universidad Autónoma de Madrid, campus de Cantoblanco, dentro del Instituto de Ciencias Forenses y de la Seguridad (ICFS). Su objetivo es promover la formación, coordinación y cooperación entre los CCFFSE a nivel nacional y entre los diferentes CCFFSE Europeos integrantes de la red 2CENTRE.

Actualmente cuentan con Centros de Excelencia asociados al 2CENTRE: Irlanda, Francia, Bélgica, Lituania, Inglaterra, Grecia, Rumanía y, por supuesto, España.

Figura 4: *Red de Centros de Excelencia*

El CNEC desarrollará tres líneas de acción:

– Formación y certificación a CFSE: EL CNEC impartirá formación específica para CFSE, proporcionándoles los conocimientos necesarios para obtener la Certificación de la Agencia de Certificaciones en Ciberseguridad ACC.

– I+D: desarrollo de herramientas forenses para la prevención y la lucha contra los delitos tecnológicos.

– Laboratorio DLAF: Creación de un Laboratorio de herramientas forenses *open source* para CFSE Nacionales y Europeos.

Referencias bibliográficas

[1] Government Accountability Office (2011); GAO-12-137. Gobierno de Estados Unidos.

[2] http://www.homeland1.com/Critical-Infrastructure-cyber-security/articles/1246214-FBI-director-Cyber-threats-will-become-top-worry. Accedido en diciembre de 2012.

[3] http://elpais.com/diario/2010/04/22/ciberpais/1271903068_850215.html Accedido en diciembre de 2012.

[4]http://cert.inteco.es/cert/NotasActualidad/seguridadticpymesusoindebidoinfraestructuras20120229

[5] http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudiofraude2C2011

[6] Eddad Stark en Juegos de Tronos. George R.R. Martin. Ediciones Gigamesh. ISBN 978-84-96208-42-1.

[7] Informe del año 2012 de la Fundación ESYS sobre seguridad (presentado en SICUR, febrero de 2012).

[8] "Cyber Security Jobs Survey in EU: Situation and Prospective for the next 5 to 10 years". ENISA (European Network and Information Security Agency) 2010-2011.

[9] CSIS Commission on Cybersecurity for the 44th Presidency. July 2010: "Human Capital Crisis in Cybersecurity: Technical Proficiency Matters".

[10] Informe "Ciberseguridad en España" del Real Instituto Elcano, de Julio de 2010.

[11] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.htm

Accedido en diciembre de 2012.

Retos presentes y futuros en materia de ciberseguridad

Ponencia de D. Antonio ngel Ramos Varón
Profesor titular de la
Universidad Complutense de Madrid

Es diplomado por la Universidad Complutense de Madrid. "Experto en seguridad informática de redes de ordenadores y antihacking", en los módulos de metodología de la intrusión a sistemas informáticos. Profesor en masters y postgrados sobre seguridad informática y de las comunicaciones en diferentes universidades. Ha participado en diversas colaboraciones informáticas universitarias y publicaciones de libros. Autor de libros como: Hacker 2006, Hacking Práctico, Protege tu PC, entre otros, de la editorial Anaya Multimedia. Ha impartido diferentes seminarios y talleres de hacking de sistemas y seguridad informática en España e Iberoamérica. Realiza parte de su labor como formador y asesor a departamentos de IT de empresas e instituciones. Consultor de StackOverflow.

Observación: *El desarrollo del debate y la ponencia escrita así como las conclusiones son estrictamente opinión del autor y reflejan su manera de percibir la realidad en base a su experiencia en numerosos proyectos y actuaciones ante un problema que considera de alta prioridad*.

INTRODUCCIÓN

Han pasado muchos años desde que la película Juegos de Guerra (1983) ambientada en el escenario de la guerra fría pusiera de manifiesto la posibilidad y alcance de un ciber ataque. Ciertamente esta película me cautivó y despertó en mí lo que finalmente ha sido mi profesión: hacker. Hacker porque no ciberdelincuente o cibercriminal son dos términos totalmente opuestos pero que disponen de iguales potenciales, unos los utilizan para hacer nuestras vidas digitales más seguras y otros para ejercer en un lucrativo negocio que es el cibercrimen y en su siguiente fase el ciberterrorismo o la agresión en la red.

No olvidemos que en la actualidad servicios imprescindibles para el desarrollo de nuestra sociedad: finanzas, telefonía, sanidad, pensiones, aeropuertos, metro, etc. están

controlados en gran parte por redes de ordenadores y sistemas digitales. ¿Que pasaría si determinados individuos con los conocimientos necesarios y el adecuado financiamiento pudieran llegar a comprometerlos y alterar su normal funcionamiento? Esto ha dado nacimiento a grupos de individuos maliciosos y a la aparición de una serie de comportamientos antisociales en la red Internet que tan solo un par de décadas atrás eran impensables.

ZONA DE GUERRA

La mejor manera de saber como actuar es darnos cuenta de lo mal que estamos o de lo bien que estamos. Los ataques informáticos se han sucedido y cada vez con mayor frecuencia desde la década pasada (incluso mucho antes Robert T Morris 1988), pero debemos poner un punto de inicio en este debate. El año 2010 *Ed Skoudis (http://www.sans.org/instructors/ed-skoudis)* prestigioso investigador del *Sans Institute,* asesor de la casa blanca y conocido como especialista en juegos de guerra y ciberataques, entre otras menciones, argumentaba *"Un atacante lo suficiente determinado y con los conocimientos necesarios puede entrar prácticamente en cualquier organización en la actualidad"*. En este momento mucha gente responsable de servicios IT y gestores de áreas de informática de instituciones y empresas se echaron las manos a la cabeza y tomaron la determinación de trabajar en mitigar esta posibilidad o amenaza.

Año 2012, todo sigue igual por no decir peor. Importantes organizaciones y multinacionales son comprometidas y sus datos expuestos y vendidos. Quizás no estemos haciendo lo suficiente, quizás no estemos haciendo nada o estemos mal guiados, pero no hay peor *leader* de equipo que aquel que no reconoce sus debilidades y no se deja aconsejar de la gente adecuada.

Pero entendamos como esto va evolucionando y haciendo el problema cada vez más complejo de solucionar:

El *negocio* que mueve el crimen organizado en la red, es uno de los negocios más lucrativos del planeta, incluso tan importante como el negocio de la droga, y además no se precisa de infraestructuras ni operativos logísticos, sino de una conexión de 10 euros al mes ADSL en tu casa. Esto ha permitido generar una estructura empresarial alrededor de este mundo que no tiene que envidiar a una empresa o multinacional. Disponemos de canales de venta y comunicación que funcionan los 365 días del año, las 24 horas del día. ¿Y porque no tiramos abajo estos canales si sabemos que existen? Porque *Arpanet (Advanced Research Projects Agency Network),* hoy en día nuestra Internet se desarrolló para eso, siempre disponible, siempre operativas las comunicaciones.

Sigamos avanzando en la materia, empiezan a montarse servicios a la carta para realizar ciberataques o realizar actividades delictivas las *botnes* (redes de ordenadores infectados sin que los usuarios lo sepan) que actúan bajo las ordenes de un *bot master* (el dueño de esa red de ordenadores, la persona que pudo infectar a estos usuarios y controlar sus ordenadores) o bajo las ordenes de alguien que quiera alquilar estos servicios. Y es cuando surge la parte realmente lucrativa de estos y muchos más servicios que podemos encontrar en la red Internet y ahora en la llamada *Deep Web* (especie de red en paralelo dentro de Internet donde los ciberagresores o ciberdelincuentes operan).

El *Dinero* el factor más motivante del planeta Tierra para la mayoría de los humanos, esto es lo que promete el realizar actividades ilegales en la red, además se hace publicidad y ostentación de este, con el fin de no solo alimentar el ego del trasgresor sino animar a jóvenes y personas con conocimientos a formar parte de este. Quizás en determinados entornos sociales, países donde la realidad social es muy distinta a la de los países desarrollados en términos de justicia social puedan ser entendibles. Cuando un joven de 23 años ingeniero en ciencias de la computación, sabe o percibe que los próximos 20 años de su vida serán de programador o administrador de sistemas ganando el equivalente 250 euros al mes. Con lo fácil que le resultaría abrir un candado digital y solucionar en parte sus problemas económicos o de su familia, pero por otra parte la tendencia no es menor en los países desarrollados, el factor en común "el dinero", en unos por necesidad o agobio en otros países porque es el mensaje que se nos ha venido y lanzando durante años, tanto tienes tanto vales.

Pero deberemos saltar un paso más hacia adelante, pasar de lo que no es otra cosa que un negocio mafioso ilegal, pasamos al concepto de agresores en la red, a lo que llamaríamos una respuesta país en un escenario de guerra en la red. Aquí el objetivo y la motivación es distinta se trata de escenarios donde se puede someter a: un estado, institución o empresa mediante un ataque a sus sistemas telemáticos en toda regla, con el fin de: su colapso, producir importantes perdidas económicas, espionaje o simplemente generación de pánico en la población. Ya la prestigiosa revista *the economist* trata en su número de julio de 2010 el problema en primera página, con un extenso editorial en interior donde se describe el escenario de una confrontación en la red y/o una agresión desde Internet, lo que es el quinto elemento: tierra, mar, aire, espacio y ahora el *ciberespacio* y como países como es el caso de los Estados Unidos por nombrar uno, están tratando el problema y preparándose.

Mediante el análisis de ciberarmas y distintas variantes de ciberaques, descubrimos un amplio y nuevo "escenario de operaciones" desde: Millones de ordenadores que atacan un objetivo simultáneamente (ataque volumétrico), sofisticado software malicioso para propagarlo en sistemas de producción industrial, ataques a infraestructuras críticas, o ataques a los millones de dispositivos móviles que utilizamos (smartphones, tablets, etc.). Auque suena todo a ciencia ficción pensemos que ya tenemos datos empíricos mas que suficientes para darnos cuenta que esto esta sucediendo.

Cuando Julio Verne nos descubría el viaje a la luna o veinte mil leguas de viaje submarino muchos pensaron que era un imposible pero otros vieron la posibilidad. Aquí la posibilidad es ya una realidad.

TENDENCIAS

Por supuesto que existen soluciones y herramientas que pueden ayudar a mitigar, abortar o combatir ciberataques. Pensemos que grandes fabricantes de tecnología que cotizan en el *Nasdaq* no son ajenos a ello e invierten cantidad ingente de dinero en investigación y desarrollo de lo que podemos llamar *contra respuestas,* últimamente me ha sorprendido fabricantes como: Arbor, Palo Alto o Radware, pero que decir que no los únicos de un importante portafolio.

Pero los agresores dentro de la red no son ajenos y ciertamente como pudimos ver en la conferencia sus desarrollos y ataques son cada vez mas sofisticados en términos: tecnológicos, creativos y desarrollados. Ataques y desarrollos que desafían los millones de dólares invertidos por las empresas de seguridad y que en muchas ocasiones suelen funcionar y les proporciona la victoria en determinada batalla. El desarrollo de tan sofisticadas técnicas, programas y ataques informáticos obedecen a grupos totalmente organizados y muy pocas veces se tratará de un individuo solitario aunque estos casos se han dado y entiendo que también se seguirán dando.

AUTOCRÍTICA Y CONCLUSIONES A ESTA PRIMERA PARTE

Si disponemos de soluciones ¿Por qué fallan más de lo esperado o no dan el rendimiento que se espera de ellas? Aquí esta el gran debate que pretendo abra una vía de autocrítica.

Primero: ¿Dónde están los hackers que nos asesoran? ¿Dónde está verdaderamente un presupuesto suficientemente atractivo para que yo pueda tenerlos de mi lado? Pues no esperaremos que den lo mejor de si por un reconocimiento telefónico o una palmadita en la espalda. Mi experiencia me dice que lamentablemente la mejor manera de tener un gran equipo es tener dinero para fichar a los mejores, creo que es bastante obvio, ahí tenemos a nuestros clubs Real Madrid y Barcelona, y en ese momento podremos exigir hasta su última gota de sudor en el partido. La realidad Española "no hay recursos", igual acabamos de perder el mejor recurso la inteligencia.

Segundo: Nos perdemos en una excelente oratoria, exposiciones donde todos nos cubrimos de elogios y después de cientos de hojas de informes de una prestigiosa consultora donde nuestro consultor es un tipo que en su mayoría jamás ha visto y analizado un datagrama (de una manera simple: paquete de información que viaja por una red). Así no se gana ninguna batalla ni en la vida ni en la red Internet.

Tercero: Formación e inteligencia a nuestros equipos, no todo es fichar individuos, nuestros grupos de profesionales con una constante formación y orientada correctamente puede perfectamente desarrollar las capacidades necesarias para ser un grupo de primera. La realidad, no hay dinero para eso, desde mi experiencia mucha gente de valía pasa mendigando un correcta formación porque ellos si quieren ser útiles al máximo en la organización, esta formación nunca llega o se les manda a un curso nada que ver.

Cuarto: La gestión inadecuada de los lideres, en un número muy importante de ocasiones se contrata al conocido o falso amigo, porque es lo mas fácil y porque el comercial me visita todas las semanas. La meritocracia que a muchos llevó a importantes puestos de gestión donde se encuentran ahora se perdió, es parte del pasado. Además esta se termina destruyendo cuando el proceso de contratación se basa en: el balance bancario, escrituras de la sociedad y los mil requisitos burocráticos y banales, no importa lo que aportes, importa lo que aparentes ser y eso hemos visto recientemente en nuestro sistema financiero es fácil de maquillar.

Quinto: La negación a dejarse guiar y dejarse asesorar. Cuando se habla de trabajo en equipo no es un termino y unas powerpoint que nos pasan en un cuso de *couching*. Es algo

profundo que debe nacer de la persona y la persona debe adoptar. El imaginar situaciones de acción y sus soluciones con nuestro equipo es fundamental. La imaginación es más importante que el conocimiento *(Albert Einstein)*.

NUEVOS ESCENARIOS DEL SIGLO XXI

Aunque en el ámbito del ciberespacio nos tocará ver como el escenario actual conocido cambia y crece, en esta exposición se hace referencia a lo que considero una clasificación actual de grupos de influencia y actividad en la red:

Los *White hat hackers* o *hackers:* Su notoriedad cada vez es mayor dentro de los medios de comunicación, acompañada de importantes eventos y conferencias mundiales como: *blackhat, defcon* o nacionales en el caso de España como la NocON Name, la Rooted y un sin fin de eventos no menores pero que agrupan a verdaderos especialistas del desarrollo de software, las redes, sistemas operativos y comunicaciones. Importantes descubrimientos en términos de brechas de seguridad se hacen públicos con el objeto de que sean resueltos y en consecuencia nuestras vidas digitales sean más seguras. También destacar dentro de todo este mundo, por algunos denominado "mundo de frikis", la existencia de individuos que son consultados y contratados por grandes cuentas, instituciones y gobiernos para conformar y liderar equipos de auditorias y proyectos críticos de integraciones o seguridad de la información.

Anonymous y el activismo en la red "hacktivismo": Mucho se habla de Anonymous y su amenaza. De los hacktivistas o activistas en la red, del grupo wikileaks por mencionar a algunos. Debemos de pensar y estar preparados para entender y analizar estos movimientos y para los que van a llegar vía: Twister, redes sociales, etc. Pensemos por ejemplo que en los años 70 un millón de personas marchaban sobre Washington DC en protesta por la guerra de Vietnam o en defensa de los derechos raciales, estos movimientos no eran enteramente pacíficos y se producían los altercados por todos conocidos, así ha sido durante décadas e incluso en la actualidad es asumido, ahora enfrentamos recientemente una huelga general que tiene características análogas de compartimiento.

Gente que protesta por lo que podemos considerar causas licitas o menos licitas, con las que podemos simpatizar o no, pero que es el reflejo de una sociedad que necesita ser escuchada por un sistema que solo otorga placebos, buenas maneras y ninguna solución, donde todo tiene que ajustarse a unos parámetros donde muchas veces no hemos sido consultados. Aquí nace el hacktivismo, Internet proporciona el campo de acción perfecto para reivindicar y ser escuchados, en un medio que ellos no controlan, la tecnología y la red proporcionan desde: las redes sociales hasta software para la realización de ataques de DOS o DDoS (ataques de denegación de servicios) que no viene a ser otra cosa que las pancartas, las pintadas y los contenedores quemados que en la vida real vemos. En el caso concreto de Anonymous y desde mi modesta opinión no representan una amenaza, Anonymous es predecible, puesto que todos sus acciones son comunicadas incluso con días de antelación, toda persona puede pertenecer y seguir las acciones de Anonymous (http://www.anonops.com/), Anonymous no ha matado a nadie ni ha dejado a un anciano de 70 años en la calle durmiendo debajo de un puente, vamos a mi todavía no me constan estos hechos.

Por tanto aquello que es predecible es controlable, todo obedece mas a una campaña de crear enemigos de la humanidad que puede interesar a determinados grupos de influencia, grupos de influencias que sienten temor por un entorno que no controlan y no pueden controlar "la red Internet". Cierto que siempre al igual que en: las religiones, política, fundaciones, etc. Habrá gente que intentará sacar partido personal de este tipo de movimientos, he incluso gente que realmente pueda tener fines perversos, pero en muchas ocasiones es un conjunto dentro de estos movimientos que explota a otros, los cuales suministran su poder de computo para alguna causa que quizás no han analizado o racionalizado, pensemos que las masas se comportan en ocasiones sin conciencia y esto no es ajeno al mundo de Internet. Un verdadero agresor en la red procurará siempre no ser trazable, no ser notorio, permanecer bajo el radar e intentar pasar desapercibido el mayor tiempo posible.

Blackhats o ciberdelincuentes: Estos grupos conforman en términos civiles la verdadera amenaza en la red. Gente que ha entendido lo que es el lucrativo negocio del fraude y la estafa digital, el asalto a bases de datos, los robos de identidad e información y la extorsión a empresas e instituciones. Son un grupo en continuo crecimiento y conforman estructuras complicadas de combatir y mitigar. Alta sofisticación, alto conocimiento y alta organización. Y el mayor problema un alto beneficio económico.

Tres de los problemas principales que detecto en mi experiencia para equiparar un poco las fuerzas son:

Primero: La falta de una legislación actual que entienda del problema, no que intente abordar el problema pues eso no me sirve. Las leyes siempre van inevitablemente por detrás de la sociedad pero es que la sociedad virtual va mucho más rápido que la sociedad real.

Segundo: El exceso de buenísimo y pulcritud en una sociedad galante de los derechos de los individuos (que después no es tan así) se termina protegiendo al malhechor más que a la víctima. Pudiéndose estar más o menos de acuerdo o pensando que esas reglas son las que se tienen que jugar, y que deseamos ser héroes espartanos, solo cabe decir que: la batalla ahí fuera en la red esta perdida.

Tercero: La diferencia en número, en tecnología, conocimiento y libertad de acción es abrumadora. No se pretende dar una visión fatalista sino una visión realista, se trabajará con los medios que hay, pero no podemos pedir que una persona con un palo en la mano pueda enfrentar con garantías de éxito a una banda de tipos que llevan una colt 1911 semiautomática. Solo estamos viendo el pico del iceberg.

Ciberejércitos y cibersoldados: En la actualidad determinados países si han tomado muy en serio, la creación de unidades de cibersoldados que no solo puedan defender infraestructuras digitales, sino dar respuesta de ataque contra-ataque en una situación bélica en este caso en la red. En este campo existen distancias casi insalvables entre aquellos que si invierten dotaciones presupuestarias y reclutamiento de personal para esta actividad, frente a otros países que solo empiezan a analizarlos o se pierden en meras intenciones con un inexistente presupuesto y una inexistente dotación de personal cualificado.

Tenemos por un lado países cuyos esfuerzos son notables como los Estados Unidos, UK, Israel Francia y China entre otros donde el concepto de *homeland defense* es aplica-

do con todo su significado. La realidad de nuestro país deja mucho que desear, nuevamente enfrentamos la inexistencia de: recursos, y la falta de intención real dentro de un discurso demagogo. ¿Por que demagogo? desde el que escribe esta ponencia, estoy cansado de asistir a ponencias y conferencias donde todos debaten lo importante que es trabajar en la materia y lo prioritario del tema. Hace más de un año que un grupo de colegas y yo desarrollamos el primer grado universitario de "Ciberguerra y ciberinvestigación" que ha sido presentado en varias Universidades, que pretende durante una carrera universitaria generar especialistas en escenarios de ciberguerra, ciberdefensa y ciberinvestigación, grado universitario que podría poner en la cabeza a España en este tipo de estudios, solo existe un precedente en de este tipo de estudios en Corea del Sur, aquí en España de las entidades contactadas solo se han encontrado negativas y aquellas que han mostrado cierto interés se han perdido en procesos burocráticos de aprobaciones, luchas departamentales, etc. Resultado no interesa a nadie, resultado lo que nos cuentan en estas conferencias a las que suelo asistir, algunas veces de ponente, es pura lucubración. España de nuevo pierde oportunidades de encontrarse en el grupo de los líderes, es algo a lo que nos hemos acostumbrado desde que pasó el tiempo en el que en nuestro imperio no se ocultaba el sol.

AUTOCRÍTICA Y CONCLUSIONES A ESTA SEGUNDA PARTE

Disponemos de una fuente localizable de individuos y grupos de individuos que podrían ser fundamentales en la ayuda de creación de sistemas de protección ante ciber ataques en ambas direcciones defensa y contra respuesta. Estos individuos son en gran parte desaprovechados por no querer invertir recursos en ellos.

Los medios de comunicación y grupos de influencia nos muestran una realidad distorsionada de lo que son los agresores en la red en muchas ocasiones. A nadie se le hubiera ocurrido encarcelar y criminalizar a todos los manifestantes de una huelga o marcha social. Efectivamente siempre existirán grupos instigadores que desvirtúan cualquier movimiento de protesta social y pueden cometer actos delictivos. Pero aquí entra en juego qué es delictivo y qué no. Me parece recordar que en las cruzadas matar a un infiel en tierra santa era abrir una puerta al cielo y ahora sería inconcebible dicho planteamiento. La amenaza en Internet no viene de mano de los movimientos hacktivistas.

En la actualidad alguien en algún despacho algunos iluminados pero no tontos, han diseñado la versión de ciberguerra para todo los públicos, versión que permite mucho juego desde: seminarios pagados, conferencias nacionales e internacionales, encuentros entre organismos de diferentes países, proyectos que después nunca concluyen (los rentables *never ending projects*). Todo esto que choca frontalmente con aquellos países que trabajan en la materia en profundidad y la seriedad que merece el tema.

El término de cibercomandos y cibersoldados puede no ser políticamente correcto, pues choca con el buenísimo moralista al que nos han acostumbrado o nos quieren acostumbrar, pero no olvidemos que muchas veces el correcto equilibrio de fuerzas en términos de defensa y armamento han servido en la historia de la humanidad para evitar confrontaciones, y en general los conflictos se han producido cuando una de las partes se siente o se encuentra por encima del otro. No es otra cosa que el balance de fuerzas, que se

puede dar en una negociación de cualquier tipo, no es igual negociar de tú a tú, que de pequeño a grande.

RETOS Y RIESGOS

En esta sección de desarrollo de la ponencia describiremos tres áreas de creciente interés en términos de seguridad digital, y no quiere decir que sean las únicas, tan solo su selección obedece algunos proyectos sobre los que recientemente he sido consultado o estoy involucrado.

BYOD *(bring your own device):* Por si no fuera poco el mantener un control sobre zonas críticas digitales como: nodos de comunicaciones, servidores expuestos a Internet, el propio parque informático interno de organizaciones tanto de puestos de trabajo, portátiles y servidores, llegaron los smarphones y tablets. Y además una nueva tendencia llevar y trabajar en nuestra compañía con nuestros propios dispositivos móviles, independientemente de felicitar a quien diseñó la idea y que consiguió traspasar el coste de adquisición de los dispositivos de trabajo al trabajador y no a la empresa, sin aparente crítica alguna, se trata efectivamente de un importante reto en términos de seguridad de la información corporativa.

Pensemos que estos dispositivos son utilizados para el uso de información de la organización y que en algunos casos puede ser más o menos sensible, además de servir para divertimento y entretenimiento del usuario. Este uso tan flexible o fácil entra en oposición con el término de seguridad, recordemos la facilidad de uso de un sistema es inversamente proporcional a la seguridad en este, es decir: a una alta seguridad disminuye la facilidad de uso por el individuo y a muy poca seguridad resulta muy fácil su uso. Esta premisa ha sido dinamitada con la llegada del BYOD donde la facilidad y comodidad de uso del propietario del dispositivo entrará en confrontación con la seguridad exigida sobre la información por la organización o empresa donde trabaja. En la actualidad ya hay importantes fabricantes que han empezado aportar soluciones de gestión y seguridad de estos dispositivos y sobre la temática que estamos tratando.

DLP *(Data Loss Prevention):* La prevención de fuga de datos, este tema resulta de gran interés pues aquí el agente que entra en juego es el ser humano. Pensemos que la cadena siempre se rompe por el eslabón más débil y en una cadena digital participada de personas, la personal resulta ser el eslabón más débil. Aquí el problema que enfrentamos es el control de la información que contiene el puesto de trabajo. En DLP el planteamiento principal en la protección de la información institucional no se centra frente ataques intencionados y programados de obtención de la información (aunque esta área también queda englobada como fácilmente comprenderemos), se centra en la fuga y perdida de la información por irresponsabilidad del usuario, desconocimiento del usuario o a veces la buena fe del usuario, por ejemplo imaginemos un empleado que para seguir trabajando en casa se envía por mail los ficheros o se lleva en un disco externo la base de datos, su intención esta muy lejos de robar información a la compañía pero esta incumpliendo probablemente buenas prácticas o políticas de control del uso de la información corporativa. Por otra parte es cierto que si somos capaces de controlar o prevenir la fuga de información de esta

manera, estaremos estableciendo una nueva capa de seguridad contra fuga o sustracción de información intencionada (el empleado desleal).

Infraestructuras críticas y sistemas SCADA: Es uno de los temas actuales del debate de la seguridad informática frente ciber ataques. En un principio desde siempre o tradicionalmente las infraestructuras críticas y sistemas Scada *(Supervisory Control And Data Acquisition)* han sido primero sistemas totalmente cerrados, normalmente gestionados por maquinaria computacional y protocolos propietarios donde tan solos los ingenieros de esa especialidad tenían el control y la gestión. Pero recientes ataques dirigidos como el caso del virus stuxnet, entre otros ha despertado la preocupación de que puedan ser atacados y debido a la funcionalidad que desempeñan generar grandes desastres o importantes pérdidas.

¿Pero si son sistemas aislados como podría suceder esto? ¿Y hasta donde pueden ir las consecuencias? Históricamente han sido sistemas aislados pero las demandas de gestión, negocio y monitorización han traído consigo la apertura de posibles puertas. Además pensemos que los equipos de ingenieros y responsables de este tipo de sistemas no tienen porque saber de seguridad informática, deben estar centrados el importante trabajo que tienen y usan estas nuevas pasarelas o puertas como herramientas. Aquí aparecen los problemas: sistemas de software de gestión sobre sistemas operativos conocidos y que sabemos como atacarlos y además le sumamos el mundo Web (las conocidas *scada web applications*) entradas vía Web a sistemas de control de monitorización de los procesos industriales o sistemas críticos y por si fuera poco vía Internet.

Esta nueva situación si activa un semáforo amarillo, si vamos a dejar que estos sistemas pierdan su condición de cerrados totalmente (donde la única posición de ataque sería de disponer de un individuo dentro de la organización) a una semi-apertura o interconexión con sistemas computacionales no tan robustos y atacables. Aunque es cierto y parece lógico que los cuerpos de ingenieros que desarrollan tan complicados sistemas no han dejado de la mano de los ordenadores la gestión absoluta, en muchos de los casos apocalípticos que nos quieren pintar como el ataque de una central nuclear o el sistema de gas de una ciudad, existen o deberán existir procesos manuales de confirmación o acción que solo una persona puede hacer o validar. Con lo cual un ataque serio a este tipo de infraestructuras y sistemas deberá de disponer de factores entre si complementarios: apertura al exterior de los sistemas que pueda ser accedidos exteriormente, y personal dentro de la organización o con acceso a los sistemas conocidos y atacables. Pero si por otra parte en este desarrollo de ponencia he querido reflejar que sueños como lo de Julio Verne se han hecho realidad, no puedo decir que ataques contra las infraestructuras criticas o los sistemas Scada son una ilusión, hemos tenido los primeros avisos o pruebas de concepto y esto solo es indicativo que debemos de poner todo nuestro esfuerzo en trabajar y proveer soluciones de manera anticipada antes que el problema se haga complejo de tratar. Esto solo se consigue con una verdadera voluntad política, con las dotaciones presupuestarias necesarias y con el personal cualificado preciso para el caso.

Para finalizar el desarrollo de la ponencia hacer una mención a los ataques contra sistemas críticos de defensa, desde hace mucho tiempo, y recordemos la primera guerra de Irak por no ir muy atrás, se pretende dejar ciego y sordo al enemigo, esto en el ciberespa-

cio cobra un valor especial pues la posibilidades se amplían enormemente debido a la red de sistemas informáticos interconectados para suministrar comunicaciones, así también mencionar la realidad de ataques dirigidos a los sistemas digitales y computerizados de sofisticadas armas disponibles en la actualidad.

Sin más mi agradecimiento a todos por su asistencia el día de la ponencia y el interés mostrado.

Retos presentes y futuros en materia de ciberseguridad

Ponencia de D. Mario Farnós Buesa
Alférez de la Guardia Civil
Grupo de Delitos Telemáticos de la UCO

Dentro de la mesa redonda que me ha tocado departir, me gustaría dar unas pequeñas pinceladas desde un punto de vista policial, toda vez que nosotros trabajamos en un área más operativa, que técnica y me gustaría dejar constancia de las dificultades que nos vamos a encontrar en un futuro en materia de ciberseguridad.

Antes de afrontar los retos a tener en cuenta respecto a la ciberseguridad; una vez hablado y debatido sobre el cibercrimen, las ciberamenazas y las redes sociales, tenemos que tener en cuenta la situación de la que procedemos, y saber el estado en el que nos encontramos respecto a los cibercriminales.

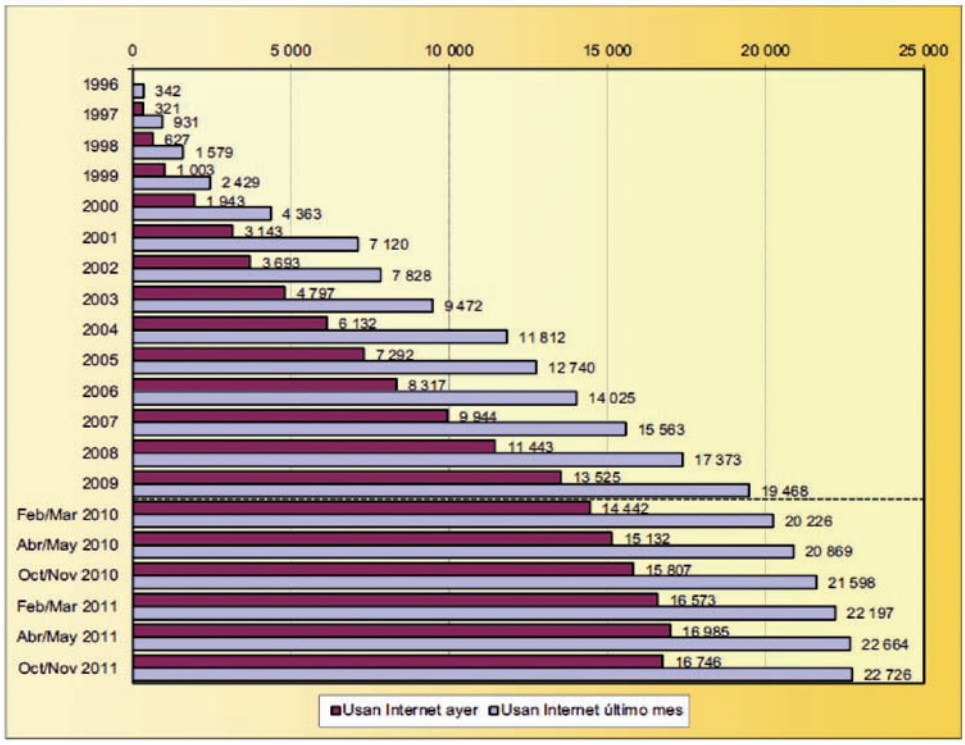
Ya podemos avanzar que estamos a remolque.

No es mi intención entrar en el tópico de la globalización de Internet, lo difícil que es legislar esta materia, no, vamos a ver cual es la respuesta que objetivamente podemos dar nosotros.

Está claro que tanto técnica, como económicamente, tenemos que apoyarnos en otros sectores, aquí muy bien representados como es Instituto Español de Estudios Estratégicos (IEEE), la Agencia de Acreditación de la Ciberseguridad, los expertos en seguridad informática y Tuenti, del Grupo Telefónica.

Centrándome en el Grupo de Delitos Telemáticos de la Guardia Civil, y su evolución junto con la ciberdelincuencia y sobre todo el desarrollo de las redes sociales, comentar que el GDT fue creado a mediados de 1996, cuando los usuarios de Internet en España no llegaban a 250.000.

Según los últimos datos, y según que fuente consultemos, ahora nos encontramos entre 22 y 30 millones de usuarios en España y seguimos creciendo.



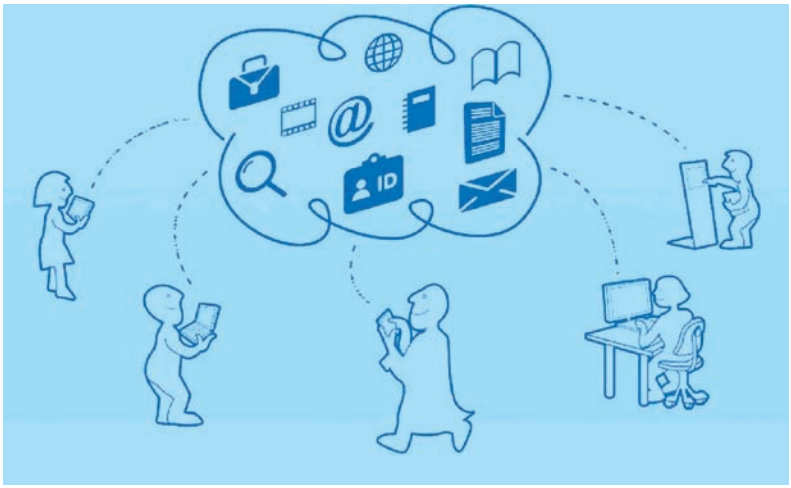
Datos recogidos de AIMC a través del Estudio General de Medios (EGM)

No vamos a demonizar a los usuarios de Internet, al decir que hay más usuarios, hay más delincuentes, no, la realidad es que al haber más usuarios hay más posibles víctimas, al existir más víctimas hay más vulnerabilidades que explotar y diferentes opciones delictivas que realizar.

Este incremento de los usuarios nos obliga a replantearnos el futuro debido a varias causas, entre la que destacaría:

PRIMERO.–La expansión de las redes sociales.

SEGUNDO.–La supervisión de las “Cloud Computing” o servicios en la nube.



TERCERO.–Las nuevas perspectivas laborales, con la posibilidad de trabajar desde cualquier lugar y en cualquier momento.

CUARTO.–El incremento en el campo de la ciberdelincuencia, con una delincuencia profesionalizada, perfectamente estructurada, dedicada a la obtención de vulnerabilidades, ya sean a nivel particular u oficial, y su posterior venta.

Es en este estamento del Ciberespacio donde nosotros desarrollamos mayoritariamente nuestro cometido, en la parte más social, donde los individuos interactúan.

El problema radica en que una persona puede tener varias identidades y una identidad puede ser utilizada por varias personas, ya sean reales, suplantadas o ficticias, lo que permite cierto anonimato y dificulta la persecución de las conductas punibles. Estas identidades pueden ser cuentas de correo electrónico, cuentas de usuario o perfiles en redes sociales.

Pero también hay que considerar que esta tecnología digital y expansión de las redes sociales, las nubes, expone a la sociedad a los ciberataques o ataques digitales, de ahí la necesidad de destinar recursos, tanto humanos como materiales, y es donde las empresas previendo esos riesgos, emplean recursos suficientes para que no se produzcan este tipo de ataques.

El modelo de ciberseguridad que se está implantando y de la que se observa una evolución, que se acentuará más en el futuro, es el paso de una cultura reactiva, es decir, se produce el daño, reaccionamos... a una cultura de prevención y flexibilidad, es decir tenemos en cuenta las posibles amenazas, o en nuestro caso tipos delictivos y tratamos de adelantarnos al mismo, también en caso de que se produzcan hay que tratar de amoldarse a la situación y evolucionar con ella.

A lo mejor nosotros como unidad policial, tenemos que mantenernos en un segundo plano, es decir continuamos en una posición reactiva, cuando se produce el delito y se denuncia, actuamos, de ahí la interacción necesaria con otras entidades, empresas u organismos.

No en vano la ciberseguridad se enfocaba a la protección de la información, ya sea de accesos, usos, revelaciones, etc., no permitidas y actualmente hay una evolución, consiste en aplicar un proceso de análisis de riesgos y gestionar los mismos, todo ello relacionado con el uso, revelaciones, etc., de la información. La seguridad del sistema se consigue cuando este se encuentra en un estado de riesgo conocido y controlado.

Y si hablamos de redes sociales, ¿podemos afirmar que es un entorno conocido? y ¿controlado?, mismas dudas nos generarían los servicios del cloud computing.

El hecho de destinar recursos a la ciberseguridad, reporta un beneficio ya que estando en la vanguardia del conocimiento y aplicación de esas tecnologías se obtiene una ventaja que podemos adaptar a las condiciones operativas de cada momento.

En la parte que nos pueden afectar las amenazas, y por ende, las denuncias que nos encontramos y encontraremos irán dirigidas contra la información y/o contra las infraestructuras de las TIC.

PRIMERO.–Denuncias contra la información tenemos:

a) Robo y publicación de datos personales: De todos es conocido el asunto de una concejal de un pueblo de la provincia de Toledo, de la que se han publicado datos de su vida íntima. La extorsión dentro de esta tipología delictiva crece exponencialmente.

b) Robo de identidad digital: Utilizando algunas de las numerosas identidades que hay disponibles se abren cuentas bancarias, se dan de alta líneas telefónicas.

c) Fraude: Compra-venta de productos, utilización fraudulenta de tarjetas bancarias, timos en la red.

SEGUNDO.–Denuncias contra la infraestructura TIC, provocan la interrupción temporal, parcial o total de determinados servicios o sistemas, existe un aumento de los ataques dirigidos, generalmente mediante el envío de código dañino.

El problema sucede con la publicación o puesta en conocimiento de estos códigos, una vez consumada la finalidad para la que fueron creados, por ello se dirigen indistintamente contra cualquier usuario que pueda ser vulnerable.

Para finalizar, no quiero dejar de citar un artículo de Samuel LINARES, en el que comparaba la situación de la ciberseguridad con los amigos y la familia, donde opinaba que el panorama actual de la ciberseguridad es como una familia, no podemos escogerla, nos ha venido dada.

Cada miembro de la familia tiene sus características y cualidades, y el secreto, de un buen entendimiento en la familia, está en la convivencia y suma de fuerzas en pro de un objetivo común (es decir una mejora general de la ciberseguridad y protección de nuestras infraestructuras y sus servicios).

Claro que en toda familia hace falta un patriarca o matriarca que, en momentos de conflicto o discusión, establezca unas reglas que todos deben seguir de forma obligatoria, al menos hasta que los miembros de la familia tengan la suficiente madurez.

Ese es el escenario actual de la ciberseguridad:

– No contamos con una coordinación común basada en unos procedimientos.

– Carecemos de una normativa especifica sobre ciberseguridad.

– Falta agilidad en la articulación de mecanismos internacionales para obtener respuestas.

Si bien todos en la familia estamos dispuestos a aportar nuestras experiencias, todavía no llegamos al acuerdo de aportarlas como si fuéramos un grupo de amigos.

Referencias bibliográficas

– http://www.aimc.es/-Navegantes-en-la-Red-.html
– http://pyme-marketing.com/usar-las-redes-sociales-para-hacer-crecer-tu-negocio/
– Informe del Consejo General de la Abogacía Española sobre la utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal.
– http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_LAS.pdf
– http://www.redseguridad.com/opinion/articulos/los-amigos-se-escogen-la-familia-no

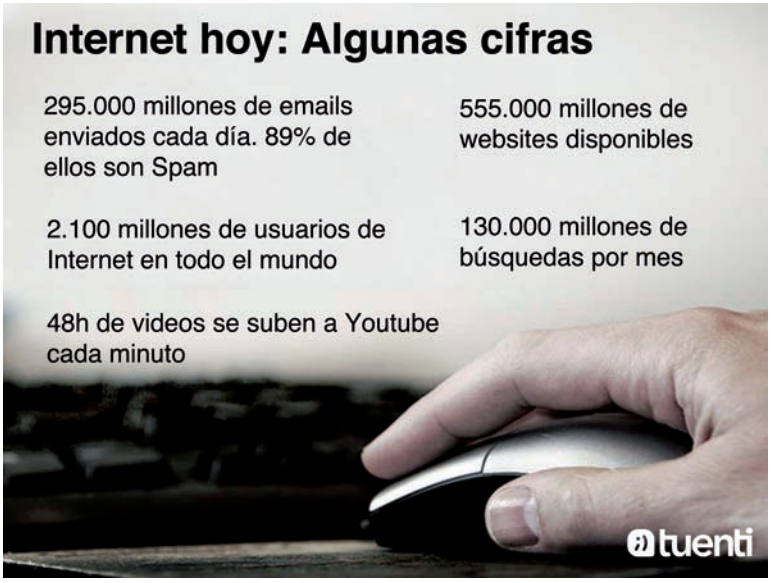
Retos presentes y futuros en materia de ciberseguridad

Ponencia de D. scar Casado Oliva
Licenciado en Derecho
Por la Universidad Autónoma de Madrid

Máster en Derecho de las Telecomunicaciones, Servicios Audiovisuales y Nuevas Tecnologías por el Instituto de Empresa.

Es abogado especializado en derecho de las Tecnologías de la Información y la Comunicación, Privacidad y Protección de Datos, Propiedad Intelectual, Comercio y Contrataci n Electr nica y Telecomunicaciones. Actualmente es el Director Jurídico y de Privacidad de Tuenti. Asimismo es vocal y miembro de la Junta Directiva de ENATIC, profesor del Instituto de Empresa y ponente y colaborador habitual en diversos foros y publicaciones relacionadas con el Derecho de las TIC, siendo coautor de diferentes obras.


01
Entorno

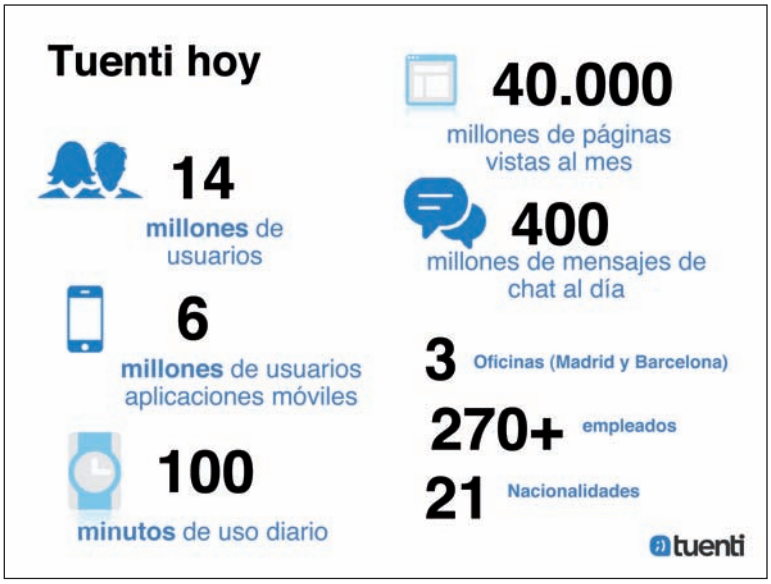

Internet hoy: Algunas cifras
295.000 millones de emails enviados cada día. 89% de ellos son Spam
555.000 millones de websites disponibles
2.100 millones de usuarios de Internet en todo el mundo
130.000 millones de búsquedas por mes
48h de videos se suben a Youtube cada minuto
tuenti

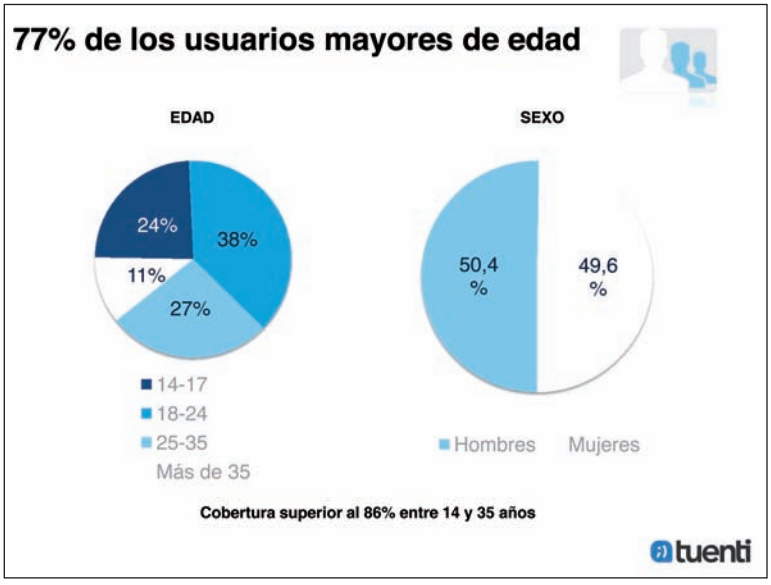

Internet es ya una realidad
68,5%
Población española internauta
13,6h.
Horas a la semana que pasa conectado el internauta español (13 horas el telespectador).
68min.
Tiempo dedicado por los españoles en redes sociales.
9 de 10
Usuarios participan en redes sociales.
96%
Jóvenes españoles que se conectan diariamente a Internet (68 minutos/día)
799m.
Internet es el segundo medio en inversión publicitaria en España.
Fuente: 1,5 IAB; 2 Mediascope; 3 Estudio Injuve; 4 McKinsey; 6 EGM
tuenti


02
Redes Sociales


Internet colaborativo
Canal multidireccional abierto que permite lograr la máxima interacción entre los usuarios y les ofrece nuevas posibilidades de colaboración, expresión y participación.
Internet social
Social Networking: Herramientas diseñadas para la creación de espacios que faciliten la creación de comunidades de intercambio social.
THE SOCIAL INTERNET
tuenti

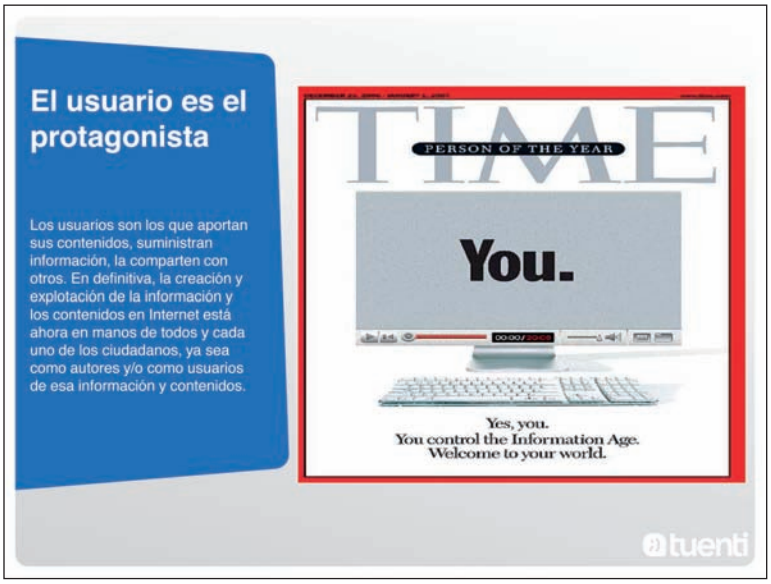

Redes sociales: ¿conversamos?
30% Tiempo en Internet que dedicamos a las redes sociales.
82% De los internautas españoles utiliza social media de forma habitual.
39% De los usuarios de redes sociales las consulta a diario .
96% De jóvenes entre 14 y 24 se han registrado alguna vez en una red social .
75% De usuarios de redes sociales opina que es el medio más divertido, frente al 14% que opina lo mismo sobre la TV.
tuenti


Tuenti hoy
14
millones de usuarios
6
millones de usuarios aplicaciones móviles
100
minutos de uso diario
40.000
millones de páginas vistas al mes
400
millones de mensajes de chat al día
3 Oficinas (Madrid y Barcelona)
270+ empleados
21 Nacionalidades
tuenti


77% de los usuarios mayores de edad
EDAD
24%
38%
11%
27%
14-17
18-24
25-35
Más de 35
SEXO
50,4 %
49,6 %
Hombres
Mujeres
Cobertura superior al 86% entre 14 y 35 años
tuenti


03
Internet segura, depende de todos


Seguridad en Internet: responsabilidad de todos
PADRES
Difundir
Concienciar
Educar
USUARIOS
Educar
Respetar
Responsabilidad
GOBIERNO E INSTITUCIONES PÚBLICAS
Políticas Públicas
Códigos de Conducta
Autorregulación
INDUSTRIA
Generar herramientas
Supervisar
Informar
tuenti


El usuario es el protagonista
Los usuarios son los que aportan sus contenidos, suministran información, la comparten con otros. En definitiva, la creación y explotación de la información y los contenidos en Internet está ahora en manos de todos y cada uno de los ciudadanos, ya sea como autores y/o como usuarios de esa información y contenidos.
TIME
PERSON OF THE YEAR
You.
Yes, you.
You control the Information Age.
Welcome to your world.
tuenti

Usuario y uso seguro de Internet

El uso de Internet debe ir acompañado de:

- ❑ **Responsabilidad**
- ❑ **Seguridad**
- ❑ **Privacidad**

tuenti

Responsabilidad

- **Tres decisiones del usuario**:
  - ✓ Cómo quiere utilizar Internet (qué productos y servicios).
  - ✓ Cómo y con quién se quiere relacionar .
  - ✓ Qué información desea compartir: fotos, su perfil, su email, información en general, etc.
- Internet ofrece un mundo de posibilidades de comunicación, productos y servicios, **pero cada uno de nosotros debe asumir su responsabilidad sobre su uso**.
- Hay que **respetar a los demás usuarios** (p.ej: compartir fotos o videos con el consentimiento de otros implicados, respetar ideas ajenas, etc.).

tuenti

Seguridad

- Como en cualquier otra área de la vida, los usuarios deben tomar las **precauciones necesarias para proteger su información**:
  - ✓ Crear una **contraseña** que no sea evidente.
  - ✓ Cambiar de **contraseña** frecuentemente.
  - ✓ **Acceder a páginas seguras.**
  - ✓ No abrir **correos spam** y denunciarlos.
  - ✓ Navegar con **ordenadores seguros y antivirus.**

tuenti

Privacidad

- Como parte de su responsabilidad de uso de Internet, los usuarios deben entender que ellos mismos tienen a su alcance **herramientas que les permite controlar su privacidad**.
- ¿Qué significa la **privacidad en Internet**?
  - Decidir lo que es **público y privado.**
  - **Restringir o permitir acceso a información** que generas.
- En caso de duda, consultar la política de privacidad del servicio o producto que se utiliza para conocer qué información se recoge, y las herramientas de control que ofrece.

tuenti

El papel de las empresas en el uso seguro de Internet

tuenti

04

Tuenti: Nuestra estrategia de seguridad y privacidad

Garantía de privacidad y seguridad

Modelo de acceso por **invitación o teléfono móvil verificado**.

La información personal de los usuarios **no se indexa en ningún buscador**.

Gente **real,** información **real,** relaciones **reales**.

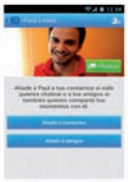
tuenti

Nuevo modelo de privacidad muy sencillo

agregar como

amigo

contacto



Tú

Amigos

Contactos

"Chatea con tus contactos, comparte sólo con tus mejores amigos"

tuenti

Nuevo panel de privacidad muy sencillo y fácil de manejar

- Interfaz sencilla y fácil de manejar.
- El usuario puede configurar el grado de privacidad con el que quiere relacionarse en la red social.
- El usuario puede controlar en todo momento la privacidad de su perfil y sus diferentes elementos: fotos, tablón, recepción de mensajes y/o la visibilidad de números de teléfono.

TRANSPARENCIA, CONTROL Y ELECCIÓN

tuenti

Máximo nivel de privacidad por defecto

- ✓Sólo tus amigos ven tu tablón.
- ✓Sólo tus amigos pueden descargar tus fotos.
- ✓Sólo tus amigos pueden ver tu número de teléfono.
- ✓Sólo tus amigos pueden enviarte mensajes privados.

tuenti

Nueva Política de Privacidad

- ❑ Lenguaje sencillo y comprensible.
- ❑ Fácilmente accesible, clara y didáctica.
- ❑ Informamos de forma transparente a los usuarios sobre el uso de sus datos personales cuando utilizan nuestro servicio.
- ❑ Educamos a través de medios audiovisuales sobre privacidad.
- ❑ Los usuarios pueden controlar sus datos personales.

TRANSPARENCIA, SENCILLEZ Y CLARIDAD

tuenti

05 Tuenti: Educación y colaboración

Nuestro compromiso con la seguridad de los menores

Tuenti está comprometido con la protección de los menores en su plataforma y nuestra motivación principal es ofrecer una experiencia segura a todos nuestros usuarios. Nuestros objetivos son:

- ***Dotar*** a los menores, padres y educadores de las herramientas adecuadas para que puedan reportar cualquier contenido inapropiado, perfil sospechoso o falso, suplantación de identidad o cualquier otro material o conducta ilegal.
- ***Proteger*** a los menores a través de colaboraciones con las autoridades policiales y organizaciones.
- ***Informar y educar*** a los menores para mantener su seguridad y proteger su privacidad en Tuenti.

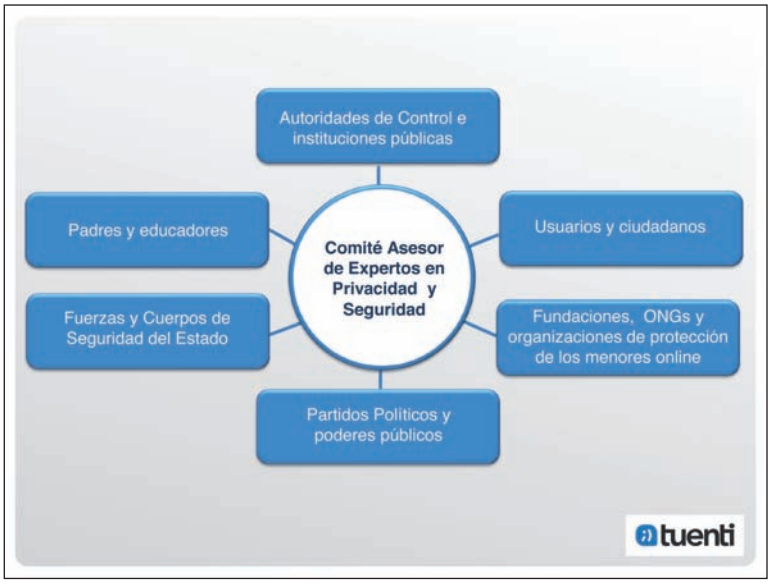
tuenti

Nuevo Centro de Ayuda y Seguridad (tuenti.com/privacidad)

- **Objetivo:** Espacio donde formar e informar a menores, padres y educadores con el fin de conseguir un uso responsable y seguro de nuestra red social. Es además un canal de comunicación bidireccional y de acceso libre para todos, sean o no usuarios registrados de la red social.

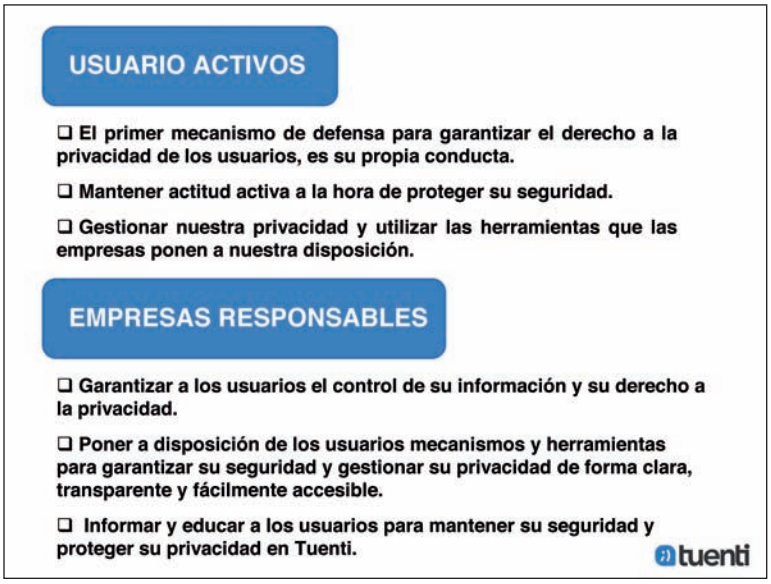
- **Funciones:**
  - ✓ Proporcionar información de forma centralizada sobre las herramientas de seguridad y mecanismos de reporte.
  - ✓ Ofrecer consejos y recomendaciones de seguridad a los menores, padres y educadores.
  - ✓ Colaborar con organizaciones, con otras empresas del sector y con instituciones públicas dedicadas a la protección de menores.
  - ✓ FAQs, Glosario.

tuenti


Autoridades de Control e instituciones públicas
Padres y educadores
Comité Asesor de Expertos en Privacidad y Seguridad
Usuarios y ciudadanos
Fuerzas y Cuerpos de Seguridad del Estado
Fundaciones, ONGs y organizaciones de protección de los menores online
Partidos Políticos y poderes públicos
tuenti


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
CONFIANZA ONLINE
DEFENSOR DEL MENOR DE ANDALUCÍA
esnq
EUROPEAN SOCIAL NETWORKS GROUP
fundación alia2
AUTOCONTROL
ANAR FUNDACIÓN
red.es
protegeles.com
CHAVALES esto es nuestro web
European Commission
plataforma de infancia
Fundación hazloposible
oficina de seguridad del internauta
CONTROLA CLAVE
Telefónica
Pantallas Amigas
fundación mapfre
INTECO
Foro generaciones interactivas
WWW 2.0
Banesto FUNDACIÓN
unicef
Save the Children
Fundación Antena 3
Fundación BT
Cruz Roja Juventud
AMETIC
JUNTA DE ANDALUCÍA
ins@fe
cecu madrid
Siena
tuenti


06
Conclusiones


USUARIO ACTIVOS
❑ El primer mecanismo de defensa para garantizar el derecho a la privacidad de los usuarios, es su propia conducta.
❑ Mantener actitud activa a la hora de proteger su seguridad.
❑ Gestionar nuestra privacidad y utilizar las herramientas que las empresas ponen a nuestra disposición.
EMPRESAS RESPONSABLES
❑ Garantizar a los usuarios el control de su información y su derecho a la privacidad.
❑ Poner a disposición de los usuarios mecanismos y herramientas para garantizar su seguridad y gestionar su privacidad de forma clara, transparente y fácilmente accesible.
❑ Informar y educar a los usuarios para mantener su seguridad y proteger su privacidad en Tuenti.
tuenti


¡Gracias!
tuenti.com/privacidad
Tuenti Technologies I Plaza de las Cortes 2, 4ª Planta I
28014 I Madrid I Tel. +34 91.429.40.39 I
privacidad@tuenti.com
tuenti

9 788481 503081