

# **Trabajo Fin de Máster**

Estudio de Metodologías de Ingeniería Social

Máster Interuniversitario en Seguridad de las Tecnologías de la  
Información y de las Comunicaciones (MISTIC)

Alumno: **Rafael Marín Jiménez**

Área del trabajo final: **Ad-hoc**

Consultora: **Angela María García Valdés**

Profesor: **Víctor García Font**

Fecha Entrega: **04/06/2018**



Esta obra está sujeta a una licencia de [Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-sa/3.0/es/)

**FICHA DEL TRABAJO FINAL**

<b>Título del trabajo:</b>	<i>Estudio de Metodologías de Ingeniería Social</i>
<b>Nombre del autor:</b>	<i>Rafael Marín Jiménez</i>
<b>Nombre del consultor/a:</b>	<i>Ángela María García Valdés</i>
<b>Nombre del PRA:</b>	<i>Víctor García Font</i>
<b>Fecha de entrega (mm/aaaa):</b>	06/2018
<b>Titulación::</b>	<i>Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones</i>
<b>Área del Trabajo Final:</b>	<i>TFM Ad-hoc</i>
<b>Idioma del trabajo:</b>	<i>Castellano</i>
<b>Palabras clave</b>	<i>Ingeniería Social, Engaño, CiberSeguridad</i>

**Resumen del Trabajo (máximo 250 palabras):**

Este trabajo consiste en un estudio sobre las técnicas de ingeniería social y los métodos usados para obtener información. Para ello se hace uso de algunos estudios e informes publicados, en los que el factor humano y por tanto la ingeniería social, adoptan un papel protagonista.

En primer lugar se lleva a cabo la caracterización de la temática a través del análisis del factor humano como recurso vulnerable habilitante, del conocimiento de las distintas categorías y técnicas empleadas, del estudio de las etapas en las que se divide según diversos autores y de su configuración como proceso. A continuación se adentra en las principales motivaciones de un ciberdelincuente de cara al empleo de vectores de ataque basados en ingeniería social, básicamente los beneficios alcanzables a través de la información obtenida. Como contrapartida, se ofrece una visión respecto del tratamiento que esta técnica tiene en las normas legales, poniendo el foco en la consideración como delito penal. El trabajo no olvida realizar un repaso de las estadísticas relativas a ciberincidentes registrados y cibercriminalidad, los estudios publicados y algunas brechas de seguridad populares. Finalmente se exponen algunas estrategias de gestión de riesgos con impacto en la ingeniería social, enumerando pautas para combatirla a distintos niveles.

El resultado de este trabajo podría definirse como una detallada manifestación del estado del arte entorno a esta amenaza de seguridad para las organizaciones, pretendidamente actualizado y fundamentado en una ingente cantidad de fuentes autorizadas de información. Una buena base para la capacitación de profesionales de seguridad de la información y la elaboración de material destinado a empleados.

**Abstract (in English, 250 words or less):**

This work consists of a study about social engineering techniques and the methods used to obtain information. For that purpose, some studies and published reports are used in which the human factor and, therefore, social engineering take a crucial role.

In the first place, the characterization of the subject is carried out through the analysis of the human factor as a vulnerable enabling resource, the knowledge of the different categories and techniques used, the study of the stages in which it is divided according to different authors and its configuration as a process. Then, it delves into the main motivations of a cybercriminal for the use of attack vectors based on social engineering, basically the benefits achievable through the information obtained. In return, a view is offered regarding the treatment that this technique has in the legal norms, placing the focus on consideration as a criminal offense. The work does not forget to review the statistics related to registered cyber-incidents and cybercrime, published studies and some popular security gaps. Finally, some risk management strategies with impact on social engineering are exposed, listing guidelines to respond it at different levels.

The result of this work could be defined as a detailed manifestation of the state of the art knowledge around this security threat for organizations, supposedly updated and based on a huge number of authoritative sources of information. A good base for the training of information security professionals and the preparation of material for employees.

## Sumario

1	Introducción.....	2
1.1	Contexto y justificación del Trabajo.....	2
1.2	Objetivos del Trabajo.....	3
1.3	Enfoque y método seguido.....	4
1.4	Planificación del Trabajo.....	5
1.5	Presupuesto del proyecto.....	8
1.6	Análisis de viabilidad/riesgos que pueden surgir en el desarrollo.....	8
1.7	Estado del arte.....	9
1.8	Breve descripción de los otros capítulos de la memoria.....	13
2	Descripción de ingeniería social.....	15
2.1	Definición y contexto.....	15
2.2	El elemento humano.....	18
2.2.1	Características humanas Innatas.....	19
2.2.2	Características humanas aprendidas.....	20
2.2.3	La persuasión.....	21
2.3	Categorías y técnicas.....	22
2.3.1	Categorías.....	22
2.3.2	Técnicas.....	23
2.4	Roles que intervienen y sus características.....	27
2.4.1	El ingeniero social.....	27
2.4.2	El "empleador" o contratista.....	28
2.4.3	La víctima.....	29
2.4.4	El responsable/s de seguridad.....	29
3	Etapas de la Ingeniería Social.....	29
3.1	Etapas Gartner-2001.....	30
3.2	Etapas Richardus Eko 2017.....	31
4	El proceso de la ingeniería social.....	34
5	Descubrimiento del tipo de información que puede llegar a obtenerse.....	37
6	Formas de utilización de la información para obtener beneficios.....	40
7	Análisis legal de la ingeniería social en el marco de la ciberdelincuencia.....	45
7.1	Panorama internacional.....	45
7.2	Enfoque nacional.....	48
7.3	La ingeniería social como ciberdelito.....	50
8	La ingeniería social en números.....	51
8.1	Ciberincidentes registrados.....	51
8.1.1	Instituto de Auditores Internos.....	51
8.1.2	Verizon.....	52
8.1.3	CCN-CERT IA-09/18: Ciberamenazas y Tendencias Edición 2018.....	54
8.1.4	APWG: grupo de trabajo antiphishing.....	55
8.2	Cibercriminalidad.....	56
8.2.1	Portal estadístico del Ministerio del Interior español.....	56
8.2.2	Fiscal General del Estado.....	60
8.3	Estudios publicados.....	62
8.3.1	Special Eurobarometer 464a:.....	62
8.3.2	Sobre la anatomía de los ataques de ingeniería social:.....	64
8.3.3	Todo es cuestión de Benjamins:.....	64
8.3.4	CEFRIEL: La subestimada amenaza de la ingeniería social.....	65
8.3.5	Prueba de intervenciones frente a la amenaza de la ingeniería social.....	66

---

8.3.6	ONTSI - Ciberseguridad y Confianza en los hogares españoles.....	68
8.4	Brechas de seguridad.....	69
8.4.1	La ICANN fue objeto de un ataque de spear phishing.....	69
8.4.2	Carbanak.....	70
8.4.3	Otras brechas conocidas.....	71
9	Estrategias de gestión de riesgos.....	71
9.1	Especializar a los profesionales de ciberseguridad.....	72
9.2	Evaluar el factor humano.....	74
9.3	La transferencia del ciberriesgo.....	78
10	Pautas para combatir la ingeniería social.....	80
10.1	Pautas para la víctima potencial.....	81
10.1.1	Conoce las formas de ocultar la identidad que usan los estafadores.....	82
10.1.2	Conoce los tipos de estafas y sus señales:.....	82
10.1.3	Reacciona o actúa siguiendo las siguientes recomendaciones:.....	84
10.2	Pautas para la empresa/organización.....	85
10.2.1	Buenas prácticas recomendadas.....	85
10.2.2	Estándares de seguridad.....	87
10.2.3	Auditorías.....	88
10.2.4	Formación.....	93
10.2.5	El Plan de Cultura de Ciberseguridad.....	96
10.3	Pautas para los estados.....	100
10.3.1	Medición.....	100
10.3.2	Regulación.....	101
11	Conclusiones.....	105
12	Glosario.....	107
12.1	Términos.....	107
12.2	Acrónimos.....	108
13	Bibliografía.....	110
14	Autorizaciones de reproducción de contenidos.....	116
15	Anexos.....	122
15.1	Anexo I: Phishing.....	122
15.2	Anexo II: Conjunto de herramientas de ingeniería social (SET).....	125

## Índice de ilustraciones

Ilustración 1: Jornada de descanso.....	7
Ilustración 2: Jornada laboral.....	7
Ilustración 3: Diagrama de Gantt.....	8
Ilustración 4: ISO 27032:2012 - Controles frente a ataques de Ingeniería Social.....	16
Ilustración 5: INTECO. Proceso de ataque ATP.....	17
Ilustración 6: CEFRIEL. Proceso de ataque ATP.....	18
Ilustración 7: Ejemplo diagrama DAIS. Extracto material UOC.....	35
Ilustración 8: DAIS normalizado. Elaboración propia.....	36
Ilustración 9: DAIS para la modificación de una nota en el expediente académico.....	37
Ilustración 10: Comercio clandestino de datos. Informe McAfee Intel Security 2015.....	41
Ilustración 11: Comercio clandestino de datos. Informe McAfee Intel Security 2015.....	41
Ilustración 12: Direcciones de correo electrónico en venta. <a href="https://www.welivesecurity.com">https://www.welivesecurity.com</a> .....	42
Ilustración 13: Ejemplo identidad a la venta. Comercio clandestino de datos. Informe McAfee Intel Security 2015.....	43
Ilustración 14: Cuadro tipologías penales. SEC: Sistema Estadístico de Criminalidad....	49
Ilustración 15: IAI. Guía de supervisión de la ciberseguridad.....	52
Ilustración 16: Porcentaje de brechas de seguridad por categoría de activo.....	53
Ilustración 17: Brechas sociales ordenadas por tipo de industria (n=351).....	54
Ilustración 18: Tipos de datos comprometidos en brechas sociales (n=362).....	54
Ilustración 19: CCN-CERT IA-09-18 CIBERAMENAZAS Y TENDENCIAS 2018.....	55
Ilustración 20: APWG. Estadísticas destacadas de phishing del último trimestre de 2017 .....	56
Ilustración 21: Elaboración propia (SEC). Hechos conocidos. Cibercriminalidad.....	57
Ilustración 22: Elaboración propia a partir de los datos del SEC. Hechos esclarecidos. Cibercriminalidad.....	58
Ilustración 23: Elaboración propia a partir de los datos del SEC. Detenciones e investigados.....	59
Ilustración 24: Elaboración propia a partir de los datos del SEC. Victimizaciones. Cibercriminalidad.....	60
Ilustración 25: Acusaciones formuladas por el Ministerio Fiscal en 2016.....	61
Ilustración 26: Diligencias de investigación del Ministerio Fiscal en 2016.....	62
Ilustración 27: Eurobarómetro. Factsheets. España. 3.QB12.....	63
Ilustración 28: Eurobarómetro. Factsheets. España. 3.QB3.4.....	63
Ilustración 29: Resultados evaluaciones. Fuente: Cefriel.....	65
Ilustración 30: ¿Cómo robó 1 billón de dólares el cibergrupo Carbanak? Un ataque dirigido a un banco.....	70
Ilustración 31: Ciberseguridad. Una guía de supervisión. Instituto de Auditores Internos.....	72
Ilustración 32: KSA-T del Ciberinstructor.....	73
Ilustración 33: KSA-T del Analista Evaluador de Vulnerabilidades.....	74
Ilustración 34: CCN-CERT IA-09-18 Ciberamenazas y tendencias 2018.....	79
Ilustración 35: Cobertura de un producto típico de ciberriesgos. Fuente: AON.....	80
Ilustración 36: Marco de Trabajo para Construir "Firewalls" Humanos. Reproducido con autorización.....	86
Ilustración 37: CSC7-Control y objetivo de control de auditoría (IAI).....	89
Ilustración 38: CSC17-Control y objetivo de control de auditoría (IAI).....	89
Ilustración 39: Retroampliación inversa. Diagrama DAIS normalizado. Material UOC.....	92

Ilustración 40: Retroampliación inversa. Diagrama DAIS normalizado y ampliado. Material UOC.....	92
Ilustración 41: INCIBE. Fases del kit de concienciación.....	99
Ilustración 42: ENISA. Phishing como vector de ataque.....	122
Ilustración 43: Itinerario dañino más frecuente seguido por los atacantes.....	122
Ilustración 44: Posición del phishing en la "kill chain".....	124





# 1 Introducción

## 1.1 Contexto y justificación del Trabajo

El trabajo consiste en un estudio sobre las técnicas de ingeniería social y los métodos usados para obtener información. Pero, ¿cuál es la necesidad de este estudio?, ¿qué problema se pretende resolver con ello? Para dar respuesta a estas cuestiones haremos uso de algunos estudios publicados, en los que el factor humano y por tanto la ingeniería social, adoptan un papel protagonista.

A pesar de que la mayoría de los ciberataques en 2016 fueron piratería y relacionados con malware, tres de las cinco principales amenazas de ciberataques se relacionaron con factores humanos, siendo estos; ingeniería social a través de correos electrónicos de phishing, errores humanos y uso indebido deliberado.<sup>1</sup> En 2015, 21.8% y en 2016, 15.8% de todas las filtraciones de datos se debieron a phishing, spoofing o ingeniería social, mientras que en 2017, los errores humanos representaron entre 19% y 36% de todas las violaciones de datos, dependiendo del país o región.<sup>2</sup> Además de las ciberamenazas, existe el desafío adicional de garantizar la seguridad física cuando se habla de operadores humanos, especialmente cuando se enfrentan a amenazas internas, ya que la ciberseguridad abarca elementos humanos / físicos intrínsecos. Las políticas dirigidas a mantener un escritorio limpio de documentos clasificados, bloquear pantallas y sistemas cuando el usuario está lejos del ordenador, cuestionar al personal que no muestra sus credenciales de identificación en las áreas o departamentos de negocio y aplicar controles de acceso a edificios, son todas medidas de protección física que deben incorporarse en una organización.

Así pues, queda demostrada la contribución humana al ciberriesgo. Sin embargo, no es tarea fácil impartir formación, aumentar la conciencia e influir en el comportamiento de los empleados para mitigar estos riesgos. Estas actividades están predestinadas al fracaso si se ignoran el factor humano en el desarrollo y despliegue de políticas y procesos de ciberseguridad.

El personal buscará activamente eludir las políticas de seguridad que les impiden completar sus funciones, les imponen lo que ellos consideran una carga injustificada y/o están desalineadas respecto de lo que debe ser priorizado. Esto generalmente no es por malicia o ambivalencia, sino por el deseo de hacer correctamente su trabajo. Por ejemplo, las políticas corporativas estrictas sobre el uso de dispositivos privados en el trabajo pueden considerarse innecesariamente gravosas para los empleados. La imposición de contraseñas múltiples y complejas que deben ser cambiadas regularmente sin permitir el uso de gestores de contraseñas, obliga al personal a escribir sus contraseñas para memorizarlas, posiblemente utilizando medios electrónicos. El personal (en contra de las políticas de seguridad) deja iniciada la sesión en los ordenadores de los servicios de emergencias del hospital, priorizando el tratamiento inmediato de los pacientes con el fin de salvar sus vidas, a riesgo de desproteger la información de los pacientes.<sup>3</sup>

1 2016 – Verizon – Data Breach Investigations Report.

2 2017 – Ponemon Institute – Cost of Data Breach Study

3 ENISA, Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures, 2016.

Además, los seres humanos poseen una limitada capacidad para cumplir con los requisitos de seguridad en el lugar de trabajo. Superado cierto umbral, cualquier intento de imponer requisitos y procedimientos de seguridad adicionales se topará con resistencia e intentos de eludirlos. Se ha observado en muchos lugares de trabajo, que la mayoría de los usuarios han superado este umbral de cumplimiento desde hace mucho tiempo.<sup>4</sup>

El desarrollo de una cultura de ciberseguridad es importante para gestionar el riesgo asociado al factor humano, al tiempo que permite la adopción y el uso de nuevas tecnologías por parte de las empresas. Se debe buscar efectividad, flexibilidad y adaptabilidad, respaldados por una fuerte cultura de ciberseguridad. Las innovaciones, como adoptar una política de uso de dispositivos propios (byod) o adquirir un nuevo socio comercial, pueden hacer que las organizaciones se expongan, pero son necesarias para mantener la competitividad y el crecimiento. Una buena cultura de ciberseguridad inculcará una mentalidad de seguridad en las personas en todas las facetas de su trabajo e incluso puede extenderse a su vida privada.

## 1.2 Objetivos del Trabajo

Los objetivos que se expresan a continuación, cuando no lo mencionen expresamente, deben ser enmarcados en el ámbito de la ingeniería social como riesgo para la seguridad de la información. Como es bien sabido, por repetido y no tanto por asentado en las organizaciones, la seguridad de la información no debe ser vista como un fin en sí misma, sino más bien como un medio para lograr el éxito del negocio, garantizar los derechos y la confianza de empleados/clientes/usuarios, cumplir con el marco legal de aplicación, etc.

Expuestos los antecedentes, a continuación se enumeran los objetivos generales del presente TFM:

1. Recopilar material de acceso público de distintas fuentes de información de confianza, para construir el marco de trabajo de soporte al resto de los objetivos.
2. Documentar, textual y gráficamente cuando sea posible, los conceptos, métodos, estrategias y roles que intervienen en los procesos de ingeniería social.
3. Ilustrar los principales tipos de información de interés para el ingeniero social, poniendo el foco en los beneficios que pueden proporcionar.
4. Exponer las repercusiones legales derivadas del empleo no autorizado de la ingeniería social.
5. Poner en valor el factor humano como elemento a considerar en la política de seguridad de la información de una organización.
6. Enumerar las mejores prácticas y recomendaciones para mitigar el riesgo de exposición a la ingeniería social, ponderando el uso de diagramas de ataque de ingeniería social.
7. Desarrollar los ítems de un plan de cultura de ciberseguridad, acotando el alcance al contexto de la ingeniería social, y trabajando el conocimiento, las creencias, las percepciones, las actitudes, las suposiciones, las normas y los valores de las personas.

---

<sup>4</sup> Herley, C. More is Not the Answer.

8. Diseñar e implementar objetos de aprendizaje con herramientas abiertas que faciliten la implantación de los ítems del plan de cultura de ciberseguridad.

Estos objetivos están enumerados atendiendo a una mera ordenación cronológica, pensados de manera secuencial, de modo que para alcanzar uno es preciso haber satisfecho el anterior. No obstante, caben excepciones que se verán reflejadas en la concurrencia de alguna de las tareas derivadas de cada objetivo.

En relación a la priorización que se asigna a tales objetivos a fin de valorar la importancia de los mismos de cara al resultado final del TFM, resulta oportuno reflejar lo siguiente:

- Hay tres grandes bloques de objetivos; el primero comprende los objetivos 1, 2 y 3, cuya finalidad es la caracterización de la temática del TFM; el segundo comprende los objetivos 4 y 5 que persigue enfatizar el factor humano para satisfacer el cumplimiento legal; y el tercero comprende los objetivos 6, 7 y 8, dedicado a ofrecer soluciones al problema de la ingeniería social.
- El bloque tercero sería un requisito imprescindible para toda empresa, una vez asumida la importancia de controlar la ingeniería social. Esto significa que todos los objetivos previos han de ser considerados como los cimientos sobre los que construir el programa de trabajo y medidas derivadas orientadas a mitigar los riesgos de seguridad de la información asociados al factor humano.

### 1.3 Enfoque y método seguido

La metodología empleada para el desarrollo del presente TFM está basada en el estudio de los recursos y la información relevante accesible públicamente, y puede disgregarse en las siguientes técnicas:

1. El aprendizaje de contenidos basado en lecturas, análisis y reflexión de textos sobre la materia.
2. La búsqueda y gestión de información necesaria para el análisis de las situaciones, realización de comparativas, toma de decisiones, etc.
3. La participación como usuario en los recursos online disponibles (juegos, redes sociales, foros, encuestas/test, módulos educativos, etc.)
4. La recogida de datos cuantitativos de organismos oficiales o entidades especializadas en la materia.
5. La documentación estructurada del material investigado, las experiencias de usuario, los casos de uso y las posibles soluciones.
6. El diseño e implementación de objetos virtuales de aprendizaje específicos.

Esta metodología parece adecuada para alcanzar los objetivos propuestos, potenciando la autonomía del autor y minimizando el consumo de recursos. Inicialmente no se llevará a cabo trabajo de campo, ni implementación y validación de una innovación, a excepción de sugerencia detallada al respecto de la directora del TFM.

Las fases o etapas en las que se divide el proyecto están estrechamente relacionadas con los hitos establecidos por la asignatura, quedando reflejadas en la planificación de tareas

descrita en el siguiente apartado. A modo de resumen, dichas fases son: Preparación, PEC1, PEC2, PEC3, PEC4-memoria, PEC5-presentación y Defensa.

## 1.4 Planificación del Trabajo

Cada objetivo definido va a requerir de un conjunto de tareas para su consecución, además de las tareas de preparación y soporte, lo que reflejamos en la siguiente tabla:

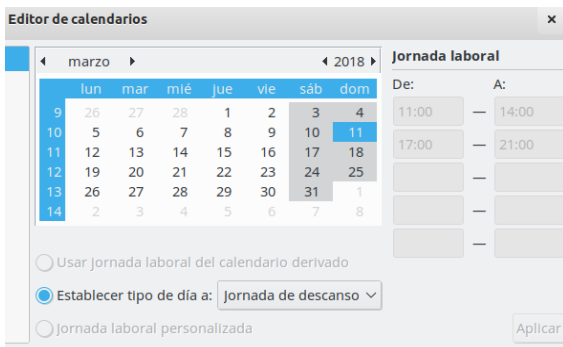
<b>Objetivo 1:</b>	Recopilar material de acceso público de distintas fuentes de información de confianza, para construir el marco de trabajo de soporte al resto de los objetivos.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Determinar las fuentes de información de confianza.</li> <li>b) Localizar la información y recursos de interés de cada fuente.</li> <li>c) Revisar los derechos que rigen la reutilización de la información elegida.</li> <li>d) Evaluar minuciosamente la información y recursos reutilizables.</li> <li>e) Seleccionar y clasificar la información final como marco de trabajo.</li> </ul>
<b>Objetivo 2:</b>	Documentar, textual y gráficamente cuando sea posible, los conceptos, métodos, estrategias y roles que intervienen en los procesos de ingeniería social.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Adaptar el formato y contenido de la plantilla para la elaboración de la memoria.</li> <li>b) Definir los apartados que alojarán los contenidos recogidos en el objetivo.</li> <li>c) Extraer la información del material, combinarla y expresarla de forma personal.</li> <li>d) Generar las ilustraciones y gráficas que aporten valor al texto cuando las mismas no existan o no sean reutilizables.</li> </ul>
<b>Objetivo 3:</b>	Ilustrar los principales tipos de información de interés para el ingeniero social, poniendo el foco en los beneficios que pueden proporcionar.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Construir posibles casos de uso que motiven el empleo de ingeniería social.</li> <li>b) Identificar la información objetivo del ingeniero social para cada caso.</li> <li>c) Documentar la relación entre la información obtenida y los beneficios derivados.</li> <li>d) Ejemplificar los casos acudiendo a noticias reales, películas, documentales...</li> </ul>
<b>Objetivo 4:</b>	Exponer las repercusiones legales derivadas del empleo no autorizado de la ingeniería social.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Localizar la normativa legal de aplicación al caso de la ingeniería social.</li> <li>b) Encontrar jurisprudencia regional, nacional y comunitaria.</li> <li>c) Hallar informes de analistas expertos en derecho.</li> <li>d) Redactar una visión de conjunto.</li> </ul>
<b>Objetivo 5:</b>	Poner en valor el factor humano como elemento a considerar en la política de seguridad de la información de una organización.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Analizar y documentar la naturaleza humana.</li> <li>b) Enmarcar el factor humano entre las vulnerabilidades del sistema.</li> <li>c) Documentar el riesgo real del factor humano a partir de las investigaciones existentes.</li> <li>d) Esbozar estrategias de mitigación del riesgo poniendo el foco en la política de seguridad.</li> </ul>
<b>Objetivo 6:</b>	Enumerar las mejores prácticas y recomendaciones para mitigar el riesgo de exposición a la ingeniería social, ponderando el uso de diagramas de ataque de ingeniería social (DAIS).

<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Expresar formas de auditar el elemento humano.</li> <li>b) Planificar formación teórica y práctica, dirigida y personalizada.</li> <li>c) Diseñar un plan de cultura de ciberseguridad.</li> <li>d) Aplicar técnicas de retro-ampliación inversa del diagrama DAIS.</li> </ul>
<b>Objetivo 7:</b>	Desarrollar los ítems de un plan de cultura de ciberseguridad, acotando el alcance al contexto de la ingeniería social, y trabajando el conocimiento, las creencias, las percepciones, las actitudes, las suposiciones, las normas y los valores de las personas.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Seleccionar los ítems del plan de cultura de ciberseguridad afectados.</li> <li>b) Establecer las áreas culturales a cubrir para cada ítem.</li> <li>c) Desarrollar el contenido de cada ítem.</li> </ul>
<b>Objetivo 8:</b>	Diseñar e implementar objetos de aprendizaje con herramientas abiertas que faciliten la implantación de los ítems del plan de cultura de ciberseguridad.
<b>Tareas:</b>	<ul style="list-style-type: none"> <li>a) Adquirir conocimiento básico del funcionamiento de la/s herramienta/s elegida/s.</li> <li>b) Formular los ítems elegidos del plan de cultura de ciberseguridad como objetos de aprendizaje virtuales, estableciendo sus objetivos, contenidos y sistema de evaluación.</li> <li>c) Trasladar los objetos de aprendizaje a la/s herramienta/s elegida/s.</li> <li>d) Generar el archivo/s exportable/s estandarizado para su utilización en plataformas de teleformación, típicamente SCORM.</li> </ul>
<b>Tareas de preparación y soporte:</b>	<ol style="list-style-type: none"> <li>1. Revisión de la Guía del TFM de Aplicación Profesional.</li> <li>2. Revisión del Plan Docente del TFM.</li> <li>3. Revisión del documento titulado "Presentación de documentos y elaboración de presentaciones".</li> <li>4. Revisión del documento titulado "Redacción de textos científico-técnicos".</li> <li>5. Revisión de los criterios de evaluación del TFM.</li> <li>6. Revisión de la Guía del TFM comunicado por la tutora.</li> <li>7. Elaboración del modelo de documento para la entrega de las PEC.</li> <li>8. Instalación del software específico empleado como recursos del TFM.</li> </ol>

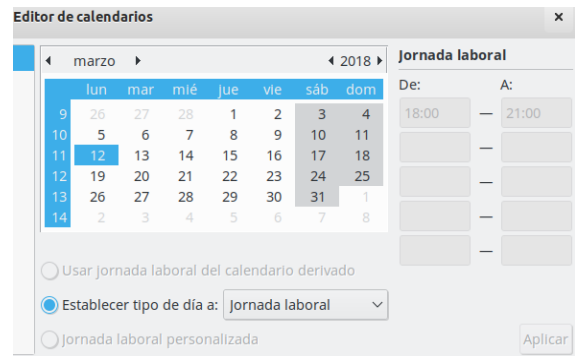
Para la adecuada planificación del trabajo haremos uso de la herramienta *Planner*<sup>5</sup>, donde comenzaremos definiendo un calendario, unos recursos y las mencionadas tareas. El calendario establecerá la jornada laboral, la jornada de descanso y las horas aproximadas de dedicación. Los recursos registrarán el material, el hardware, el software y las personas que serán precisos para el desempeño de las tareas. Finalmente, se realizará un inventario de tareas agrupadas por objetivos y éstos por fases, especificando el esfuerzo de trabajo previsto para cada una.

Calendario:

<sup>5</sup> Una aplicación de gestión de proyectos para el escritorio GNOME.  
<http://live.gnome.org/Planner>



*Ilustración 1: Jornada de descanso*



*Ilustración 2: Jornada laboral*

## Recursos:

### Información

- Referenciados en el apartado anterior

### Software

- LibreOffice: paquete ofimático o de productiva.
- Planner: aplicación de gestión de proyectos para escritorio GNOME.
- eXe Learning: editor de recursos educativos interactivos gratuito y de código abierto.
- OpenShot Video Editor: crea, modifica y edita ficheros de vídeo.

### Materiales

- Ordenador/Portátil
- Videocámara y micrófono

### Humanos

- El autor del presente TFM: Rafael Marín Jiménez
- Profesora colaboradora, directora del TFM: Ángela María García Valdés
- Profesor: Víctor García Font

## Diagrama de Gantt:

Para consultar el detalle completo de la planificación sin agregación de tareas, se debe revisar el documento "TFM\_v2\_planner.html".

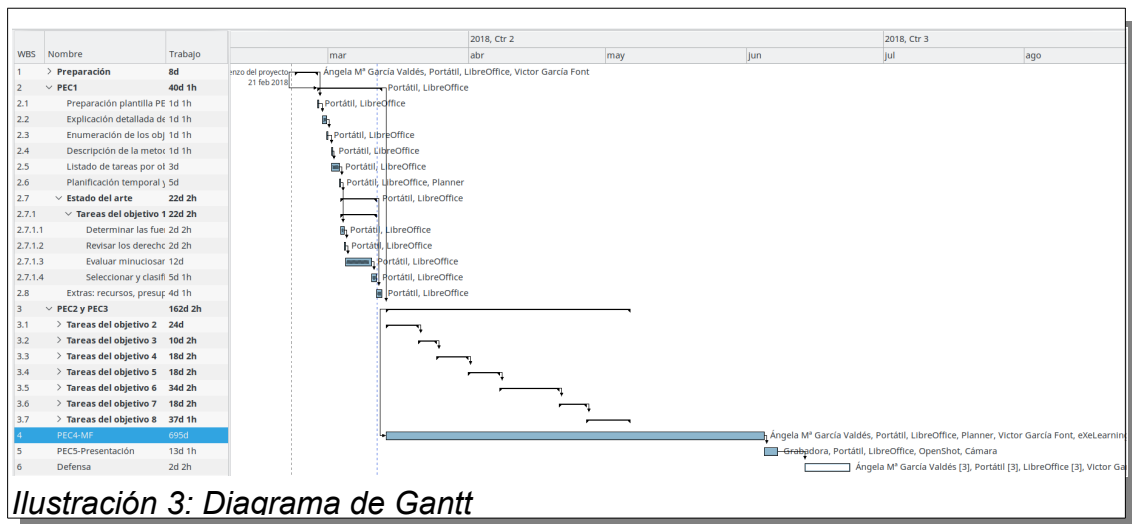


Ilustración 3: Diagrama de Gantt

## 1.5 Presupuesto del proyecto

El proyecto no contempla recursos económicos en su planificación inicial, potenciando el trabajo de investigación y la utilización de recursos gratuitos. Si la evolución del proyecto o las directrices que marque la dirección del mismo desde la UOC, orientan los objetivos del mismo en otro sentido, los fondos deberán ser aportados por quien corresponda.

## 1.6 Análisis de viabilidad/riesgos que pueden surgir en el desarrollo.

- La planificación temporal de tareas del punto 6 de la presente PEC, establece plazos razonables para el desarrollo de cada ítem en base a la complejidad del mismo, la disponibilidad del autor, los plazos impuestos por el plan docente, etc.
- Más allá del profesor y la directora del TFM, no hay dependencia de terceros que puedan interferir en el normal desarrollo de las tareas planificadas.
- Los recursos empleados en el TFM están al alcance del autor en todo momento, a excepción de los documentos publicados por terceros que tengan derechos de autor muy restrictivos, no permitiendo su utilización en modo alguno. Esta situación debe ser considerada excepcional. Los recursos software se apoyan en licencias GPL2+ free/libre tool, LGPLv3,..., según el caso.
- Dado que no se precisa de aportación económica para ninguna de las tareas planificadas en el TFM, este hecho no supone un posible impedimento a la viabilidad.
- Entre la información que se pretende tratar no se encuentran datos personales que puedan requerir del consentimiento de sus titulares. Si excepcionalmente fuese preciso el acceso a información personal, previamente se llevaría a cabo un proceso de anonimización que evitase considerar la normativa al efecto.
- Es posible que la limitada experiencia del autor en el campo de la ingeniería social -motivo por el cual apuesta por este trabajo-, y el bajo nivel de concreción respecto



del producto a obtener en el que incurre la definición del TFM, conlleve un riesgo para el mismo. En tal caso, esta PEC debería ser útil para detectar las desviaciones de los objetivos planteados respecto de los esperados.

## 1.7 Estado del arte

A continuación se expone el inventario de fuentes de información que serán consideradas durante la elaboración de la memoria del presente trabajo fin de master. De cada fuente se describe la organización de la que procede, el título de la publicación/software, la categoría o tipo del mismo a criterio del que escribe, la fecha aproximada desde la que está disponible y un breve resumen de su contenido. Esta colección de información permite esbozar una idea de los trabajos más significativos y recientes en el área de la ingeniería social, no pretendiendo ser exhaustiva, pero si heterogénea, actual y representativa.

FUENTE	DOCUMENTO/URL	TIPO <sup>6</sup>	FECHA	RESUMEN
UOC	Asignatura "Vulnerabilidades de Seguridad", módulo 5 "Ingeniería social". PID_00178969	Guía	Septiembre 2011	El proceso de la ingeniería social, estrategias y técnicas, casos prácticos, casos especiales, análisis, prevención y reflexiones. 46 páginas.
ProQuest	Social engineering Winder, Davey. PC Pro; London Iss. 277, (Nov 2017): 99.	Artículo	Noviembre 2017	Definición, impacto, tipos de ataque, empleados, solución, concienciación, trucos para practicar. 4 páginas.
ProQuest	A test of interventions for security threats from social engineering Workman, Michael. Information Management & Computer Security ; Bradford Vol. 16, Iss. 5, (2008): 463-483.	Estudio	2008	Investigación empírica para localizar los factores más relevantes de la ingeniería social y los protocolos de actuación recomendables. 27 páginas.
Facultad de Ingeniería USBMed	Análisis y desarrollo de estrategias para la prevención del uso de la Ingeniería Social en la Sociedad de la Informaicón. Ing. USBMed, Vol. 4, No. 2, Julio-Diciembre 2013	Artículo (Reflexión)	De Julio a Diciembre 2013	Introducción, fases del ataque a un sistema, Kevin Mitnick, datos, el ingeniero social, encuesta a víctimas y recomendaciones. 7 páginas.
digitalguardian.com	Social Engineering Attacks: Common Techniques & How to Prevent an Attack	Artículo	Enero 2018	28 expertos en seguridad de la información discuten cómo prevenir los ataques de ingeniería social más comunes. 25 páginas.
CrossMark	Fighting against phishing attacks: state of the art and	Estudio	De Enero a Marzo de	Phishing, historial y motivación. Taxonomía de ataques y soluciones.

6 [Guía|Estudio|Artículo|Juego|Varios]

FUENTE	DOCUMENTO/URL	TIPO	FECHA	RESUMEN
	future challenges Neural Comput & Applic (2017) 28:3629–3654 DOI 10.1007/s00521-016- 2275-y		2016	Problemas tipo frente a ataques y su aplicación al IoT. Herramientas y datos empleados por los investigadores. 26 páginas.
CrossMark	Social Engineering Framework: Understanding the Deception Approach to Human Element of Security IJCSI International Journal of Computer Science Issues, Volume 14, Issue 2, March 2017 ISSN (Print): 1694-0814   ISSN (Online): 1694-0784 www.IJCSI.org https://doi.org/ 10.20943/01201702.816	Estudio	Marzo 2017	Investigación que muestra la existencia de patrones correlacionables, organizados de una manera lógica y estructurada. 10 páginas.
Incibe	Dossier: Desarrollar cultura en ciberseguridad.	Guía	Noviembre 2016	Introducción, desarrollo de acciones formativas y de sensibilización, redacción del marco normativo interno y supervisión de buenas prácticas. 15 páginas. Incorpora recursos adicionales: infografías, videos, documentación de soporte y enlaces a recursos relacionados.
Incibe	Juego de rol. ¿Estás preparado para ser atacado?	Juego de rol	Diciembre 2016	Situaciones o retos de seguridad que se dan a menudo en la empresa, para que sirvan de entrenamiento.
Incibe	Kit de concienciación	Varios	Enero 2017	Incorpora múltiples recursos gráficos, elementos interactivos y una programación detallada.
Incibe	Blog	Varios	2016	Toma conciencia para evitar los ataques de ingeniería social La ingeniería social en la empresa: aprovechando la naturaleza humana Infografía: los 6 pasos de los ciberdelincuentes Como combatir la ingeniería social Phishing: Historias reales
OSI	Social Lab, el wargame de la ingeniería social	Juego online	2012	Social Lab es un wargame de ingeniería social. Se trata de un juego en el que hay que ir pasando distintas pruebas y cuyo principal objetivo es que el jugador aprenda algunas de las técnicas que emplean los «hackers» para llegar hasta los usuarios en una red social.

FUENTE	DOCUMENTO/URL	TIPO	FECHA	RESUMEN
Isaca	Como auditar el elemento humano y evaluar el riesgo de seguridad de su organización	Artículo	2016	Análisis de riesgos centrado en humanos, correlación con eventos o incidentes de seguridad detectados automáticamente o notificados, planificación personalizada de formación teórica y práctica. Todo ello en un proceso de mejora continua. 7 páginas.
Isaca	The Underestimated Social Engineering Threat in IT Security Governance and Management		2015	El factor humano como una parte necesaria de la seguridad de la información. Formas de evaluar el factor humano. Situación de riesgo actual. Formas de mitigar el riesgo. La estrategia de gestión del riesgo de ingeniería social.
Isaca	Detección de phishing y pérdida computacional modelo híbrido: Un enfoque de aprendizaje automático	Artículo	2017	Modelo híbrido propuesto para la detección de Phishing y la pérdida computacional. Las técnicas de aprendizaje automático. Algoritmo Bagger para árbol de decisión. Metodología para el clasificador híbrido basado en CART. Cálculo de pérdidas para empresas después de un ataque de phishing. Estrategias Mitigación del Riesgo. 9 páginas.
Enisa	ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends	Estudio	Enero 2017	Evaluación del panorama europeo en ciberseguridad en 2017, mostrando comparativas de amenazas con respecto a 2016. Además de caracterizar el top 15 de las ciberamenazas, se evalúan los vectores de ataque entre los que se encuentra el factor humano. 114 páginas.
Enisa	Cyber Security Culture in organisations	Guía	Noviembre 2017	Detalla como construir un caso de negocio que implemente un programa de ciberseguridad. Enumera elementos y recursos para el éxito del programa. Describe buenas prácticas para el despliegue de las iniciativas. Trata otros aspectos como el legal y la importancia del factor humano en la ciberseguridad.
Nist	NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment	Guía	Septiembre 2008	Este documento es una guía de los aspectos técnicos básicos de la realización de evaluaciones de seguridad de la información. Presenta técnicas y métodos de prueba y examen técnicos que una organización podría usar como parte de una evaluación, y ofrece

FUENTE	DOCUMENTO/URL	TIPO	FECHA	RESUMEN
				información a los evaluadores sobre su ejecución y el impacto potencial que pueden tener en los sistemas y redes. Entre su contenido se encuentra un apartado que versa sobre las técnicas de validación de vulnerabilidades objetivo como la ingeniería social. 80 páginas.
Sans	Methods for Understanding and Reducing Social Engineering Attacks		Abril 2016	Descripción de la ingeniería social. Ejemplos reales de ataques de ingeniería social exitosos. Métodos usados por los ingenieros sociales para conseguir acceso a la información sensible. La psicología de la ingeniería social. La solución. 34 página.
Mc Graw Hill Education	People-Centric Security: Transforming Your Enterprise Security Culture	Libro	Agosto 2015	Entendiendo, midiendo y transformando tu cultura de seguridad. 416 páginas.
IAI	Ciberseguridad: Una guía de supervisión	Guía	Octubre 2016	Abarca las principales cuestiones relativas a la ciberseguridad y un completo análisis de buenas prácticas de Auditoría Interna para la evaluación y revisión de los controles en esta materia. También se incluyen los 20 Controles Críticos de Seguridad que todas las organizaciones deben implementar y cuál es el papel de Auditoría Interna en la revisión de cada uno de ellos. 52 páginas
Minsiterio del Interior.	Portal estadístico de criminalidad	Estudio	2016	Infracciones penales relacionadas con la cibercriminalidad.
Cybersecurity Insiders & CA technologies	Insider Threat Report 2018	Estudio	Noviembre 2017	Se trata de un informe de amenazas internas resultante es una investigación exhaustiva sobre el tema hasta la fecha, que revela cómo los profesionales de TI y seguridad están tratando con personas con información privilegiada y cómo las organizaciones se están preparando para proteger mejor sus datos críticos e infraestructura de TI. 35 páginas.
Europol EC3	Internet Organised Crime Threat Assessment (IOCTA) 2017	Estudio	Septiembre 2017	Entre su contenido destaca el tratamiento del crimen dependiente del ciberespacio, la convergencia entre el terrorismo y el ciberespacio y los factores criminales

FUENTE	DOCUMENTO/URL	TIPO	FECHA	RESUMEN
				transversales como la ingeniería social. También muestra una distribución geográfica del cibercrimen. 80 páginas
Verizon	2017 Data Breach Investigations Report	Estudio	Abril 2017	Este informe está compuesto por brechas de datos e incidentes de seguridad del mundo real, ya sea investigados por Verizon o proporcionados por una de sus fuentes de datos más destacadas. Las declaraciones están basadas en datos, ya sea por el conjunto de incidentes que es la base de esta publicación o por conjuntos de datos no relacionados con incidentes aportados por varios proveedores de seguridad. No se usan encuestas. 76 páginas
Trust Sec	SET User Manual Made for SET 6.0	Guia	Mayo 2014	Manual de usuario de la herramienta informática denominada Software Engineering Toolkit.
B.O.E. D.O.U.E. EUR-Lex	Normativa legal	Norma	2018	Código penal. Reglamento General de Protección de Datos. Protección civil del honor, la intimidad y la propia imagen. Etc.
ISO	Related to ISO 27001:2013	Norma Estándar	2013	A.7 Human resource security Seis controles que son aplicados antes, <u>durante</u> o después de ocupar el puesto de trabajo.

## 1.8 Breve descripción de los otros capítulos de la memoria

Los contenidos que se presentan a partir del siguiente capítulo se estructuran en grandes bloques que pretenden satisfacer los objetivos enfocados a reflejar el trabajo de investigación y documentación realizado entorno a la ingeniería social. Básicamente el resultado de este TFM podría definirse como una detallada manifestación del estado del arte entorno a esta amenaza de seguridad para las organizaciones, pretendidamente actualizado y fundamentado en una ingente cantidad de fuentes autorizadas de información.

<b>Objetivo 1:</b>	Recopilar material de acceso público de distintas fuentes de información de confianza, para construir el marco de trabajo de soporte al resto de los objetivos.
<b>Contenidos:</b>	N/A
<b>Objetivo 2:</b>	Documentar, textual y gráficamente cuando sea posible, los conceptos, métodos, estrategias y roles que intervienen en los procesos de ingeniería social.

<b>Contenidos:</b>	Capítulo 2. Descripción de la ingeniería social. Capítulo 3. Etapas de la ingeniería social. Capítulo 4. El proceso de la ingeniería social. En algunos aspectos se trata de contenidos transversales a distintos capítulos.
<b>Objetivo 3:</b>	Ilustrar los principales tipos de información de interés para el ingeniero social, poniendo el foco en los beneficios que pueden proporcionar.
<b>Contenidos:</b>	Capítulo 5. Descubrimiento del tipo de información que puede llegar a obtenerse. Capítulo 6. Formas de utilización de la información para obtener beneficios.
<b>Objetivo 4:</b>	Exponer las repercusiones legales derivadas del empleo no autorizado de la ingeniería social.
<b>Contenidos:</b>	Capítulo 7. Análisis legal de la ingeniería social en el marco de la ciberdelincuencia. Capítulo 8. La ingeniería social en números.
<b>Objetivo 5:</b>	Poner en valor el factor humano como elemento a considerar en la política de seguridad de la información de una organización.
<b>Contenidos:</b>	Capítulo 2. Descripción de la ingeniería social. Capítulo 8. La ingeniería social en números. Capítulo 9. Estrategias de gestión de riesgos.
<b>Objetivo 6:</b>	Enumerar las mejores prácticas y recomendaciones para mitigar el riesgo de exposición a la ingeniería social, ponderando el uso de diagramas de ataque de ingeniería social (DAIS).
<b>Contenidos:</b>	Capítulo 10. Pautas para combatir la ingeniería social.
<b>Objetivo 7:</b>	Desarrollar los ítems de un plan de cultura de ciberseguridad, acotando el alcance al contexto de la ingeniería social, y trabajando el conocimiento, las creencias, las percepciones, las actitudes, las suposiciones, las normas y los valores de las personas.
<b>Contenidos:</b>	Capítulo 10. Pautas para combatir la ingeniería social.
<b>Objetivo 8:</b>	Diseñar e implementar objetos de aprendizaje con herramientas abiertas que faciliten la implantación de los ítems del plan de cultura de ciberseguridad.
<b>Contenidos:</b>	Material didáctico en formato SCORM.

## 2 Descripción de ingeniería social.

Este capítulo es fundamental para la comprensión general del tema sobre el que versa este trabajo. Está dedicado a estructurar información de diversas fuentes, haciendo un recorrido que comienza por acotar la definición de ingeniería social en el marco de la ciberseguridad. Continúa por el análisis de las características del ser humano tipificadas como vulnerabilidades a los ojos de un ingeniero social. Avanza hacia las técnicas de ataque orientadas a explotar tales vulnerabilidades, ampliando algunas de ellas a través de anexos. Da un paso más exponiendo la ingeniería social como un proceso desde un punto de vista metodológico. Y finalmente otorga un apartado al estudio de los roles que intervienen y sus características.

### 2.1 Definición y contexto

Hay varias teorías, conceptos y escuelas de pensamientos relacionados con la definición y caracterización de este tipo de ataque. A continuación exponemos algunas por orden cronológico:

- La ingeniería social es la intención maliciosa de los ciberatacantes que intentan comprometer ilegalmente los activos de una organización mediante el uso de las relaciones con las personas (Dolan, 2004).
- Ingeniería social es el término para usar el engaño humano como medio para el robo de información (Hermansson et.al., 2005).
- Ingeniería social es una descripción de las técnicas que utilizan la persuasión y / o el engaño para obtener acceso a los sistemas de información (McClure, 2005).
- Los ataques de ingeniería social implican el uso de tácticas engañosas o manipuladoras en un individuo para obtener un resultado orientado a obtener acceso no autorizado a activos de información (Lineberry, 2007).
- La ingeniería social no depende de una pieza defectuosa en un equipo de alta tecnología para montar el ataque; más bien, usa un ataque experto en la psique del oponente (Long, 2008).
- Los ataques de ingeniería social tienen el objetivo de recopilar una cierta cantidad de datos para usarlos más tarde en un ataque técnico (Evans, 2009).
- La ingeniería social es el arte de explotar el eslabón más débil de los sistemas de seguridad de la información: las personas que los utilizan (Huber, 2009).
- La ingeniería social se refiere a varias técnicas que se utilizan para obtener información con el fin de eludir los sistemas de seguridad, a través de la explotación de la vulnerabilidad humana (Bezuidenhout et.al., 2010).
- El objetivo de los ataques de ingeniería social es obtener acceso directo, ya sea físico o digital, al sistema de información o información de una organización (Foozy, 2011).

Según el glosario<sup>7</sup> de términos publicado en la web de ENISA, *la ingeniería social se refiere a todas las técnicas dirigidas a hablar con un objetivo para que revele información específica o realice una acción específica por razones ilegítimas.*

Sergi Robles Martínez y Sergio Castillo Pérez, en el módulo dedicado a la ingeniería social (PID\_00178969) dentro de la asignatura "Vulnerabilidades de Seguridad", ofrecen la siguiente definición: *en el contexto de la seguridad informática, llamaremos ingeniería social a la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento la manipulación psicológica de personas. Así, un sistema vulnerable a ataques de ingeniería social será aquel susceptible a ser atacado mediante estas técnicas.*

Destacar que la norma ISO 27032, publicada en 2012 y dedicada a la ciberseguridad, introduce como complemento a los controles ya definidos en la ISO 27001, orientaciones técnicas para abordar riesgos comunes de ciberseguridad entre los que se incluye los ataques de ingeniería social. En la figura de la derecha se puede observar como el capítulo 12.5 refleja el comentario anterior, ofreciendo en primer lugar una introducción, continuando con las políticas, para adentrarse en tercer lugar en los métodos y procesos (categorización y clasificación de la información, concienciación y formación, prueba/evaluación), en cuarto lugar trata los aspectos relacionados con las personas y la organización y finalmente aborda los temas técnicos.

Ahora que conocemos en qué consiste esta técnica, y como parte de su caracterización, cabe destacar algunas de las razones que conducirían a un atacante a utilizarla. En primer lugar, es fácil de desplegar sin tener que emplear mucho tiempo en la adquisición de competencias, destrezas y capacidades. En segundo lugar, es relativamente eficiente en coste porque no requiere muchos recursos en la mayoría de los casos. En tercer lugar, las estadísticas muestran un tasa alta de éxito en comparación con otras técnicas de ataque. La cuarta razón considera que el riesgo de ser atrapado por la autoridad es relativamente bajo porque "el control" está en poder de la víctima y no del ingeniero social. Y por último, no debemos olvidar que las variantes del tipo de ingeniería

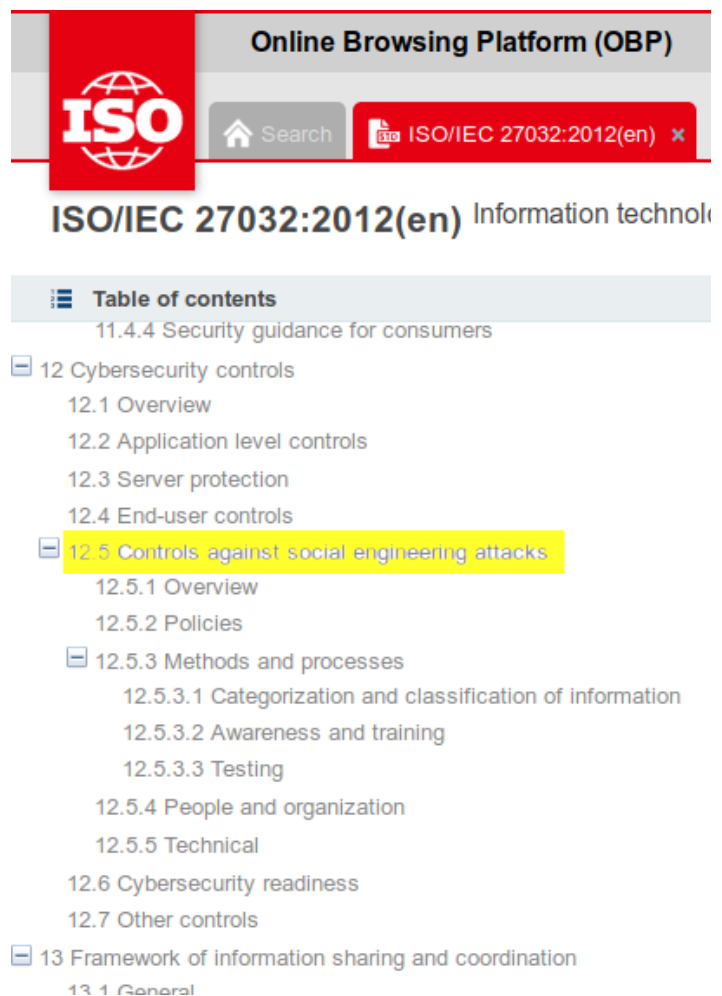


Ilustración 4: ISO 27032:2012 - Controles frente a ataques de Ingeniería Social

<sup>7</sup> <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering>

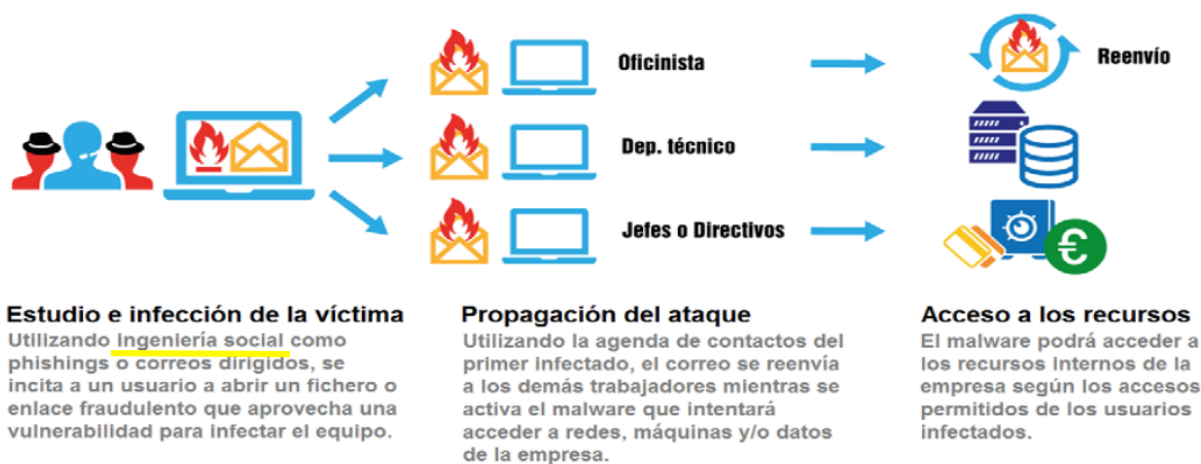


social son ilimitadas, donde todo el mundo puede usar su creatividad e innovación para alcanzar un escenario eficaz.

Nada mejor para terminar de entender el concepto de ingeniería social que ponerlo en contexto en el marco de una amenaza para la seguridad de la información. Si analizamos el modelo<sup>8</sup> que implementa una Amenaza Persistente Avanzada (APT): estudio de la víctima, infección y propagación, observamos como en el primer paso entra en juego la ingeniería social. Al tratarse de un ataque específico dirigido, el atacante debe conocer en profundidad su objetivo, desde la configuración de los sistemas hasta sus políticas de seguridad. Esto le permite elegir el punto más débil en la cadena para atacar.

Algunos ataques muy sofisticados técnicamente han comenzado con un simple engaño a uno de los usuarios de la red. La infección comienza con una ejecución. Persuadir a un usuario de que lance un ejecutable, si el sistema no cuenta con las medidas de seguridad necesarias, puede ser más sencillo que cualquier otro método.

**Ilustración 1: Proceso de ataque ATP**



Fuente: INTECO

Ilustración 5: INTECO. Proceso de ataque ATP

Otro modelado de APT, en este caso llevado a cabo por la empresa CEFRIEL<sup>9</sup>, pone de manifiesto la frecuencia con la que esta amenaza comienza mediante un ataque de ingeniería social. Primero consultando información en internet y las redes sociales (OSINT), luego contextualizando el mensaje dirigido a el/los objetivo/s (Target selection) y en tercer lugar remitiendo mensajes de correo electrónico a la víctimas potenciales (SE attack).

<sup>8</sup> INTECO (ahora INCIBE). Cuaderno de notas del observatorio: ¿QUÉ SON LAS APTs?

<sup>9</sup> <https://www.cefriel.com>

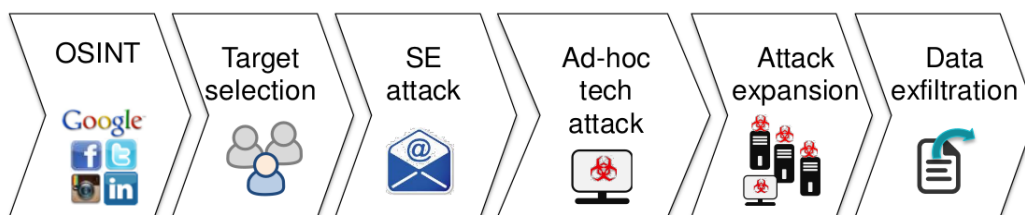


Ilustración 6: CEFRIEL. Proceso de ataque ATP

Para finalizar este apartado dedicado a la definición de la ingeniería social, saliendo del contexto de la ciberseguridad para entrar ligeramente en el terreno psicosocial, podemos afirmar que es un hecho que casi todos los humanos serán víctimas de alguna forma de ingeniería social durante su vida, sin que ello deba conducir a una violación masiva de datos. Aunque la mayoría de las personas creen que son inmunes a tales trucos porque son de alguna manera más inteligentes o más conscientes que otros, podría ser tan simple como sucumbir a la sonrisa o el cumplido de un niño para permitirle jugar un poco más. El cumplido puede haber sido sincero, pero si su propósito va más allá de hacer sentir mejor al destinatario del mismo, se trata de manipulación, de engaño, y por lo tanto de ingeniería social. Hay autores que afirman que cualquier forma de engaño para beneficio personal cae en la categoría de ingeniería social.

## 2.2 El elemento humano

Tras un sistema de información siempre hay personas, como los usuarios, los administradores, o el personal de desarrollo y mantenimiento. Si incluimos a las personas, "wetware" para algunos autores, como parte integrante de estos sistemas de información, resulta que suele ser, con diferencia, el eslabón más débil de toda la cadena de seguridad.

El elemento humano debe ser considerado en su conjunto, tanto empleados contratados directamente por la organización como personal externo que actúa como prestador de servicio, voluntario, becario,... En el primer caso, la persona tiene un rol con acceso autorizado a cierta información y puede dar lugar a amenazas internas derivadas de situaciones de descontento y actuaciones imprudentes o desalineadas con los procedimientos definidos. En el segundo caso, el desconocimiento, la inconsciencia o la falta de percepción de riesgo, se pueden ver impulsados por un ataque de ingeniería social.

Es fundamental ampliar la gobernanza de la seguridad de la información para incluir el factor humano en el análisis y evaluación del riesgo corporativo. Para hacer esto de una manera efectiva, hemos de comprender y medir el riesgo real antes de proponer medidas y así personalizadas para mitigarlo adecuadamente.

A continuación vamos a enumerar una serie de características humanas susceptibles de ser explotadas mediante ingeniería social, clasificadas atendiendo a su naturaleza: innatas/congénitas y aprendidas/adquiridas.

### 2.2.1 Características humanas Innatas

Comprender las tendencias que posee una persona requiere tiempo y esfuerzo, es necesario observarlas y conocerlas para hallar sus debilidades y evitar así que se conviertan en oportunidades para el ingeniero social.

- La confianza en los demás:

El ser humano muestra una disposición natural para aceptar y confiar en la palabra de alguien, lo que lo hace vulnerable y al tiempo puede anular cualquier esfuerzo previo realizado para proteger la información. Aunque la ingeniería social puede ser compleja e inteligente, por lo general es simple y se ve favorecida por circunstancias como la presión emocional (enfado, camaradería, desesperación...).

- Similitud de pensamiento:

Las personas generalmente piensan que los otros comparten sus mismos sentimientos e ideas, lo que se denomina el efecto del falso consenso. Tener elementos en común, como por ejemplo aficiones, gustos musicales o artísticos, o incluso compartir los mismos problemas, crean un fuerte incentivo para tratar a alguien de una manera especial, más favorable.

El ingeniero social puede utilizar estas creencias para manipular a la víctima y conseguir que realice alguna acción. O bien comentar casualmente que se ha nacido en la misma ciudad para pedir posteriormente una información no pública.

- El deseo por lo excaso:

Cuando hay escasez de un bien o servicio en el que se podría estar interesado, o su disponibilidad es solo por un período de tiempo limitado, las personas tienden a quererlo más. Saber que esta disponibilidad limitada puede crear competencia entre otras personas para su adquisición incrementa más aún el deseo de adquirirlo.

Un ejemplo de fomento del deseo por un ingeniero social podría ser anunciar que solo quedan tres unidades de pendrive para las primeras personas que contesten una encuesta.

- La reciprocidad:

Cuando alguien da algo, o promete que lo hará, las personas sienten una fuerte tendencia a devolver algo a cambio, incluso si lo que se ha recibido nunca fue solicitado. Esta regla básica de la interacción humana es innata a las personas y funciona aun cuando el coste de lo dado y recibido es muy diferente.

Un ejemplo de recurso a la reciprocidad es desconectar inadvertidamente a alguien el cable de acceso a la red de un ordenador simulando una avería para solucionar el problema después y pedir un favor a cambio.

- La consistencia:

Se trata de una conducta de la personalidad que mueve al ser humano a mantener cierta coherencia consigo mismo, a no lesionarse, a no contradecir sus acciones pasadas. Incluso aunque en la situación actual, mantener esta coherencia ya no tenga sentido, las personas tenderán a actuar del mismo modo para evitar el sentimiento de desconfianza de los demás.

Por tanto, se puede predecir la reacción de una persona a partir de sus acciones pasadas.

- Otras características:

El ego/autoestima, la generosidad, la mentalidad abierta, la responsabilidad, la extraversión, la aceptabilidad, el neuroticismo,... Existen muchos caracteres de la personalidad que podrían ser explotados por un ingeniero social, bajo la premisa de la observación y estudio de la persona objetivo, la víctima.

## 2.2.2 Características humanas aprendidas

Al contrario que sucede con las características innatas, las aprendidas son aplicables a todas las personas como norma general, no requiriendo mucho esfuerzo por parte del ingeniero social para aprovecharse de ellas.

- La confiabilidad

Como parte de una sociedad civilizada, la mayoría de las personas se esfuerzan por ser consideradas dignas de confianza, y al hacerlo, esperan que los demás actúen igual. Es esta presunción de honestidad y confiabilidad sobre un individuo desconocido lo que permite a un ingeniero social actuar como tal, por ejemplo para acercarse a un empleado con la oculta intención de acceder sin autorización a una oficina.

Está demostrado que incluso después de un proceso de formación específico dirigido a mitigar los ataques de ingeniería social, persisten los casos de éxito por el fuerte arraigo de esta característica en el ser humano.

Más adelante veremos como mediante determinadas técnicas (pretexto) es posible favorecer el grado de confianza que una persona tiene depositado en otra, pero el simple contacto continuado en el tiempo es suficiente para ello.

- La lealtad

La víctima de ataque de ingeniería social entiende que facilitar el acceso a las instalaciones de la organización, pe. a un proveedor, es un comportamiento leal, una muestra de fidelidad y compromiso. Nada más lejos de la realidad cuando su actuación, contraria a la formación recibida, está más próxima a la traición, involuntaria, pero traición al fin y al cabo.

- La demostración de utilidad

La inclinación natural del ser humano a ser útil a los demás suele ser una de las características más atacadas por los ingenieros sociales. Esta forma de ser no sólo persigue brindar ayuda a quien lo necesita sino que además se obtiene como recompensa una sensación de bienestar, de humanidad, por haber hecho lo correcto. Este impulso no controlado en un empleado puede dar lugar a que incumpla las reglas establecidas y difundidas en los procesos de capacitación. Un caso típico de ataque de un ingeniero social que aprovecha esta vulnerabilidad, sería esperar en la puerta de la oficina hasta la llegada de un empleado autorizado y hacerse pasar por un nuevo empleado que ha olvidado su tarjeta de acceso.

- La obediencia

Los buenos empleados no suelen discutir la voluntad de sus superiores, son obedientes y acatan sus decisiones. Parece claro que esta característica del ser humano no es innata puesto que lo intuitivo es hacer siempre lo que se quiere, lo que se desea y no lo que dicen los demás.

Los padres, la familia, el colegio e incluso la organización para la que se trabaja, se encargan de inculcar estas características en las personas, y una vez aprehendida, se transforma en instinto. El miedo a un castigo en casa, a un parte docente en el colegio o a no perder el puesto de trabajo, hace aflorar este instinto.

Si un ingeniero social, durante la jornada laboral, se presente ante un empleado como alguien con autoridad, bien por el puesto que dice ocupar (pe. policía) o bien por tenerla delegada por otro responsable conocido de la organización (pe. director), la víctima hará uso de su instinto de obediencia dando legitimidad al atacante.

- Otros factores aprendidos:

Son aquellos que se asumen como propios en la medida en que se observan en el comportamiento de las personas del entorno, bien dentro de una comunidad religiosa, en el marco de una cultura común, como consecuencia de experiencias compartidas o incluso personales, etc.

### 2.2.3 La persuasión

Expuestas estas "debilidades" humanas propias de las víctimas de ingeniería social, cabe realizar una breve mención en otras características del ser humano, la persuasión. En este caso, se trata de una herramienta en favor del ingeniero social empleada para explotar tales debilidades. Según el diccionario de la lengua española, persuadir se define como la acción de inducir, mover, obligar a alguien con razones a creer o hacer algo. Por tanto, persuadir no es más que una forma de influir en los demás para lograr que deseen hacer algo, que reaccionen de una determinada manera, que piensen o creen en una idea. El arte de la persuasión está en construir la relación atacante-víctima, principalmente mediante muestras de empatía, para obtener confianza. Los profesionales del mundo del marketing y ventas, los comerciales, son muy buenos en el uso de esta técnica.

Analizando el modo de pensar de las personas, como influyen unas sobre otras y como se relacionan entre sí desde la perspectiva de la psicología social, se observan dos formas principales de persuadir:

- Mediante argumentos sistémicos y lógicos para estimular una respuesta favorable, induciendo a la persona a pensar detenidamente y dar un consentimiento.
- Y lateralmente, mediante indicaciones periféricas y atajos mentales para eludir el razonamiento lógico y la contra-argumentación. Se persigue provocar la aceptación, sin pensar en profundidad sobre el tema. Por ejemplo, a través de mensajes o acciones en el inicio de la interacción que provoquen reacciones emocionales, como excitación o miedo.

La autoridad/obediencia, la parquedad, la similitud, la reciprocidad, el compromiso, la consistencia y la prueba social, son factores humanos explotados por la persuasión periférica.

La manipulación psicológica antes referida, básicamente requiere capacidad de convicción del atacante, persuasión, con objeto de hacer creer a la víctima lo rentable y provechosa que será su participación. Para ello, los ingenieros sociales emplean técnicas de engaño como son: enmascarar, reempaquetar, deslumbrar, imitar, inventar y dibujar.

## 2.3 Categorías y técnicas

### 2.3.1 Categorías

La Ingeniería Social se divide principalmente en dos categorías diferentes, a saber, el engaño técnico o basado en la computadora y el engaño basado en la interacción humana (Hermansson et al., 2005):

- En el primer caso, el Ingeniero Social, como su nombre indica, confía en la tecnología para engañar a la víctima del ataque y que ésta proporcione la información necesaria para cumplir con el propósito del ataque. Ejemplos: suplantación de identidad (dirigida o no), cebo,...
- Mientras que el otro enfoque de Ingeniería Social se basa simplemente en el engaño a través de la interacción humana. Ejemplos: Pretextos, rebufo o quid pro quo.

En cambio, algunos expertos e investigadores a menudo emplean otras categorías menos generalistas, clasificando los tipos de ingeniería social según sus modos o técnicas de ataque, como por ejemplo:

- Vishing, buceo en contenedor, ingeniería social en línea, persuasión e ingeniería social inversa (Granger, 2001).
- Ataque técnico, ataque del ego, ataque de simpatía e intimidación (Turner, 2005).
- Suplantación, confianza, difusión, sobrecarga, deber moral, reciprocidad, urgencia y enfoque directo (Redmon, 2006).

- No técnicos, que son engaños, pretextos, buceo en contenedor, espionaje, voz autorizada, personal de soporte y experto técnico; y técnicos que son ventanas emergentes de phishing, vishing, popup, software interesante y centros de spam (Thapar, 2007).
- Pretextos, phishing, vishing (phishing telefónico), caballo de Troya, hostigamiento, quid pro quo y ataque híbrido (Prince, 2009).
- Personificación, autorización de terceros, en persona, inmersión en el basurero, ventanas emergentes, adjuntos de correo electrónico y sitios web (Foozy et.al., 2011).

### 2.3.2 Técnicas

- Precarga (Preloading):

Consiste en plantar ideas o pensamientos específicos a individuos de una manera que no sea obvia o dominante. Una vez que las ideas son aceptadas, los ingenieros sociales pueden utilizarlas más adelante para comenzar a iniciar un ataque. Un ejemplo podría ser el establecimiento de una buena relación durante una conversación, o mediante el consenso de algunos principios universalmente asentados.

- Pretextos (Pretexting):

Esta técnica es el uso de un pretexto, una falsa justificación, un escenario inventado para respaldar una serie de acciones específicas, orientadas a ganarse la confianza de la víctima, a la que se pretende engañar para que revele información personal o para que actúe de forma poco convencional.

Ejemplo 1: El atacante afirma que trabaja para soporte de TI y solicita la contraseña del objetivo para fines de mantenimiento.

Ejemplo 2: Un atacante se hace pasar por auditor externo de servicios de TI con la intención de manipular al personal de seguridad física de la empresa para que le permita entrar al edificio.

Un buen ingeniero social tiene que interpretar con seriedad su papel, como si fuera el verdadero personaje al que suplanta. Convencer a la gente es la finalidad de esta técnica para ganar su confianza.

En la organización deben existir procesos adecuados de identificación y autenticación, políticas y capacitación para eludir dichos ataques.

- Cebo (Baiting):

El cebo consiste en atraer a la víctima proporcionándole acceso fácil a algo que desea para que realice una tarea específica. Baiting es como el "Caballo de Troya" del mundo real que usa medios físicos y se basa en la curiosidad o la codicia de la víctima.

Ejemplo 1: ofrecer a los usuarios descargas gratuitas de música o películas, si entregan sus credenciales de inicio de sesión a un determinado sitio.

Ejemplo 2: abandonar cerca de la víctima una unidad flash USB infectada con un registrador de teclas (keylogger), con la etiqueta llamativa del tipo "Nóminas del personal" o "Mis fotos privadas".

Uno de estos ataques fue documentado por Steve Stasiukonis, VP y fundador de Secure Network Technologies, Inc., en 2006. Para evaluar la seguridad de un cliente financiero, Steve y su equipo infectaron docenas de USB con un virus troyano y los dispersaron por el aparcamiento de la organización. Muchos de los empleados del cliente financiero recogieron los USB y los conectaron a sus ordenadores, activando así un registrador de claves y otorgando acceso a Steve a una serie de credenciales de inicio de sesión de los empleados (Johansson, 2008).

Las políticas de seguridad de tipo *air gap* que bloquean el software y hardware no autorizados, frustrarán la mayoría de los intentos de cebo, aunque también se debe recordar al personal que no confíe en fuentes desconocidas.

- Quid pro quo:

Quid Pro Quo, es una expresión en latín que significa dar o recibir algo a cambio de algo. Así, en el mundo de la ingeniería social vendría a implicar una solicitud de información a cambio de una compensación, normalmente en forma de servicio. Ejemplos:

- ◆ El atacante pide la contraseña de la víctima afirmando ser un investigador haciendo un experimento, a cambio de dinero.
- ◆ El atacante, haciéndose pasar por personal de soporte TIC, promete llevar a cabo una actualización de software rápida si el empleado deshabilita su programa antivirus e instala un software (malware) en su ordenador.

Los ataques quid pro quo son relativamente fáciles de detectar dada la asimetría entre el valor de la información requerida y la compensación proporcionada. En estos casos, la mejor contramedida sigue siendo la integridad personal y la capacidad de la víctima para identificar, ignorar e informar sobre el incidente.

- Chupar rueda o ir a rebufo (Tailgating):

Ir a rebufo es el acto de seguir a una persona autorizada a un área o sistema restringido.

Un atacante, que busca la entrada a un área restringida protegida por un control de acceso electrónico desatendido, por ejemplo, mediante una tarjeta RFID, simplemente entra detrás de una persona que tiene acceso legítimo.

Ejemplo: el atacante, vestido como un empleado y portando una caja grande, convence a la víctima, un empleado autorizado que entra al mismo tiempo, para que usando su tarjeta RFID abra la puerta del centro de procesamiento de datos.

Por cortesía, la persona autorizada generalmente mantendrá la puerta abierta para el atacante, o bien éste último puede pedirle al empleado que la mantenga abierta para él. La persona autorizada puede no solicitar la identificación al atacante, e incluso puede



aceptar la afirmación del atacante de que ha olvidado o perdido la tarjeta identificativa. Otra posibilidad es que el atacante simule la acción de presentar un token de identidad.

El acceso a áreas no públicas debe controlarse mediante políticas de acceso y / o el uso de tecnologías de control de acceso, de modo que cuanto más sensible es el área, más estricta debe ser la combinación. La obligación de llevar una insignia, la presencia de un guardia y puertas antitailgating reales, como mantraps con control de acceso por RFID, deberían ser suficientes para disuadir a la mayoría de los atacantes.

- Suplantación de identidad (Phishing):

Podemos definir el phishing como la "*práctica de enviar correos electrónicos que parecen ser de fuentes confiables con el objetivo de influir o obtener información personal*" (Hadnagy & Fincher, 2015).

Los ataques de phishing son un medio para persuadir a las víctimas potenciales a que divulguen información confidencial, como credenciales, o detalles bancarios y de tarjetas de crédito. El ataque generalmente toma la forma de correo SPAM (spamming), sitios web maliciosos, mensajes de correo electrónico, mensajes instantáneos (SMishing) o incluso llamadas telefónicas (vishing), que parecen ser de una fuente legítima, como un banco o una red social.

Los atacantes a menudo usan la táctica del miedo o la solicitud urgente para atraer a los destinatarios a responder. Se caracterizan por contener mensajes poco o nada personalizados a modo de comunicación oficial, con un fichero adjunto preparado para la carga de malware o un enlace a un sitio web ilegítimo. Y el secreto de su éxito radica en enviar miles de mensajes al azar con la esperanza de engañar a algunas víctimas.

Esta técnica de ingeniería social será tratada con mayor detalle en el anexo I, dada su relevancia.

- Suplantación de identidad dirigida (Spear-phishing):

Se trata de un ataque de phishing refinado, principalmente por correo electrónico, a pequeña escala, centrado y dirigido a una persona u organización en particular con el objetivo de penetrar sus defensas. Su éxito se fundamenta en la investigación previa del objetivo, pe. en redes sociales, a fin de diseñar el mensaje de forma muy personal y lograr la plena confianza de la víctima.

Los pasos necesarios para enviar un ataque de este tipo suelen ser los siguientes: identificar direcciones de correo electrónico objetivo, evadir el antivirus, asegurar el tráfico de salida en el malware, preparar la historia para que el mensaje sea convincente, enviar los correos electrónicos y "cosechar" los datos resultantes (pe. las pulsaciones de teclado del keylogger).

- SMiShing:

Variante del phishing, con la diferencia de que se realiza utilizando mensajes de telefonía móvil de tipo SMS (short message service).

Aquí, el usuario recibe un SMS procedente de una supuesta entidad bancaria y en el que se le fuerza, mediante ingeniería social, a realizar una llamada a un número particular, o a enviar una respuesta al mensaje con datos solicitados.

Otra variante empleada por el atacante (smisher) es informar a la víctima de que si no hace clic en un enlace e introduce su información personal, se le cobrará un servicio supuestamente contratado.

- Vishing:

Se define como la práctica de obtener información o intentar influir en la acción a través del teléfono. El vishing es una variante del phishing, con la diferencia de que es realizado por voz utilizando el sistema de telefonía tradicional, o en algunas ocasiones el ingeniero social suele usar los servicios ofrecidos por la telefonía sobre IP (VoIP). Básicamente explota la voluntad de ayudar de las personas.

El ataque se basa en utilizar un sistema automático que realiza llamadas a números de teléfono. Cuando detecta que en el otro extremo hay una persona, se le comunica que hay algún tipo de problema con su tarjeta de crédito y se le convence para que proporcione ciertos datos, entre los que figura el número de su tarjeta, la fecha de caducidad y el código de seguridad.

Los atacantes pueden falsificar su número de teléfono saliente y aparentar ser una figura de autoridad, un técnico o un compañero de trabajo. Algunos atacantes pueden usar modificadores de voz para ocultar su identidad.

- Hoax:

Un bulo o noticia falsa es un intento de hacer creer a un grupo de personas que algo falso es real. El término en inglés «hoax», con el que también es conocido, se popularizó principalmente en castellano al referirse a engaños masivos por medios electrónicos, especialmente Internet. Se basa en crear una noticia o un rumor totalmente falso y transmitirlo por correo electrónico, mensajería instantánea o redes sociales, en el que se fuerza al destinatario al reenvío de éste para que se propague y distribuya en cadena. Su temática suele ser muy variada, virus informáticos, leyendas urbanas, cadenas de solidaridad, etc.

Detrás de los hoaxes pueden existir distintos intereses, tales como causar alarma social, confundir o modificar la opinión pública, desprestigiar una empresa o recogida de correos electrónicos para posteriormente utilizarlos como destinatarios de spam. De ahí la necesidad de explotar aspectos como son el engaño, la parquedad, la prueba social, la amabilidad o la empatía entre otros.

- Scareware:

Es una forma de malware que engaña y asusta al usuario final haciéndole creer que su computadora tiene una infección cuando en realidad su sistema podría estar perfectamente, más allá del propio scareware. Este supuesto producto de seguridad (antivirus, antispysware, antimallware, limpiador del registro,...) no suele ofrecer ningún beneficio real al usuario; por el contrario, normalmente dará como resultado desde un

adware a un virus o registrador de claves que se ejecute en la computadora del usuario final.

Una variante en cuanto al método utilizado para convencer a la víctima, es el malware basado en explotar el sentimiento de culpa y el miedo que pueden sentir usuarios al descargar software ilegal. En particular, una vez instalado muestra mensajes de advertencia indicando que se están violando las leyes del copyright y que se tiene identificada la dirección IP del usuario. Seguidamente, propone evitar un juicio realizando un pago como modo de solventar la situación.

El scareware explota el engaño, la persuasión, la coacción o el miedo mediante mensajes de alarma o de amenaza para forzar a la víctima a realizar un pago.

- Medios de comunicación social:

Los ciberdelincuentes, una vez estudiados los intereses de la víctima, tratan de engañarla creando perfiles falsos en las redes sociales, por ejemplo haciéndose pasar por un personaje famoso o un amigo. Si consiguen formar parte de su grupo social, el siguiente paso será intentar que haga clic en un enlace (vídeos, fotos,...) para instalar un software malicioso. Esto aumenta considerablemente la probabilidad de infección del ordenador de la víctima con malware que permita al atacante hacerse con el control de su ordenador.

Los atacantes también buscan en los perfiles sociales de las víctimas algunos tipos de información que se suelen utilizar como respuestas a preguntas de seguridad: nombre completo, fecha de nacimiento, nombre de mascota, ciudad natal, escuela y fecha de graduación, afiliaciones, intereses y pasatiempos, etc.

## 2.4 Roles que intervienen y sus características

### 2.4.1 El ingeniero social

Cualquier persona que aprovechándose de su astucia hace uso del engaño con el propósito de recopilar información, cometer fraude o acceder sin autorización al sistema informático encaja con la definición de ingeniero social. En palabras de Michael Hoeschele<sup>10</sup>, se trata de personas que usan tácticas para aprovechar la información a su alcance, el conocimiento que tienen de los procesos internos de una organización, la confianza o la predisposición a ayudar de los demás, el respeto por las figuras que representan a la autoridad, la tecnología o cualquier combinación de todo ello.

Según describe Christopher Hadnagy en su libro titulado "Ingeniería social: el arte de la piratería humana"<sup>11</sup>, los ingenieros sociales se pueden clasificar en función de sus actividades y de los objetivos que persiguen durante los diversos tipos de ataques previos que llevan a cabo. Algunos de los más reconocidos son:

---

<sup>10</sup> CERIAS Tech Report 2006-15. Detecting Social Engineering  
(<https://pdfs.semanticscholar.org/6a62/be4b227ffa6451d97555f84bdfb2e10cb4a.pdf>)

<sup>11</sup> <https://www.social-engineer.org/social-engineering/the-art-of-human-hacking/>

- (Black) Hackers / Crackers (piratas informáticos): individuos automotivados o profesionales contratados por personas u organizaciones para comprometer sistemas informáticos con el propósito último de obtener beneficios económicos, arruinar personas, comprometer la imagen de una compañía, alterar la agenda política u otros escenarios susceptibles de incumplir la ley.
- Probadores de penetración: personas altamente competentes que utilizan sus capacidades para examinar e identificar el nivel de seguridad dentro de un perímetro con el fin de encontrar vulnerabilidades para explotar.
- Espías: personas que han sido asignadas por una organización oficial para recopilar conocimiento o información especial sobre partes específicas en el marco de una operación de inteligencia.
- Ladrones de identidad: personas que roban la identidad de alguien para actuar como si fueran personas autorizadas.
- Empleados descontentos: personal de la organización que han sufrido malas experiencias en el pasado y que los predispone a vengarse de la institución.
- Estafadores: maestros en influir y engañar a las personas para que hagan todo lo que se les dice con el fin de obtener beneficios personales.

Otros tipos de ingenieros sociales menos conocidos podrían ser:

- Corredores de información: compañías a recopilar datos y proporcionar servicios de minería de datos para diversas organizaciones, gubernamentales, crediticias,... Estas empresas son un objetivo de alto valor para los ingenieros sociales, ya que contienen grandes cantidades de información que podrían utilizarse para potenciar sus actividades. ChoicePoint, Docusearch, LexisNexis, etc. son ejemplo de este tipo de compañías.
- Reclutadores de ejecutivos: profesionales encargados de hacer "selección" de personal para empresas clientes que van a la "caza" del candidato ideal. Usan diversos recursos o herramientas para encontrar a las personas adecuadas para los requisitos laborales que los empleadores establecen. Por lo general, recopilan datos y revisan los sitios en línea para encontrar estas coincidencias.
- Comerciales, gobiernos, gente normal y corriente,...

#### **2.4.2 El "empleador" o contratista**

La actuación del ingeniero social no siempre nace de sí mismo sino que en innumerables ocasiones procede del interés de contar con sus servicios por parte de un tercero: empresa competidora de la potencial víctima, gobierno con ciertos intereses (agencias de inteligencia, fuerzas de seguridad,...), particulares con cierto poder, asociaciones inmersas en conflictos sociales, organizaciones terroristas,...

### 2.4.3 La víctima

Genéricamente, acudiendo al diccionario de la Real Academia Española, se puede definir “víctima” como *“la persona que sufre un daño o perjuicio, que es provocado por una acción u omisión, ya sea por culpa de otra persona, o por fuerza mayor”*.

En el contexto de la ingeniería social podemos diferenciar dos escenarios. El primero es aquel donde se trata a la persona como un canal o un medio para conseguir un objetivo; aquí el ingeniero social usa a la persona para extraer información de un sistema o mejor aún, acceso al mismo. El segundo escenario es aquel donde el objetivo principal es la persona; lo que busca el ingeniero social es obtener información de ella o que ésta realice alguna acción con el fin de obtener dinero, números de tarjetas de crédito o débito, acceso a cuentas de correo electrónico, etc. Un claro ejemplo de este escenario es cuando la persona recibe un mensaje de texto informando de que es la ganadora de un gran premio en efectivo, pero para poder cobrarlo previamente debe adelantar cierta cantidad en concepto de tramites de gestión y papelería.

### 2.4.4 El responsable/s de seguridad

El rol del ingeniero social no tendría ningún mérito si su actividad no tuviese que burlar las medidas de seguridad implantadas en la organización bajo las recomendaciones y supervisión del responsable/s de seguridad de la información de la misma. Medidas que afectan al factor humano y que se centran principalmente en la concienciación y la formación del personal, pero que como veremos más adelante deben abarcar también otros procesos como la selección de personal, el despido o finalización del contrato, etc.

En el plano técnico-mecánico, estas medidas deben estar pensadas para contrarrestar actuaciones humanas voluntarias o no, promovidas por la influencia de un ingeniero social. Hablamos por ejemplo de controles de acceso basados en listas blancas que permitan impedir la ejecución de vínculos a urls no autorizadas, o de tornos de control de acceso físico que impidan la entrada a las instalaciones de personal no autorizado.

## 3 Etapas de la Ingeniería Social

A pesar de que la ingeniería social se puede realizar de muchas maneras diferentes, hay estudios que ha observado la existencia de un patrón común. La siguiente tabla muestra las etapas establecidas por distintos autores o modelos a lo largo del tiempo:

Gartner, 2001	Warren et.al., 2006	Modelo de Confianza y Ataque de Ingeniería Social	Engebretson, 2013 (hackers éticos)	Singh, 2013
Recopilación de información	Reconocimiento	Situación investigada	Reconocimiento	Investigación

Desarrollo de relaciones	de Recopilación de información	de	Objetivo investigado	Exploración	Gancho
Explotación de las relaciones	Acumulación de información	de	Confianza obtenida	Explotación	Juego
Ejecución para lograr el objetivo	Uso de información	la	Ataque lanzado	Mantenimiento del acceso	Salida

A continuación vamos a describir brevemente el modelo propuesto por Gartner en 2001 y tras él haremos lo mismo con un modelo más reciente propuesto por Richardus Eko en 2017.

### 3.1 Etapas Gartner-2001

Como ya hemos adelantado, existe una secuencia predecible de cuatro pasos para los ataques de ingeniería social, a los que se suele llamar ciclo de ataque: recopilación de información, establecimiento y desarrollo de relaciones, explotación de las relaciones y ejecución del ataque. Factores como la naturaleza del ataque o el objetivo perseguido, pueden hacer necesario repetir una o varias de estas etapas, hasta conseguir el resultado esperado. Se trata de un proceso de escalada de privilegios, ganándose la familiaridad dentro de la empresa objetivo, aprovechando las recomendaciones y la información obtenidas de interacciones previas.

#### 1. Recopilación de información

De esta fase depende la probabilidad de éxito de la mayoría de los ataques, así es que conviene dedicarle el tiempo suficiente. Hay muchas formas diferentes de acceder a la información de una organización o de un individuo. Algunas de estas opciones requieren habilidades técnicas, mientras que otras requieren habilidades psicosociales para el engaño. Algunas técnicas pueden usarse desde cualquier lugar con acceso a Internet, mientras otras solo pueden emplearse estando físicamente en una ubicación específica. Hay técnicas que no requieren más equipamiento que la voz, otras solo requieren un teléfono y otras requieren sofisticados dispositivos.

Parte de la información recopilada se usa para determinar el vector de ataque, las posibles contraseñas, identificar las posibles respuestas de varios individuos, refinar objetivos, familiarizarse con el objetivo hasta sentirse cómodos y formular pretextos sólidos.

#### 2. Establecer una relación y conseguir compenetración

Esta fase establece una relación de trabajo con el objetivo. Se trata de un punto crítico ya que la calidad de la relación construida por el atacante determina el nivel de cooperación de la víctima. Algunos ejemplos podrían ser:

- Apresurarse hacia la puerta con una gran sonrisa y manteniendo el contacto visual para que el objetivo mantenga la puerta abierta y permita el acceso al atacante.
- Conectar personalmente pe. con la recepcionista, bien contando historias vía telefónica o bien personalmente mostrando imágenes de familiares.
- Creando una relación en línea con el objetivo a través de un perfil falso en un sitio web de citas o en redes sociales.

### 3. Explotar la relación

Consiste en utilizar la información y las relaciones establecidas para infiltrarse activamente en el objetivo. El atacante se centra en mantener en la víctima la voluntad de colaboración que se construyó en la fase previa procurando no levantar sospechas. Una forma de explotación puede consistir en inducir a la víctima a divulgar información sin valor aparente o bien a otorgar algún tipo de acceso. Algunos ejemplos de explotación pueden ser las siguientes acciones de una víctima:

- Mantener la puerta abierta o permitir al atacante acceder dentro de las instalaciones.
- Divulgar del nombre de usuario y contraseña por teléfono.
- Presentar al atacantes a otros miembros de la compañía para su reconocimiento social.
- Insertar una unidad flash USB, cargada con malware, en un ordenador de la empresa.
- Abrir un archivo infectado adjunto a un mensaje de correo electrónico.
- Exponer secretos comerciales en una discusión con un supuesto compañero.

### 4. Ejecución

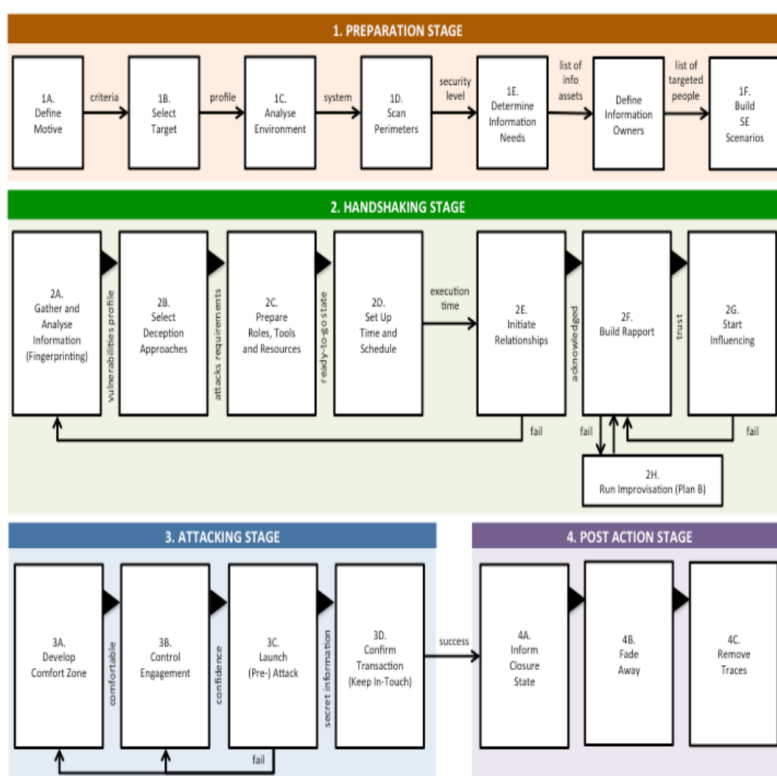
Esta fase es cuando se logra el objetivo final del ataque, máxime cuando además no se han levantado sospechas. El éxito de la ejecución será mayor si el ingeniero social logra dejar al objetivo con la sensación de que se hizo algo bueno, permitiendo así que continúen las posibles interacciones futuras. Por tanto es muy importante borrar las huellas digitales y garantizar que no quedan elementos o información para que el objetivo identifique el ataque o al atacante.

## 3.2 Etapas Richardus Eko 2017

Richardus Eko Indrajit, en su estudio titulado "Social Engineering Framework: Understanding the Deception"<sup>12</sup> y publicado en 2017 en el International Journal of Computer Science Issues, propone un marco propio basado en las anteriores clasificaciones que también divide en cuatro etapas: preparación, apretón de manos, ataque y post-acción.

---

<sup>12</sup> <https://doi.org/10.20943/01201702.816>. Reproducción parcial traducida con permiso del autor.



## 1. Etapa de preparación

Antes de que ocurra el ataque, un ingeniero social generalmente debe someterse a una serie de actividades, comúnmente siete:

- i. Motivo del ataque: beneficios económicos, ganancias políticas, desorden social, deterioro de imagen, interrupción cultural, ideología / desafío del valor, guerra y creación del terror.
- ii. Selección de objetivos: según el tipo y las características de las víctimas, se puede hacer una clasificación simple de la siguiente manera: Individuo, Grupo, Organización, Comunidad, Público, Híbrido y Aleatorio.
- iii. Análisis del entorno: realizar observaciones y análisis especiales para estudiar el perímetro de seguridad del objetivo, tanto interno como externo.
- iv. Escaneo perimetral: el sistema de información y la tecnología que lo soporta se construyen mediante el desarrollo de activos tangibles e intangibles que deberán escanearse física y lógicamente.
- v. Análisis de los requisitos de información: en función de los resultados del análisis del entorno y del escaneo perimetral, se define una lista de requisitos de información dependiendo del tipo de activo. Para recopilar esta información se debe preparar un conjunto de recursos, tanto técnicos como de otro tipo.
- vi. Determinación de los propietarios de activos: toda información tiene dueño, un individuo que tiene posesión formal de su existencia y es responsable de la misma. Resulta trascendente determinar el grado de alfabetización digital de estas personas.



- vii. Desarrollo de escenarios: los ingenieros sociales establecen su definición final de alcance, objetivos, costo y tiempo del plan de explotación. Deben asegurarse de que todos los requisitos hayan sido adquiridos o alcanzados.

## 2. Etapa de apretón de manos

Este es el proceso, estructurado en ocho fases, donde se establece el primer contacto entre el ingeniero social y su víctima objetivo:

- i. Toma de huellas digitales: es el proceso de recopilar información de los detalles del objetivo. El esfuerzo de la investigación debe centrarse en datos como: perfil, valor y análisis de comportamiento, sistema de concienciación sobre relaciones, posición social y grado de autoridad, posibles vulnerabilidades.
- ii. Modelo de engaño: phishing, pretextos, hostigamiento, suplantación, quid pro quo, implantación de malware, observación física, engaño, provocación, ingeniería social inversa y una combinación de las anteriores.
- iii. Preparación de recursos: todo intento de ataque requiere recursos, bien sean personas, bien procesos o bien tecnología.
- iv. Momento y planificación horaria: hay tres períodos de tiempo que es importante planificar: antes del día del ataque, el tiempo de despliegue del ataque y el período posterior al ataque.
- v. Iniciación de la relación: para no crear sospechas, la iniciación del primer contacto debe desarrollarse con normalidad de alguna de las siguientes formas: estructura oficial profesional, amigos y familia, proveedor-cliente, necesidades personales, requisitos técnicos (proporcionando sugerencias como solución) o roles pasivos (esperar ser contactado, empleo de ingeniería social inversa).
- vi. Generando compenetración: la compenetración es una relación estrecha y armoniosa en la que las personas o grupos en cuestión entienden los sentimientos o ideas de los demás y se comunican bien. Enfoques válidos podrían ser: empatía, cumplimiento, solución, protección, escasez, comodidad y asistencia.
- vii. Influencia (construcción de confianza): una vez que las víctimas se sienten cómodas con el atacante, el siguiente paso que debe realizar un ingeniero social es tratar de influir en ellas. Enfoques válidos podrían ser: deber moral, deseo de ayuda, sugerencia, orden, persuasión, etc.
- viii. Modelo de improvisación: como se muestra en el esquema, no todos los esfuerzos para construir una buena relación e influir en las personas son fáciles de llevar a cabo; a veces el ingeniero social debe improvisar ejecutando acciones alternativas y transmitiendo mensajes clave.

## 3. Etapa de ejecución del ataque

El despliegue del ataque está constituido por cuatro fases, a saber:

- i. Establecimiento de la zona de confort: lograda la confianza de la víctima, el ingeniero social debe posicionarla en una zona de confort empleando técnicas de

escucha, conversando coherentemente y tratando temas fundados en valores asentados/compartidos.

- ii. Control de participación: el establecimiento de la zona de confort debe ejecutarse manteniendo el control sobre la víctima con técnicas como "la interacción y estímulo entre el comandante y la base", elogiando las acciones de ésta última.
- iii. Modo (previo) de ataque: la víctima está divulgando la información específica, bien directa o explícitamente (divulgación de activos) o bien indirecta o implícitamente (información útil para alcanzar la información final).
- iv. Confirmación del éxito: el ingeniero social debe verificar la validez de la información obtenida.

#### 4. Etapa posterior a la acción

Una vez ejecutado el ataque, es momento difuminar la relación de una forma suave, protegiendo al ingeniero social de cualquier vinculación con el ataque posterior.

- i. Clausura: este es un mensaje de despedida del ingeniero social a la víctima, normalmente agradeciendo la "relación" y ofreciendo su ayuda en caso de necesidad futura.
- ii. Desvanecimiento: en esta fase, el ingeniero social debe ir eliminando poco a poco sus vínculos e información del sistema atacado, primero bajando su nivel de actividad a mínimo y luego desapareciendo.
- iii. Eliminación de rastros: finalmente es imprescindible contar con un proceso para eliminar todos los rastros que puedan vincular a la víctima con el atacante.

## 4 El proceso de la ingeniería social

Es posible analizar la ingeniería social desde un punto de vista metodológico, sin entrar en el campo de la psicología social. Acudiremos al módulo titulado "*Ingeniería Social*" de la asignatura "*Vulnerabilidades de Seguridad*" del MISTIC, para desarrollar este capítulo.

Como hemos comentado en el capítulo anterior, los ataques de ingeniería social se basan en la realización de acciones, enmarcadas en distintas fases. Cada acción puede generar resultados parciales que a su vez podrán combinarse para realizar nuevas acciones hasta conseguir el objetivo final. Este proceso que sigue la ingeniería social puede representarse gráficamente, permitiendo estudiar casos concretos hasta determinar cuáles son los puntos críticos del sistema y que estrategias de prevención diseñar.

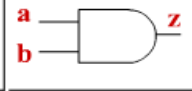

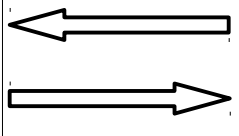
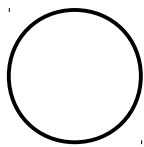
Cada una de las acciones particulares que se realizan en estos ataques vendrá caracterizada a tres niveles:

1. Estrategia (E). Determina el tipo de la acción y los objetivos que persigue. Todas las acciones pertenecerán a una de las siguientes estrategias: recogida de información (RI), forzar una acción (FA) y ataque directo (AD).
2. Técnica (T). Para conseguir los objetivos de cada estrategia se pueden emplear varias técnicas concretas, apareciendo nuevas con el paso del tiempo.

3. Vía (V). La vía identifica exactamente el medio por el cual se utiliza una cierta técnica en una acción. Una misma técnica puede aplicarse a través de vías diferentes.

Dentro del proceso de la ingeniería social, las acciones se realizarán secuencialmente hasta conseguir la finalidad del ataque. En algunos casos serán necesarias varias acciones previas para realizar otras, o existirán acciones alternativas para conseguir un mismo resultado parcial. Los diagramas de ataques de ingeniería social (DAIS) nos permitirán representar gráficamente estas relaciones de secuencialidad entre las acciones.

Un DAIS se compone de nodos acción, nodos relación indirecta, relaciones directas y nodo objetivo. Las relaciones se representan como flechas, donde el sentido indica la secuencia.

Acción de ataque	Relación indirecta		Relación directa	Objetivo
	Conjunto	Alternativa		
E [RI, FA, AD]	<p><b>AND - Y</b></p> 	<p><b>OR - O</b></p> 		
T				
V				

Veamos un ejemplo que combina distintos nodos y relaciones. Este proceso requiere por un lado ejecutar al menos una acción de recogida de información y por otro ha de ejecutarse una acción forzada. Combinando ambas será posible llevar a cabo una acción de ataque directo.

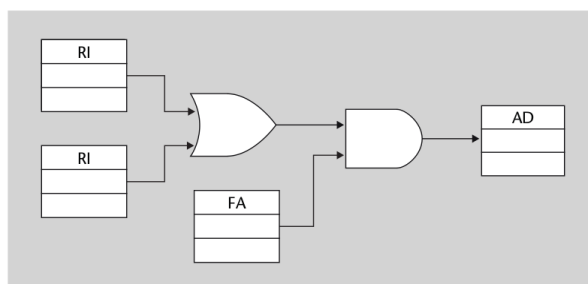


Ilustración 7: Ejemplo diagrama DAIS. Extracto material UOC

Un mismo ataque de ingeniería social puede expresarse de multitud de maneras sin variar la relación final, según se combine los nodos Alternativa y Conjunto. Esta flexibilidad se convierte en un inconveniente para comparar los DAIS de dos ataques, por lo que hemos de recurrir a su normalización.

Un DAIS normalizado será aquel en el que los nodos Alternativa y Conjuntos solo se utilizan de manera combinada como Alternativa de Conjuntos (suma de productos).

Si expresamos el diagrama DAIS de la figura anterior representando el nodo Alternativa como el operador “+”, el nodo Conjunto como el operador “\*”, y las acciones como los operandos  $A_i$ , tenemos una expresión:

$$(A1 + A2) * A3$$

$$\Downarrow$$

$$(A1 * A3) + (A2 * A3)$$

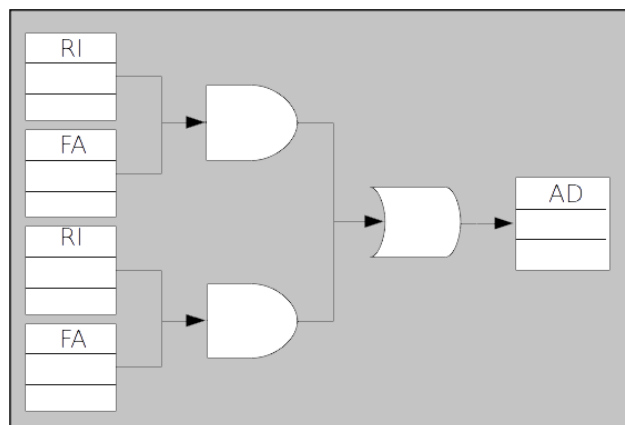


Ilustración 8: DAIS normalizado. Elaboración propia.

Después del proceso de normalización, se observa cómo sin cambiar la secuencia de acciones del ataque, éste se representa de manera equivalente como una alternativa de conjuntos.

Ahora que sabemos representar un ataque, toca aclarar las **estrategias que forman parte de un nodo acción**:

a) RI o recogida de información

La información puede ser obtenida al ser expuesta de manera inconsciente por los usuarios (sin interacción humana), o bien mediante la interacción del ingeniero social con otras personas.

El primer caso puede llevarse a cabo realizando búsquedas en Internet, agenciando físicamente la información y a través de la mera observación del comportamiento de las personas, hechos u objetos. El segundo caso incluye la interacción directa y la interacción mediante un medio de comunicación (teléfono, carta, mail, etc.)

b) FA o forzar una acción

Estrategia que emplea alguno de los aspectos explotables presentados en el apartado dedicado a las características humanas innatas y aprendidas, y cuya finalidad es la de conseguir –de manera directa o indirecta– que alguien realice una acción en beneficio del ingeniero social.

Ejemplos: impersonación de alguien que ocupase un cargo superior a la víctima para solicitar modificar una regla del firewall, ubicar un pendrive con un keylogger cerca de la víctima para propiciar su conexión a un equipo, dar pena para solicitar ayuda/información,...

c) AD o ataque directo

Ataque de carácter técnico que puede ser final o intermedio respecto al proceso de ingeniería social. Algunos ejemplos particulares de técnica empleada en este tipo de estrategia podrían ser un ataque de denegación de servicio vía un SYN flooding o una escalada de privilegios vía un desbordamiento de un buffer.

Y finalmente veamos un **caso real** de ataque de ingeniería social expresado como DAIS: consiste en alterar la nota de una asignatura en el expediente electrónico de un alumno en una universidad.

Remitimos al módulo "Ingeniería Social" de la asignatura "Vulnerabilidades de Seguridad" para conocer los detalles del escenario presentado, asumiendo que el diagrama presentado a continuación y la explicación documentada bajo el mismo es suficiente para la ejemplificación pretendida en este punto.

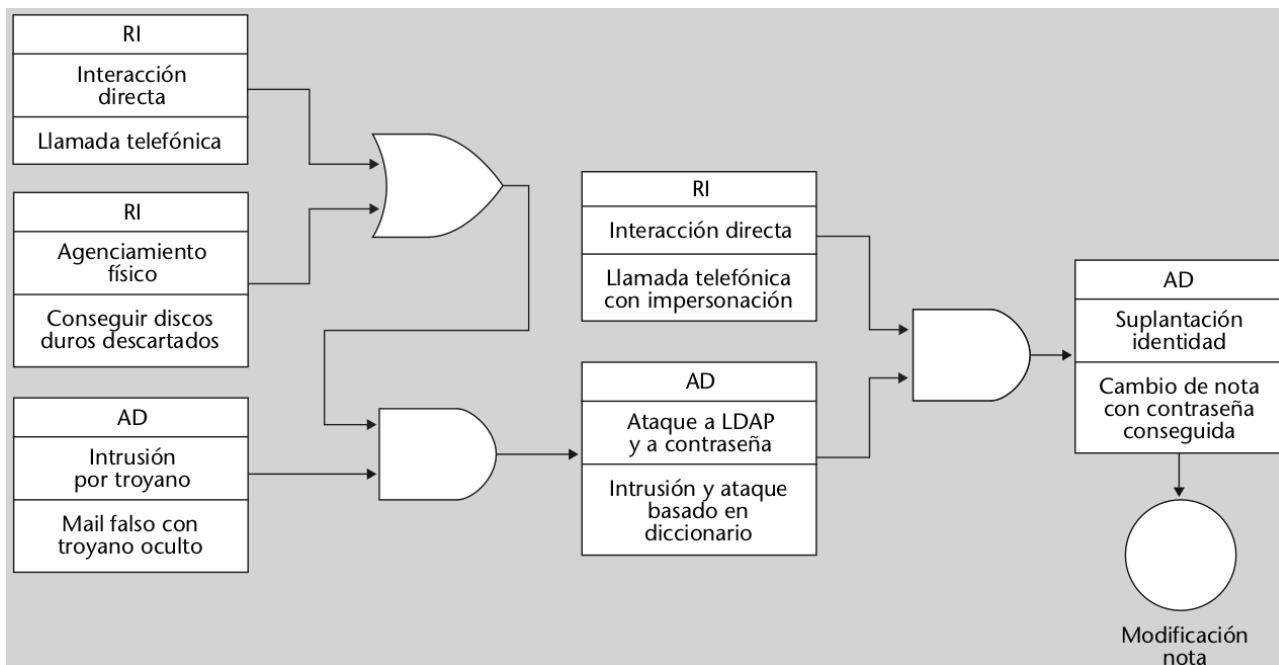


Ilustración 9: DAIS para la modificación de una nota en el expediente académico

Podemos ver las seis acciones más importantes en este ataque de ingeniería social organizadas a través de dos relaciones de conjunto y una de alternativa. En las acciones de la alternativa, comenzando cronológicamente, se intenta primero obtener información por medio de una llamada y al no conseguirlo, se opta por buscar esta información en un disco duro desinventariado.

Con la información de la localización del servidor de LDAP, juntamente (relación conjunto) con el control de una máquina interna conseguido mediante un troyano, ya se puede realizar el ataque a LDAP y al hash de la contraseña del profesor que está en él. Con otra llamada telefónica se consigue la otra contraseña necesaria para realizar el último ataque, que es el cambio de la nota.

## 5 Descubrimiento del tipo de información que puede llegar a obtenerse.

La Ingeniería Social, en manos de un consolidado experto, tiene un enorme poder, no sólo para la obtención de determinada información puntual, sino inclusive para la

generación de corrientes de opinión. Para ello, podrían incluirse determinados "ganchos" en foros, blogs, encuestas online o por televisión, sms, y redes sociales, mediante el uso de chat bots que simulan mantener conversaciones y otro tipo de personajes virtuales.

Ciñéndonos al tipo de información que puede llegar a obtenerse, podemos enumerar algunas tipologías: financiera, cuentas de servicios premium online, cuentas de programas de fidelización, credenciales de correo electrónico o redes sociales, listas de direcciones de correo electrónico, perfiles de usuarios, identidades personales, sujeta a propiedad intelectual o industrial, confidencial y un largo etc. Cada una de estas tipologías serán tratadas con más detalle en el siguiente capítulo a fin de mostrar los beneficios que pueden llegar a obtenerse con ellas.

Resulta obligado mencionar concursos, más bien competiciones, como el Social Engineering Capture the Flag (SECTF<sup>13</sup>). Se trata de eventos anuales celebrados dentro del Social-Engineer Village tanto en la conferencia DEF CON Hacking Conference en Las Vegas, NV como en la conferencia DerbyCon Information Security en Louisville, KY. El SECTF está organizado y alojado por Social-Engineer.Org (SEORG), la división educativa no comercial de Social-Engineer, LLC.

Estas competiciones se crearon para demostrar cuán serias son las amenazas de ingeniería social para las empresas y cómo incluso las personas novatas pueden usar estas habilidades para obtener información importante. Los concursos se dividen en dos partes, la fase de recopilación de información que tiene lugar antes de las conferencias, seguida de la fase de llamada en directo que se produce en DEF CON y DerbyCon.

La SECTF es un concurso en el que los participantes tienen asignadas empresas reales distintas, a las que deben "atacar" para intentar obtener cierta información previamente definida a través de un catálogo de preguntas. Cada dato o pieza de información lleva el nombre de bandera, simulando así el conocido juego "captura la bandera". El objetivo del concurso es demostrar la cantidad de información que se puede obtener libremente, ya sea a través de fuentes en línea o por teléfono.

Obviamente no todo vale, existen unas reglas que todo participantes debe seguir, ciertas normas sobre el anonimato de los intervinientes, cierto secreto para evitar prevenir a las empresas privadas objetivo, tiempos establecidos, etc.

A modo de muestra del tipo de información que puede llegar a obtenerse a través del empleo de la ingeniería social, a continuación se expone el cuadro de preguntas que debían responder los participantes en la edición de 2017:

Lista de banderas de 2017 SECTF <sup>14</sup>		
Preguntas (banderas) por áreas	Puntos de informe	Puntos de llamada
<b>Logística</b>		
¿El soporte de TI se maneja internamente o se subcontrata?	3	6

13 Informe sujeto a Copyright. Parcialmente reproducido y traducido con el permiso del autor, Cat Murdock.

14 <https://www.social-engineer.org/wp-content/uploads/2017/11/SECTF-2017.pdf>

¿A quién contratan para entregar paquetes?	3	6
¿Tienen cafetería?	4	8
¿Quién se encarga del servicio de comida?	4	8
<b>Otra tecnología</b>		
¿Cuál es el nombre de la empresa VPN?	4	8
¿Bloquea sitios web?	2	4
Si se bloquea algún sitio web, ¿cuáles? (Facebook, EBay, etc.)	3	6
¿Dispone de red inalámbrica? (si no)	2	4
Si es así, ¿cuál es el nombre de ESSID?	4	8
¿Qué marca y modelo de computadora usan?	3	6
¿Qué sistema antivirus usan?	5	10
<b>Puede ser utilizado para el pretexto en la empresa</b>		
¿Cuál es el nombre del servicio de limpieza / conserjería?	4	8
¿Quién hace la exterminación de insectos / plagas?	4	8
¿Cuál es el nombre de la compañía responsable de las máquinas expendedoras ubicadas en la empresa?	4	8
¿Quién gestiona sus (contenedores de) residuos/basura?	4	8
¿Cuál es el nombre la empresa externa de seguridad contratada o que personal interno se encarga de la seguridad?	5	10
¿Qué tipos de insignias personales de identificación utilizan para acceder a la empresa? (RFID, HID, Ninguno)	8	16
<b>Tecnología generalizada en la empresa</b>		
¿Qué sistema operativo se utiliza?	5	10
¿Qué paquete de servicio o versión?	8	16
¿Qué programa utilizan para abrir documentos PDF y qué versión?	5	10
¿Qué navegador usan?	5	12
¿Qué versión del navegador?	8	
¿Qué cliente de correo se usa?	5	10
¿Usan cifrado de disco? De ser así, ¿de qué tipo?	5	10
URL falsa (obtener el objetivo para ir a una URL) www.seorg.org	N / A	26

<b>Información específica de empleados</b>		
¿Cuánto tiempo han trabajado para la compañía?	3	6
¿Qué días del mes se les paga?	3	6
Información del horario de los empleados (hora de inicio y fin, descansos, almuerzos)	3	6
¿Cuál es el nombre de la compañía telefónica o PBX <sup>15</sup> contratada?	4	8
¿Cuándo fue la última vez que recibieron formación orientada a concienciar en seguridad?	5	10
10 puntos cada uno por cada vector de ataque realista detallado en el informe a un máximo de 50 puntos. Se debe proporcionar evidencia de respaldo para cada vector de ataque de por qué es realista.	0-50	N / A
Formato, estructura, gramática, diseño, calidad general del informe suponen un máximo de 50 puntos.	0-50	N / A

Es recomendable consultar los detalles del informe en el que se describen desde las herramientas que emplearon los participantes hasta la información que llegaron a obtener. A modo de conclusión tan sólo diremos que quedó patente el hecho de que las organizaciones continúan teniendo vulnerabilidades, o más bien que sus empleados son susceptibles de ser víctimas de ingeniería social.

## 6 Formas de utilización de la información para obtener beneficios.

### El mercado negro de datos

Hay quien opina que los datos son el "petróleo" de la economía digital. El mercado de venta de datos personales está en plena expansión precisamente porque el valor comercial de los datos personales es cada vez mayor. Los ciberdelincuentes son plenamente conscientes de ello y ponen los datos robados a disposición de cualquiera que tenga una conexión a internet y que pueda permitirse pagarlos. Se trata de una economía basada en servicios para cada fase del ataque que ha contribuido en gran medida a la forma de ofrecer los datos robados: "hacking como servicio".

A continuación haremos referencia a diferentes categorías de datos para analizar su interés o más bien su cotización en el mercado negro. Se trata de una información recabada de distintas fuentes entre las que destaca por ejemplo el informe de McAfee (Intel Security) sobre el "Comercio Clandestino de Datos"<sup>16</sup> o el blog<sup>17</sup> de Incibe

<sup>15</sup> Private Branch Exchange (<http://www.tech-faq.com/pbx.html>)

<sup>16</sup> <http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf>

<sup>17</sup> <https://www.incibe.es/protege-tu-empresa/blog/que-hacen-los-ciberdelincuentes-con-los-datos-robados>



## Datos financieros

Por datos financieros nos estamos refiriendo principalmente a datos de tarjetas de pago o de cuentas de servicios de pago online. La fugas de información que conllevan el robo de datos financieros siguen estando a la orden del día, afectando sobretodo a los comercios minoristas.

El precio de los datos de tarjetas de pago disponibles en estos mercados varía en función de un gran número de factores o información asociada: Número de tarjeta, CVV, PIN, generada por software, fullzinfo<sup>18</sup>, con COB<sup>19</sup>,...

Número de tarjeta de pago con código CVV2	Estados Unidos	Reino Unido	Canadá	Australia	Unión Europea
Generada por software	5-8 dólares	20-25 dólares	20-25 dólares	21-25 dólares	25-30 dólares
Con identificador bancario	15 dólares	25 dólares	25 dólares	25 dólares	30 dólares
Con fecha de nacimiento	15 dólares	30 dólares	30 dólares	30 dólares	35 dólares
Con Fullzinfo	30 dólares	35 dólares	40 dólares	40 dólares	45 dólares

Precios estimados por tarjeta, en dólares estadounidenses, por datos de tarjetas de pago robados (Visa, MasterCard, Amex, Discover)

Fuente: McAfee Labs

*Ilustración 10: Comercio clandestino de datos. Informe McAfee Intel Security 2015*

De cara al precio de las cuentas de servicios de pago, el factor decisivo es el saldo:

Saldo de la cuenta del servicio de pago online	Precio estimado por cuenta
400–1000 dólares	20–50 dólares
1000–2500 dólares	50–120 dólares
2500–5000 dólares	120–200 dólares
5000–8000 dólares	200–300 dólares

Cuentas de servicios de pago online a la venta.

Fuente: McAfee Labs

*Ilustración 11: Comercio clandestino de datos. Informe McAfee Intel Security 2015*

## Cuentas de servicios online de contenido premium y de programas de fidelización

El vídeo en streaming (de 0,55 a 1 dólar), televisión por cable (7,5 dólares) o acceso a canales deportivos (15 dólares) son ejemplos de precios en el mercado negro de este tipo

<sup>18</sup> El vendedor proporciona todos los detalles de la tarjeta y de su propietario

<sup>19</sup> Significa con "cambio de dirección de facturación", en alusión a información sobre credenciales de acceso a la cuenta.

de servicios, lo que obliga a los delincuentes a manejar grandes volúmenes de cuentas para obtener rentabilidad. Pero aún así, no cabe duda de que hay demanda para ello.

Los datos de acceso a programas de fidelización del sector hotelero y a las cuentas de subastas online, podrían parecer objetivos de poco valor, pero los investigadores han descubierto que también están a la venta en el mercado negro, bien para suplantar identidades o para apropiarse de la reputación del propietario.

### Credenciales para iniciar sesión

Otros tipos de datos en venta son las credenciales de acceso a sistemas de redes de confianza de las empresas, redes sociales, buzones de correo electrónico, etc. Las credenciales otorgan acceso a recursos, servicios o datos autorizados a su lícito propietario, pero en manos de un delincuente permiten a éste suplantar la identidad del titular y operar con "libertad", ya sea para hacer (mal)uso de tales recursos o servicios como para robar la información a su alcance (patentes, tecnología, innovación, investigación, datos personales,...).

En la actualidad, los sistemas de control de las infraestructuras críticas, conectados a las redes de confianza de las empresas de las que dependen, son un objetivo claro de los ciberdelincuentes, principalmente cuando se trata de acciones terroristas. Los sistemas web de administración remota suponen un riesgo importante que debe protegerse, comenzando por las credenciales de acceso.

Otro posible uso de la personalidad virtual robada podría ser la comisión de una falta o peor aún de un delito, además de propio robo de identidad: amenazas, insultos, coacciones, chantaje, estafa,...

Además, el perfil social de un individuo en sus redes sociales dispone de más información de utilidad para aquellos que pretenden venderla: números de teléfono propios y ajenos, otras contraseñas, fotos (incluso de menores).

### Direcciones de correo electrónico

Las direcciones de correo electrónico, previamente verificadas, se venden en el mercado negro como parte de enormes bases de datos para el envío de correos

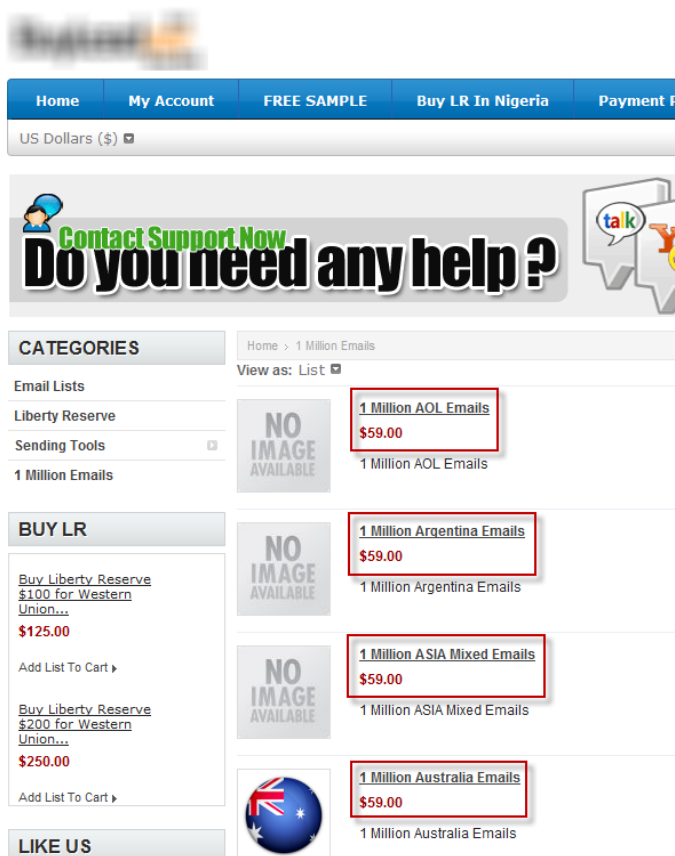


Ilustración 12: Direcciones de correo electrónico en venta. <https://www.welivesecurity.com>

no deseados (spam<sup>20</sup>). Se trata de un problema de tal trascendencia que inclusive existe un grupo de trabajo específico creado con la finalidad de luchar contra el abuso de mensajes y malware, su acrónimo es M3AAWG<sup>21</sup> o lo que es lo mismo Messaging, Malware and Mobile Anti-Abuse Working Group. En su último estudio<sup>22</sup>, con métricas agregadas desde enero de 2012 hasta junio de 2014, el grupo de trabajo determinó que el correo electrónico abusivo se mantuvo estable, con cifras que van desde el 87.1% al 90.2%.

Según consta en el blog de Incibe, el spam es un negocio porque aunque sólo el 0,001% de los receptores de dicho spam puedan hacer compras del producto spameado, estas bases de datos son relativamente baratas en comparación con lo que se puede ganar con ellas. Además es posible filtrar las direcciones por proveedor de correo, país, sector de interés, etc.

Entre las distintas utilidades que los delincuentes pueden dar a las bases de datos de correos, está la de dirigir spam con malware adjunto o enlazado. Se trata de un mecanismo de infección que lanzado a nivel global podría generar una red de ordenadores zombi (botnet) preparados para minar criptomonedas, producir ataques de denegación de servicio,..., o ser vendidos como servicio a un tercero.

### Perfiles de usuario. Identidades

Se trata de una información muy cotizada por ingenieros sociales pues su actividad principal está basada en ella, siendo la puerta de acceso a otro tipo de información, pe. financiera, confidencial,...

Los datos personales de un individuo junto con sus gustos, hábitos de compra, ideología, creencias, estado de salud, lugares que frecuenta, perfiles sociales, etc. son de enorme trascendencia en el perfilado de correos, recuperación de contraseñas, suplantación de identidad, etc. En la siguiente imagen se muestra un ejemplo de la identidad digital de una persona robada por ciberdelincuentes, lo que ocasionaría que un posible comprador podría hacerse con el control de la vida digital de esta persona.



Ilustración 13: Ejemplo identidad a la venta. Comercio clandestino de datos. Informe McAfee Intel Security 2015

20 SPAM: Sending and Posting Advertisement in Mass

21 <https://www.m3aawg.org/>

22 <https://www.m3aawg.org/documents/en/email-metrics-report-16>

Estrechamente relacionado con el mercado de identidades robadas está el mercado de información personal de seguro médico robada: compañía, número de póliza,... Estos datos no son tan fáciles de comprar como la información de las tarjetas de pago, pero aun así, hay vendedores que los ofrecen en Internet.

### **Información confidencial**

La información que una empresa tiene de sus clientes, de sus trabajadores, de sus productos o servicios, de su estrategia de negocio, así como la que conserve una administración pública en cumplimiento del ejercicio de sus obligaciones, suele tener la consideración de confidencial. Un problema de fuga de datos en el primer caso podría desencadenar una ventaja competitiva para el resto de empresas del sector e incluso la clausura de la compañía. Ese mismo problema en la correspondiente Administración, provocaría desconfianza en la ciudadanía, dimisiones o ceses de cargos directivos y probablemente un importante coste político. Así pues, el ciberdelincuente que tenga en su poder esta información, podría tener muchas facilidades para sacar dinero de esta situación (rescate), con la ventaja de que la organización afectada no estará interesada en sacarla a la luz pública, a pesar de las obligaciones legales.

Generalmente cuando se produce un ataque a una empresa por este motivo, se trata de una amenaza persistente y avanzada. No se trata de ataques oportunistas en los que se vende todo lo que se encuentra sino más bien de ataques en los que se busca algún tipo de información concreta.

### **Recursos del sistema**

Un ordenador comprometido, ya sea un equipo de usuario final, un servidor, un equipo de electromedicina, o cualquier objeto conectado del mundo IoT, puede ofrecer sus recursos hardware a procesos en ejecución controlados por el ciberdelincuente. El espacio en disco, la capacidad de procesamiento de la CPU o la GPU, la propia red de comunicación a la que el dispositivo se conecta, etc. son recursos del sistema que pueden estar siendo empleados sin el conocimiento del propietario, ejecutando acciones en paralelo.

El mercado negro se sirve de estos recursos para múltiples finalidades. Desde montar su infraestructura online, pe. instalando servidores webs desde donde publicar servicios de venta de "productos" robados, pasando por almacenar fotografías destinadas a pederastas, llevar a cabo minado de criptomonedas o incluso lanzar conexiones automáticas a web de anuncios. Todo ello pone de manifiesto la importancia de una auditoría técnica de seguridad después de un incidente de seguridad. En la actualidad, no podemos olvidar la importancia del mercado de la telefonía móvil, que ha dado lugar a delitos derivados de la apropiación ilegal de recursos de sistemas móviles infectados, pe. generando SMSs automáticamente hacia servicios premium previamente ofrecidos por el propio ciberdelincuente.

El acceso a estos mercados ilegítimos también puede ser ilegal, sobre todo para el administrador. No es extraño encontrar sistemas comprometidos que son utilizados por los ciberdelinquentes como «saltos intermedios» hacia sitios ilegítimos. De esta forma resulta más complicado rastrearles y detenerles.

### **Motivos no económicos**

La necesidad del ciberdelincuente de demostrar su capacidad de realizar una intrusión, bien por autoestima personal o como parte de un plan de reputación para futuras ofertas de sus servicios. El hacktivismo, entendido como *"la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos"*. La lucha social frente a situaciones percibidas como de abuso, desamparo o desprotección de los gobiernos hacia determinados colectivos o medios naturales... Todo ello podrían ser motivos que provocaran un ataque a los equipos de una organización y cuyo interés principal no fuese directamente el beneficio económico.

Esto es tan sólo una visión general de la forma de "monetizar" los datos a los que un ciberdelincuente, ingeniero social en primera instancia, podría tener acceso. El propio McAfee Intel Security emitió otro informe<sup>23</sup> destinado exclusivamente al robo de datos en el sector sanitario y la web Forbes se hizo eco de un informe<sup>24</sup> emitido por la empresa Symantec que ponía de manifiesto el costo de los datos robados en el mercado negro.

## 7 Análisis legal de la ingeniería social en el marco de la ciberdelincuencia.

En un mundo conectado los incidentes tecnológicos afectan de manera global, ayudados por la falta de medidas de seguridad. La velocidad a la que avanza la tecnología y las diferentes jurisdicciones, dan lugar a vacíos legales poco recomendables en una sociedad basada en un estado de derecho.

En este capítulo vamos a realizar un acercamiento top-down, revisando brevemente el panorama internacional entorno a la ciberdelincuencia, la categorización de los tipos delictivos en el panorama nacional, y aterrizando todo ello desde la perspectiva de la ingeniería social.

### 7.1 Panorama internacional

Es obligado tomar en consideración el **décimo tercer Congreso de las Naciones Unidas sobre prevención del delito y justicia penal**, celebrado en Doha entre el 12 y el 19 de abril de 2015. De su contenido podemos extraer algunos fundamentos esenciales para entender el panorama internacional entorno a la ciberdelincuencia.

En 1994, en el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos se señalaba que el potencial de la delincuencia informática -aún no se había acuñado el término ciberdelincuencia- era tan amplio como el de los propios sistemas internacionales de telecomunicaciones.

La ciberdelincuencia es un término genérico, no jurídico técnico, que alude a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos. También hay quienes centran la ciberdelincuencia en los delitos contra la información computadorizada o el uso de recursos de información con fines ilícitos.

<sup>23</sup> <https://www.mcafee.com/es/resources/reports/rp-health-warning.pdf>

<sup>24</sup> <https://www.forbes.com.mx/cuanto-cuestan-tus-datos-personales-en-el-mercado-negro/>

Actos comprendidos habitualmente en la categoría de ciberdelincuencia	
Tipo de acto	Ejemplos
Contra los datos o sistemas informáticos.	Atacan la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos.
Empleando los sistemas informáticos o de información como un medio.	Estafas, robos, daños a otras personas, incitación al odio, pornografía infantil, contra la identidad, ventas de mercancías ilícitas por internet, etc.

Cada vez cuesta más diferenciar entre ciberdelincuencia y delincuencia convencional. Las pruebas electrónicas, como los mensajes de texto, los mensajes electrónicos, los datos de navegación por Internet o los datos de redes sociales, forman parte de muchas investigaciones penales convencionales.

El desarrollo de la conectividad electrónica global (internet), ha supuesto un impulso de la ciberdelincuencia y por ende de las pruebas digitales. Baste considerar las redes zombi o botnets, que pueden constituir redes globales de decenas o centenares de miles de dispositivos infectados con programas informáticos maliciosos controlados a distancia por delincuentes. Las páginas web o aplicaciones móviles de los medios sociales, que pueden utilizarse para cometer actos de hostigamiento, incitación al odio, amenazas de violencia, extorsión, o para la difusión de información privada a escala global en cuestión de segundos. O el "Internet de las cosas", donde los delincuentes intentan también extender sus actividades.

En los últimos años los sistemas de justicia penal se han venido familiarizando más con los conceptos de direcciones IP y registros de conexión, así como con el uso de órdenes judiciales para obtener datos de proveedores de servicios electrónicos. Como resultado de ello, las huellas electrónicas que dejan los usuarios de Internet resultan cada vez más accesibles para los investigadores. No obstante, a la par se está poniendo a disposición de la ciudadanía y por tanto de los ciberdelincuentes, de forma "gratuita", herramientas de cifrado de comunicaciones y documentos, así como herramientas de navegación anónimas y servicios ocultos, que dificultan el trabajo de las autoridades.

El reconocimiento de la existencia de los delitos informáticos y la necesidad de combatirlos no solo se circunscribe al ámbito de la ONU. En el 2001, se firmó el **Convenio de Budapest** (conocido como el "convenio sobre cibercriminalidad"). el primer tratado internacional que tiene como fin hacer frente a los delitos informáticos y los actos ilícitos en internet armonizando leyes nacionales, la mejora de técnicas de investigación y el aumento de la cooperación entre los países. El convenio fue elaborado por el Consejo de Europa, junto con la participación activa de Canadá, Japón y China como estados observadores.

El 23 de noviembre del 2001, el convenio fue firmado por los Estados miembros del Consejo y también se integraron Canadá, Japón, Estados Unidos y Sudáfrica. El 1 de julio del 2004 entró en vigor.

Clasificación de delitos informáticos del Convenio	
Delitos	Actos
Intrusión: infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.	Acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos. interferencia en el funcionamiento de un sistema informático y el abuso de dispositivos que facilitan la comisión de delitos. Pe.: backdoor, bomba lógica, bots, cracker, cryptovirus, keylogger, leapfrog, spam,...
Patrimoniales: estafas y falsificación informática.	Delitos económicos, en particular, las defraudaciones bancarias empleando técnicas de phishing y pharming, sabotajes y fraudes informáticos. Introducción, borrado o supresión de datos informáticos.
Relacionados con el contenido.	La producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
Relacionados con infracciones de la propiedad intelectual y derechos afines.	Spoofing, counterfeiting, copyright, cybersquatting, piratería informática o abuso de marca.

En enero del 2008, se promulgó el Protocolo Adicional al Convenio de Europa, con el objetivo de criminalizar los actos de racismo y de xenofobia que son cometidos a través de sistemas informáticos. Ello representa la importante necesidad de contar con herramientas legales que ayuden a los países a combatir este problema.

Tomando como base este Convenio, nace la **Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los Sistemas de información** (DOUE, nº L218/8, de 14 de agosto de 2013), y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, así como su impacto en el Código Penal español. El objetivo principal de esta nueva Directiva es endurecer las penas contra el hacking ilegal y armonizar penalmente el tratamiento que dan los países de la Unión Europea a los ataques contra los Sistemas de información.

La Directiva intenta que los ataques contra los sistemas de información sean castigados en todos los Estados miembros de la UE con penas efectivas, proporcionadas y disuasorias, mejorando y fomentando la cooperación judicial entre las autoridades judiciales y demás autoridades competentes. Así, se penalizan las conductas según su artículo 2, haciendo referencia a los ataques sin autorización como elemento esencial de la conducta, siendo esta circunstancia la que va a determinar que el acceso a un sistema de información sea legal o ilegal y, por tanto, perseguible penalmente.

Conductas tipificadas como ataque a un sistema de información	
Artículo 3	<u>Acceso ilegal</u> a los sistemas de información, cometido intencionadamente.
Artículo 4	<u>Interferencia ilegal</u> en los sistemas de información, entendida como la <u>obstaculización</u> o la interrupción significativa del funcionamiento de un sistema de información.
Artículo 5	<u>Interferencia ilegal en los datos</u> , consistente en borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización.
Artículo 6	<u>Intercepción ilegal</u> , entendida como la <u>intercepción</u> , por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, intencionalmente y sin autorización.

Estas cuatro conductas, consideradas como infracciones penales, ya eran delitos en España desde la reforma del **Código Penal** operada por la Ley Orgánica 5/2010, de 23 de junio, en vigor desde el 23 de diciembre de 2010.

A la luz de los ciberdelitos, la última orientación jurídica es priorizar el enfoque en la seguridad en las redes y los sistemas de información. A tal fin obedece la recientemente promulgada **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión**, también conocida como Directiva NIS. Esta Directiva impone, por ello, a las entidades gestoras de servicios esenciales, así como a los prestadores de ciertos servicios digitales considerados clave en el funcionamiento de Internet, la obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las autoridades los incidentes que tengan especial gravedad.

## 7.2 Enfoque nacional

El enfoque nacional debe comenzar sin duda por la consideración de la **Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (CP)**. El legislador ha aprovechado esta reforma para dar cumplimiento a las exigencias de transposición impuestas por la anteriormente mencionada Directiva 2013/40/UE, relativa a los ataques a sistemas de información.

Las vulnerabilidades de los dispositivos y las redes de telecomunicaciones son aprovechadas por los ciberdelincuentes hasta conseguir controlarlos remotamente, con el objetivo de preparar futuros ataques informáticos dirigidos. Por ello, la normativa penal contempla estas conductas de intromisión como nuevas formas de delincuencia, caracterizadas por el uso de dispositivos electrónicos, bien como objetos del delito o como instrumentos para el mismo. Ahora da protección tanto a las transmisiones de datos automatizadas, como a la información a la que se pudiera acceder mediante la interferencia sobre emisiones electromagnéticas.



En este sentido, los delitos contra los sistemas de información introducidos y modificados por la Ley Orgánica 1/2015, son los que a continuación detallan:

- El delito de acoso electrónico contra la libertad de las personas. Artículo 172 ter CP.
- Delitos de descubrimiento y revelación de secretos. Artículos 197 a 197 quinquies CP.
- Delitos de daños y delitos de interferencia ilegal en sistemas de información o datos. Artículos 264 a 264 quater CP.
- Delitos contra la propiedad intelectual. Artículo 270 CP.
- Abusos con fines sexuales cometidos a través de Internet u otros medios de telecomunicación a menores. Artículo 183 ter CP.

A continuación ofrecemos una visión general de la cibercriminalidad en base a la catalogación de los tipos de hechos delictivos que establece la legislación española y de la que se hace eco el Ministerio de Interior en su portal estadístico. Así pues, vamos a mostrar un cuadro resumen, donde podemos observar un cruce entre los mencionados tipos de hecho delictivos y el articulado del Código Penal español que los comprende:

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SEC A UTILIZAR
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ACCESO ILEGAL INFORMÁTICO	Ninguna
		OTROS RELATIVOS AL MERCADO/CONSUMIDORES	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	DAÑOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ATAQUES INFORMÁTICOS	Ninguna
Falsificación informática	Arts CP 388-389, 399 bis, 400 y 401	FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE ÚTILES PARA FALSIFICAR USURPACIÓN DEL ESTADO CIVIL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Fraude Informático	Arts. CP 248 a 251 y 623.4	ESTAFA BANCARIA ESTAFAS CON TARJETAS DE CREDITO, DEBITO Y CHEQUES DE VIAJE OTRAS ESTAFAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Delitos sexuales	Arts. CP 181, 183.1, 183.bis, 184, 185, 186, 189	EXHIBICIONISMO	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		PROVOCACIÓN SEXUAL	
		ACOSO SEXUAL	
		ABUSO SEXUAL	
		CORRUPCIÓN DE MENORES/INCAPACITADOS	
		PORNOGRAFIA DE MENORES	
DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Ninguna		
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP (Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Contra el honor	Arts. 205 a 210 y 620.2 del Código Penal	CALUMNIAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		INJURIAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Amenazas y coacciones	Arts 169 a 172 y 620 del C.Penal	AMENAZAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		COACCIONES	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Ilustración 14: Cuadro tipologías penales. SEC: Sistema Estadístico de Criminalidad

Como puede observarse, las variables y medios empleados típicamente para la comisión de estos hechos delictivos son: Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

### 7.3 La ingeniería social como ciberdelito

Si bajamos en la cadena de análisis para poner la lupa en aquellos ciberdelitos que más relacionados pueden estar con la ingeniería social, lo primero que debemos determinar es si esta técnica es en sí misma un ciberdelito, y lo segundo es dilucidar en qué medida forma parte de los vectores de ataque asociados a los tipos de hechos delictivos.

La Real Academia Española recoge en su diccionario el término **estafa** y en su segunda acepción dice así:

*2. f. Der. Delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro.*

Pero la amplitud del término la encontramos en el capítulo VI, artículo 248 del Código Penal español, que en su versión consolidada dice así:

*1. Cometan estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.*

*2. También se consideran reos de estafa:*

*a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.*

*b) Los que fabricaren, introdujeran, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.*

*c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.*

Por tanto, el Código Penal español castiga la obtención de lucro empleando la "**estafa sociológica**", engañando a otro ser humano a través de cualquier fórmula de ingeniería social. Esto es aplicable tanto a las viejas maneras de actuar, como a los timos de cartas nigerianas, a algunas ventas de segunda mano, a falsas subastas en portales de internet, al phishing, a timos haciéndose pasar por organizaciones no gubernamentales, etc.

Así, las estafas, en sentido general, quedan sancionadas en el apartado 1º, en el que se encuadran las cometidas empleando ingeniería social no tecnológica. Mientras que las estafas informáticas, en sentido estricto, quedan sancionadas en el apartado 2º, en el que se encuadran las transferencias in consentidas de activos patrimoniales realizadas mediante manipulaciones informáticas o combinando las mismas con técnicas de ingeniería social (phising, pharming etc.)

No siendo un tipo delictivo en sí mismo, pero sí un agravante, el robo de identidad queda recogido en el capítulo IX relativo a los daños, artículos 264.3 y 264bis.3 del Código Penal español del siguiente modo:

*“Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.”*

Sin embargo, se echa en falta una transposición de la regulación de la inducción, la complicidad y la tentativa, desarrollada en el artículo 8 de la Directiva 2013/40/UE que dice así:

*1. Los Estados miembros garantizarán que la inducción y la complicidad en la comisión de las infracciones mencionadas en los artículos 3 a 7 sean sancionables como infracciones penales.*

*2. Los Estados miembros garantizarán que la tentativa de cometer las infracciones mencionadas en los artículos 4 y 5 sea sancionable como infracción penal.*

Parece ser remitida al régimen general del Código Penal español, lo que incrementa necesariamente la actividad jurisprudencial enconando la dificultad probatoria de estas actividades en los tipos delictivos analizados.

Sale fuera del alcance de este trabajo la exposición de las penas y sanciones asociadas a los reos de estafa.

Para finalizar este punto, parece apropiado sacar a colación una afirmación contenida en la publicación de Europol denominada Internet Organised Crime Threat Assessment (IOCTA) 2017. En ella se dice que *"existen dos tipos principales de ataques de ingeniería social que comúnmente se denuncian a las autoridades de la UE: el phishing y el compromiso del correo electrónico empresarial"*, también conocido como BEC por sus siglas en inglés.

Esta misma publicación se hace eco de informes<sup>25</sup> que sugieren que hasta el 60% de los "hackeros" no usan ningún tipo de malware, sino que se basan únicamente en credenciales comprometidas e ingeniería social. Del mismo modo, muchos ciberdelitos dependen en gran medida de la ingeniería social, como el engaño pederasta o "grooming" que tienen como objetivo a los niños conectados a internet. En el fraude de pagos, la ingeniería social se usa para obtener tarjetas de pago auténticas y números PIN de las víctimas. La ingeniería social también es un componente clave en todos los demás fraudes ciberdependientes, incluidas las estafas de soporte tecnológico, los fraudes de pago por adelantado y los fraudes románticos, que siguen prevaleciendo en toda Europa.

## 8 La ingeniería social en números.

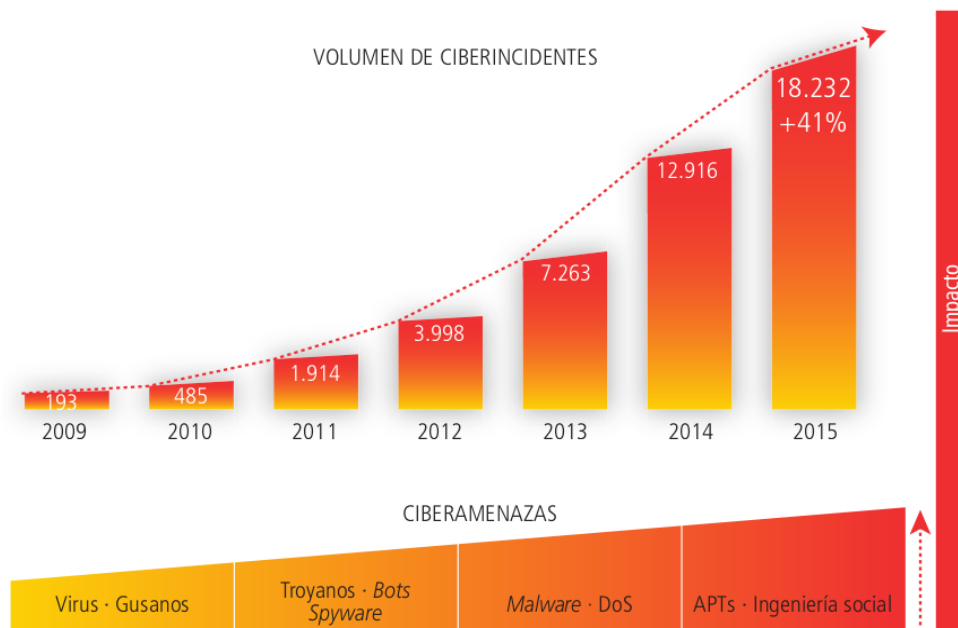
### 8.1 Ciberincidentes registrados

#### 8.1.1 Instituto de Auditores Internos

Conviene poner de manifiesto algunos datos que el Instituto de Auditores Internos (IAI) ha recabado del CCN-CERT y representado gráficamente, para entender la envergadura del problema al que se enfrentan las organizaciones. Se puede observar el importante impacto que tienen las **ciberamenazas directamente relacionadas con la ingeniería social**, las APTs.

---

25 <https://www.wired.co.uk/article/dnc-hack-proof-russia-democrats>



Fuente: elaboración propia a partir de datos de CCN-CERT

Ilustración 15: IAI. Guía de supervisión de la ciberseguridad

### 8.1.2 Verizon

Verizon Communications Inc. es una compañía global de banda ancha y telecomunicaciones y forma parte del Índice Dow Jones. Su nombre es un acrónimo de veritas y horizonte, y su sede está situada en el edificio Verizon en 140 West Street, Bajo Manhattan, Nueva York.

A los efectos del presente TFM nos interesa de esta compañía principalmente un informe anual que hace público con el nombre "YYYY *Data Breach Investigations Report*", donde YYYY debe reemplazarse por el año en el que se emite el informe.

El propio CCN-CERT español se hace eco de los datos publicados por esta corporación, pe. en su informe público titulado "*CCN-CERT-IA 16-17 Ciberamenazas y Tendencias 2017*" ofrece el siguiente gráfico donde puede verse el porcentaje de brechas de seguridad por categoría de activo y año con fundamento en el "2016 *Data Breach Investigations Report*":

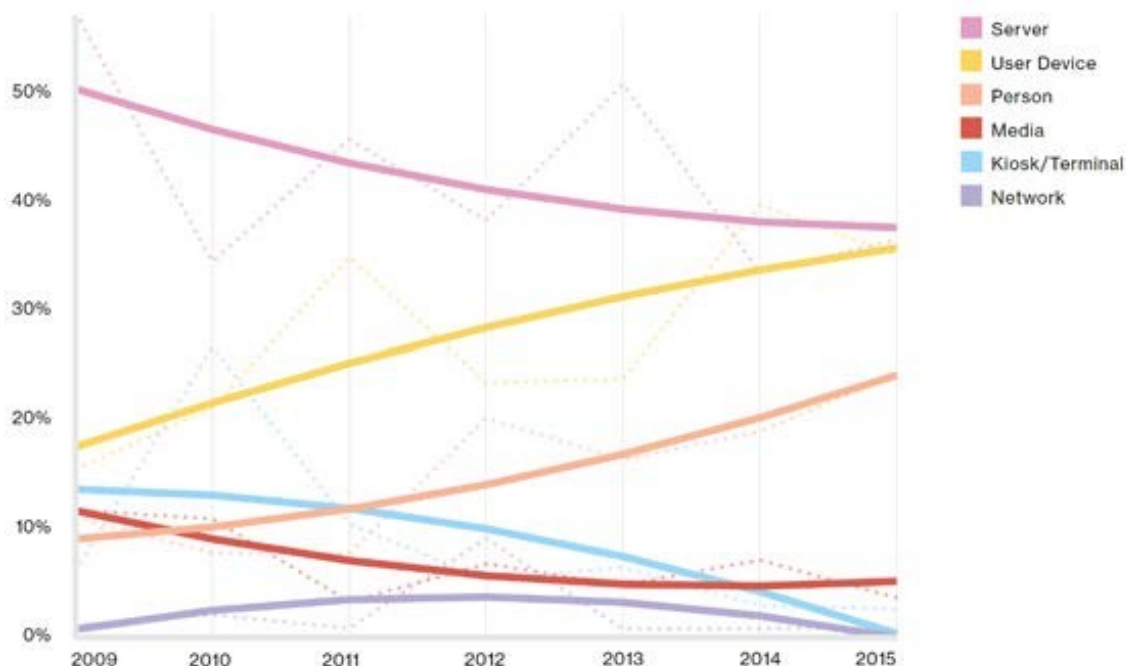


Ilustración 16: Porcentaje de brechas de seguridad por categoría de activo

En el gráfico puede observarse la línea naranja pálido correspondiente a brechas de seguridad vinculadas a personas y por tanto dentro de las cuales podríamos ubicar las relativas a los ataques de ingeniería social.

En palabras del CCN-CERT, durante 2016 han observado como muchos usuarios -personales o corporativos- han caído en la trampa del phishing a través de correo electrónico, o, incluso, de llamadas telefónicas (cuyo incremento en 2016 fue espectacular). Como se ha demostrado cuando la ingeniería social se dirige específicamente a sectores individualizados, a organizaciones o a personas concretas, el porcentaje de éxito o de los atacantes crece exponencialmente.

Volviendo a la fuente, en este caso al informe "2018 Data Breach Investigations Report", en su versión ejecutiva, Verizon afirma que la razón de ser de esta publicación es una apuesta por contribuir a la seguridad de las organizaciones, generando la confianza necesaria para que éstas puedan aprovechar al máximo las últimas innovaciones digitales. Cada informe se basa en el análisis de miles de incidentes del mundo real, más de 53,000 en 2017, incluyendo 2.216 infracciones de datos confirmadas: 53,308 incidentes de seguridad, 2,216 violaciones de datos, 65 países, 67 contribuyentes.

El informe contiene aseveraciones como esta: <<La gente comente errores (...) el 4% de las personas hará clic en cualquier campaña de phishing>>

Si acudimos al capítulo dedicado a los "ataques sociales: solo somos humanos", centrado en la persona como medio para llegar a la información y no como objetivo, podemos ver datos como los siguientes:

- El phishing y los pretextos representan el 98% de los incidentes sociales y el 93% de las infracciones.
- El correo electrónico continúa siendo el vector de ataque más común (96%).

- Frecuencia: 1450 incidentes, 381 con divulgación de datos confirmados.
- Los 3 patrones principales: Crimeware, Everything Else y Cyber-Espionage representan el 93% de todos los incidentes de seguridad.
- Fuente de amenaza: 99% agente externo, 6% agente interno, <1% socio (brechas)
- Motivación del agente: 59% financiero, 38% espionaje (brechas)
- Datos comprometidos: 47% personales, 26% secretos, 22% internos, 17% de credenciales.

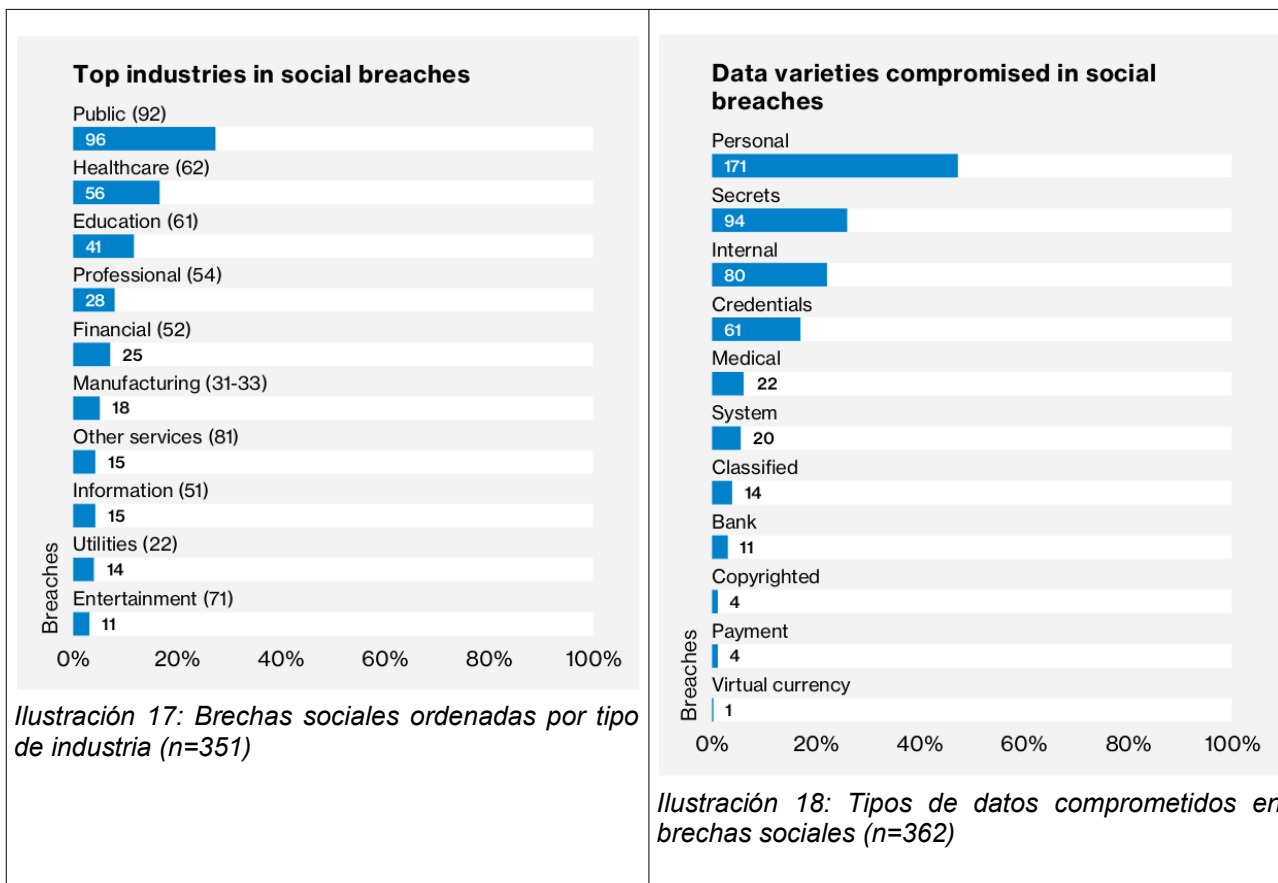


Ilustración 17: Brechas sociales ordenadas por tipo de industria (n=351)

Ilustración 18: Tipos de datos comprometidos en brechas sociales (n=362)

### 8.1.3 CCN-CERT IA-09/18: Ciberamenazas y Tendencias Edición 2018

Esta nueva versión, recién publicada durante la edición del presente trabajo, del informe de amenazas del Centro Criptológico Nacional, referido en el apartado anterior, ofrece el siguiente gráfico:

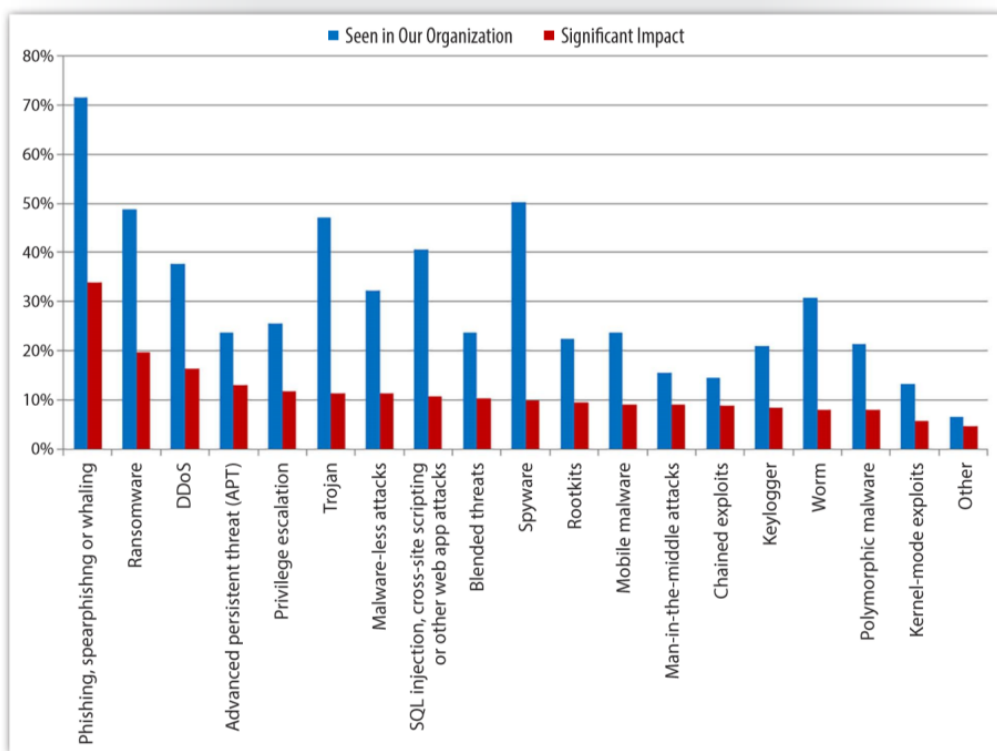


Ilustración 19: CCN-CERT IA-09-18 CIBERAMENAZAS Y TENDENCIAS 2018

En él se puede apreciar como en 2017 muchas de las técnicas directamente vinculadas a la ingeniería social, como las APT's o el grupo compuesto por Phishing, Spearphishing y whaling, suponen porcentajes muy elevados de ataques en los que aproximadamente la mitad de ellos tienen un impacto significativo en las organizaciones. En 2017 se han advertido muestras de phishing muy sofisticadas y muy difíciles de detectar. Según las fuentes<sup>26</sup> consultadas por el CCN para este informe, las campañas de phishing en 2017 aumentaron tanto en volumen como en sofisticación (Phishing-as-a-service<sup>27</sup>).

### 8.1.4 APWG: grupo de trabajo antiphishing

APWG es la coalición internacional que unifica la respuesta global al ciberdelito tanto a nivel de industria o empresa privada, como a nivel gubernamental y de los sectores de aplicación de la ley, así como para las comunidades de ONGs. También conocido como el "Grupo de Trabajo Antiphishing" como reflejan sus siglas (Anti-Phishing Working Group). Pues bien, esta coalición emite periódicamente informes de tendencias de la actividad de phishing, siendo el más reciente a fecha de redacción del presente trabajo el correspondiente al último trimestre de 2017. En él se recoge a modo de titular la siguiente afirmación: "se observaron aumentos notables en la suplantación de identidad (phishing) dirigida a los proveedores de SaaS<sup>28</sup> / webmail, así como un aumento en los ataques a los

26 Véanse: <https://securelist.com/spam-and-phishing-in-q2-2017/81537/> y [https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot\\_Quarterly\\_Threat\\_Trends\\_September\\_2017.pdf](https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf)

27 Véase: <https://www.netskope.com/blog/phishing-service-phishing-revamped/>

28 Software as a service: software como servicio.

objetivos financieros / bancarios, al almacenamiento en la nube y a los sitios de intercambio de archivos."

APWG rastrea e informa las notificaciones recibidas de phishing (campañas de correo electrónico) que son únicas. Una campaña de correo electrónico es un correo electrónico exclusivo que se envía a múltiples usuarios, dirigiéndolos a un sitio web de phishing específico (varias campañas pueden apuntar al mismo sitio web). APWG computa los correos electrónicos de notificaciones de phishing como únicos si en un mes determinado tienen la misma línea de asunto en el correo electrónico.

El APWG también rastrea el número de sitios web únicos de phishing. Esto está determinado por las URL base única de los sitios de phishing. (Un solo sitio de phishing se puede anunciar como miles de URL personalizadas, todas las cuales conducen básicamente al mismo destino de ataque). Los miembros que colaboran con el APWG también rastrean diversos conjuntos de datos y métricas adicionales para seguir la evolución del ciberdelito.

Del mencionado informe, tan sólo reflejaremos aquí los datos estadísticos destacados para el 4º trimestre de 2017:

	October	November	December
Number of unique phishing Web sites detected	65,509	54,322	60,926
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	61,322	86,547	85,744
Number of brands targeted by phishing campaigns	348	323	268

Ilustración 20: APWG. Estadísticas destacadas de phishing del último trimestre de 2017

## 8.2 Cibercriminalidad

### 8.2.1 Portal estadístico del Ministerio del Interior español

El portal estadístico del Ministerio del Interior del gobierno de España presenta anualmente los datos de cibercriminalidad, divididos por comunidades autónomas y por provincias. A su vez, cada división estructura la información en categorías según se trate de hechos conocidos o esclarecidos, detenciones e investigaciones, o victimizaciones. Y estas categorías se vuelven a dividir según el grupo penal, el tipo de hecho o la nacionalidad. Parte de esta información se expone de una forma más atractiva, aunque no de forma gráfica, en la web del Observatorio Español de Delitos Informáticos<sup>29</sup>.

Según consta en un documento<sup>30</sup> ubicado en la misma web del portal estadístico, los datos han sido obtenidos del Sistema Estadístico de Criminalidad (SEC). Para su cómputo se tienen en cuenta los hechos de los que han tenido conocimiento los siguientes cuerpos

29 <http://oedi.es/ciberdelitos/>

30 [https://estadisticasdecriminalidad.ses.mir.es/GuiasyAyudas/05\\_Cibercriminalidad.pdf](https://estadisticasdecriminalidad.ses.mir.es/GuiasyAyudas/05_Cibercriminalidad.pdf)

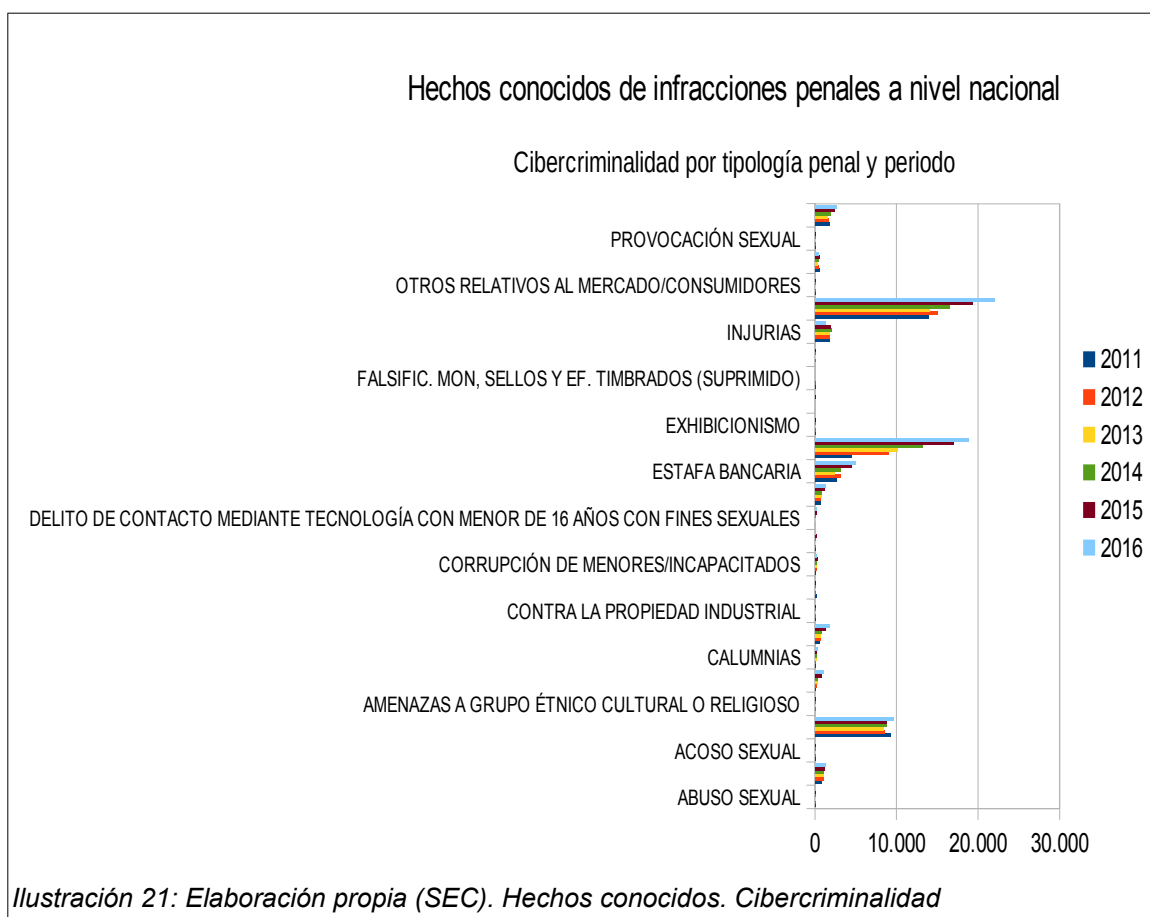


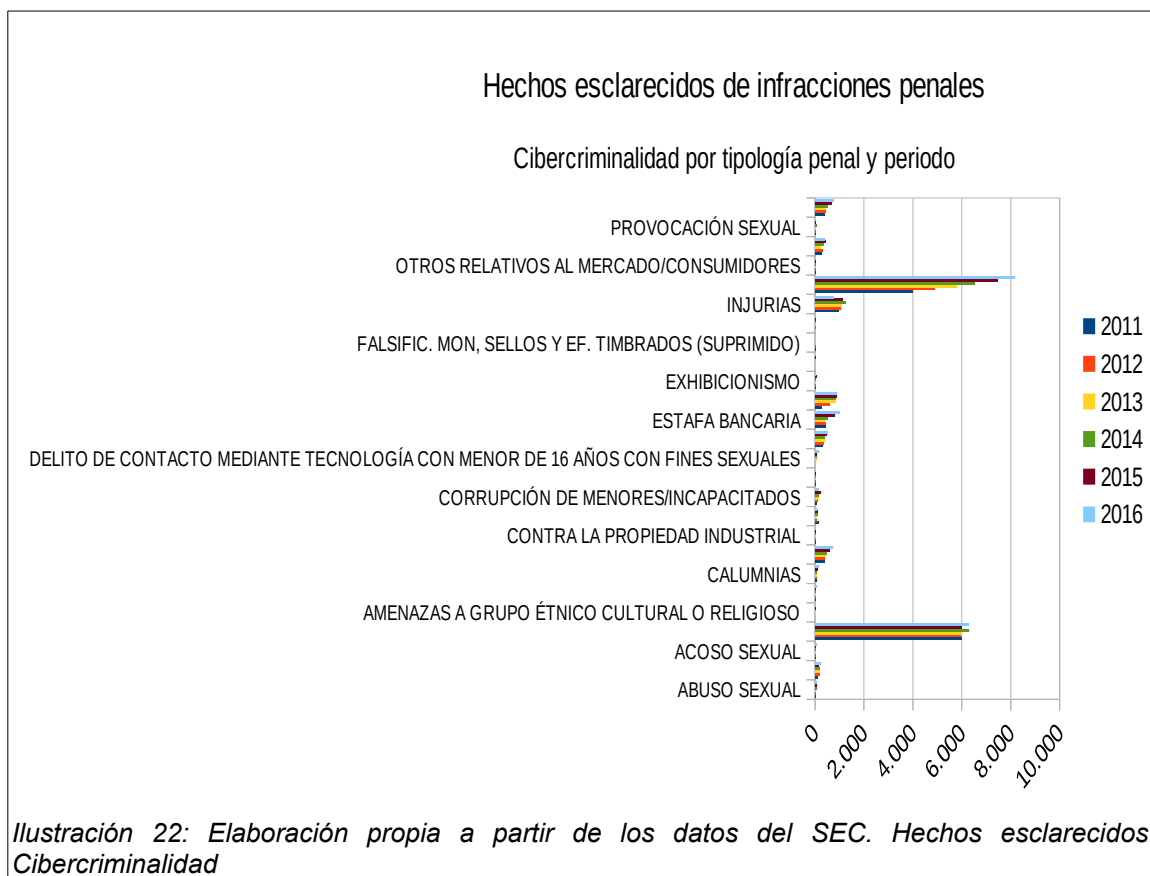
policiales: Guardia Civil, Cuerpo Nacional de Policía, Policía Foral de Navarra y las policías locales que facilitan datos al SEC.

La información que se representa en las siguientes gráficas de barras, relevante en su conjunto tanto por versar sobre la cibercriminalidad como por permitir comparar el volumen de unos tipos penales con otros, debe ser observada desde la perspectiva de la ingeniería social. En este sentido, como ya se comentó en el capítulo anterior, el tipo penal más relevante es el correspondiente a "estafas" y concretamente el tipo de hecho "otras estafas"; siendo conscientes en todo momento de que otros tipos penales pueden ser consecuencia derivada de la ingeniería social, pe. las estafas con tarjeta bancaria, el descubrimiento/revelación de secretos o el acceso ilegal informático.

Antes de exponer los datos conviene aclarar las expresiones "hechos conocidos" y "hechos esclarecidos". Por hechos conocidos se entiende el conjunto de infracciones penales y administrativas, que han sido conocidas por las distintas Fuerzas y Cuerpos de Seguridad, bien por medio de denuncia interpuesta o por actuación policial realizada motu proprio (labor preventiva o de investigación). Los hechos esclarecidos se clasifican como tales cuando en el hecho se da alguna de estas circunstancias:

- Detención del autor «in fraganti».
- Identificación plena del autor, o alguno de los autores, sin necesidad de que esté detenido, aunque se encuentre en situación de libertad provisional, huido o muerto.
- Cuando exista una confesión verificada, pruebas sólidas o cuando haya una combinación de ambos elementos.
- Cuando la investigación revele que, en realidad, no hubo infracción.





Respecto a la naturaleza de los sujetos responsables de la comisión de las infracciones penales, se computan las siguientes categorías:

- Investigado será una persona física o jurídica a la que se atribuya la participación en un hecho penal. No se adoptan medidas restrictivas de libertad para esa persona imputada.
- La detención alcanza la lectura de derechos de la persona física, privándole de libertad y poniéndolo a disposición judicial, por atribuirle la comisión de una infracción penal.

### Detenciones e investigados de infracciones penales

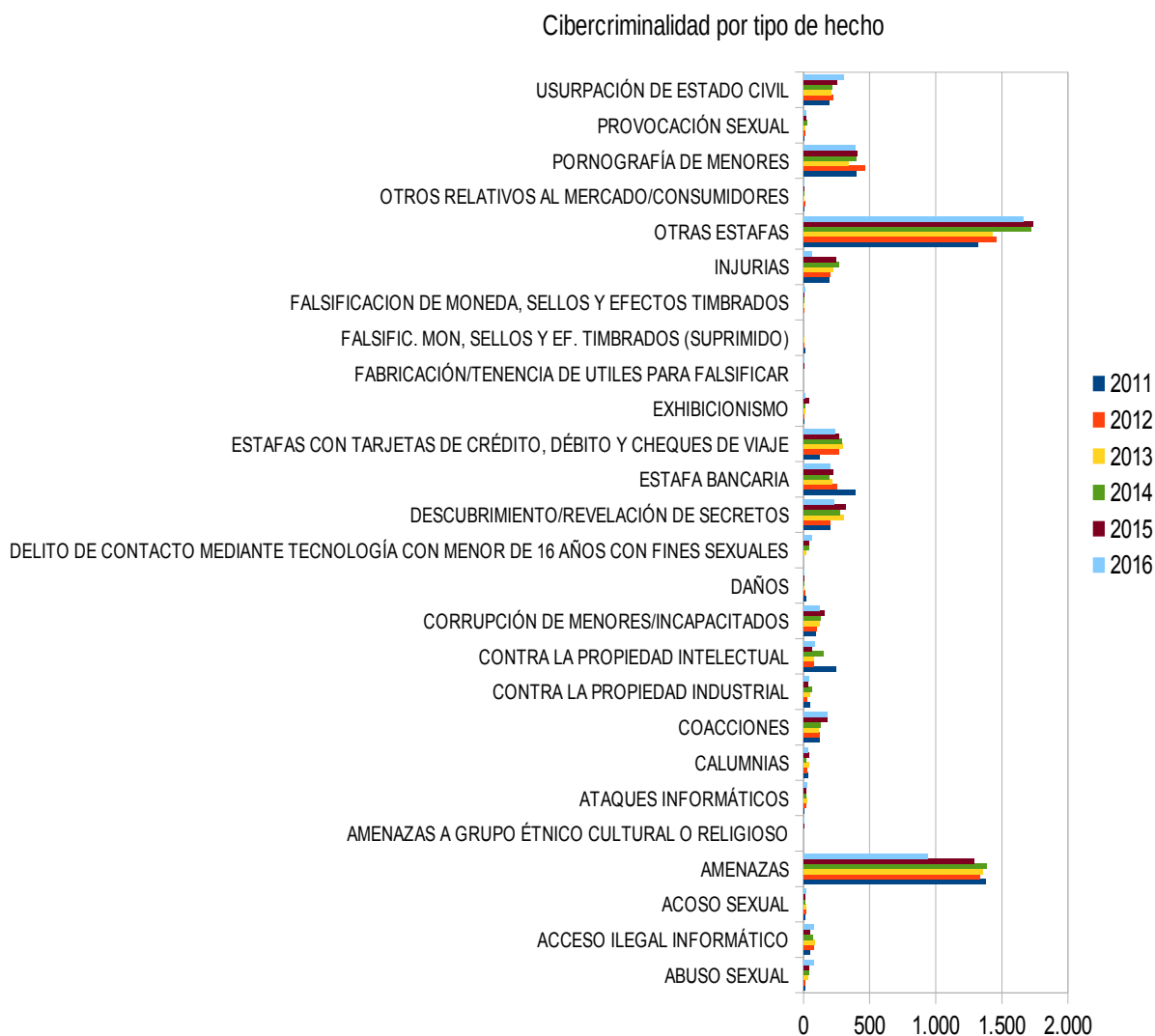


Ilustración 23: Elaboración propia a partir de los datos del SEC. Detenciones e investigados

El concepto de victimización viene referido al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal. Se diferencia del concepto de víctima, ya que éste se refiere a personas.

En una denuncia pueden darse varios hechos conjuntamente, e incluso pueden existir varias víctimas o perjudicados, siendo las victimizaciones el término que engloba a los diferentes hechos que afectan a una determinada víctima.

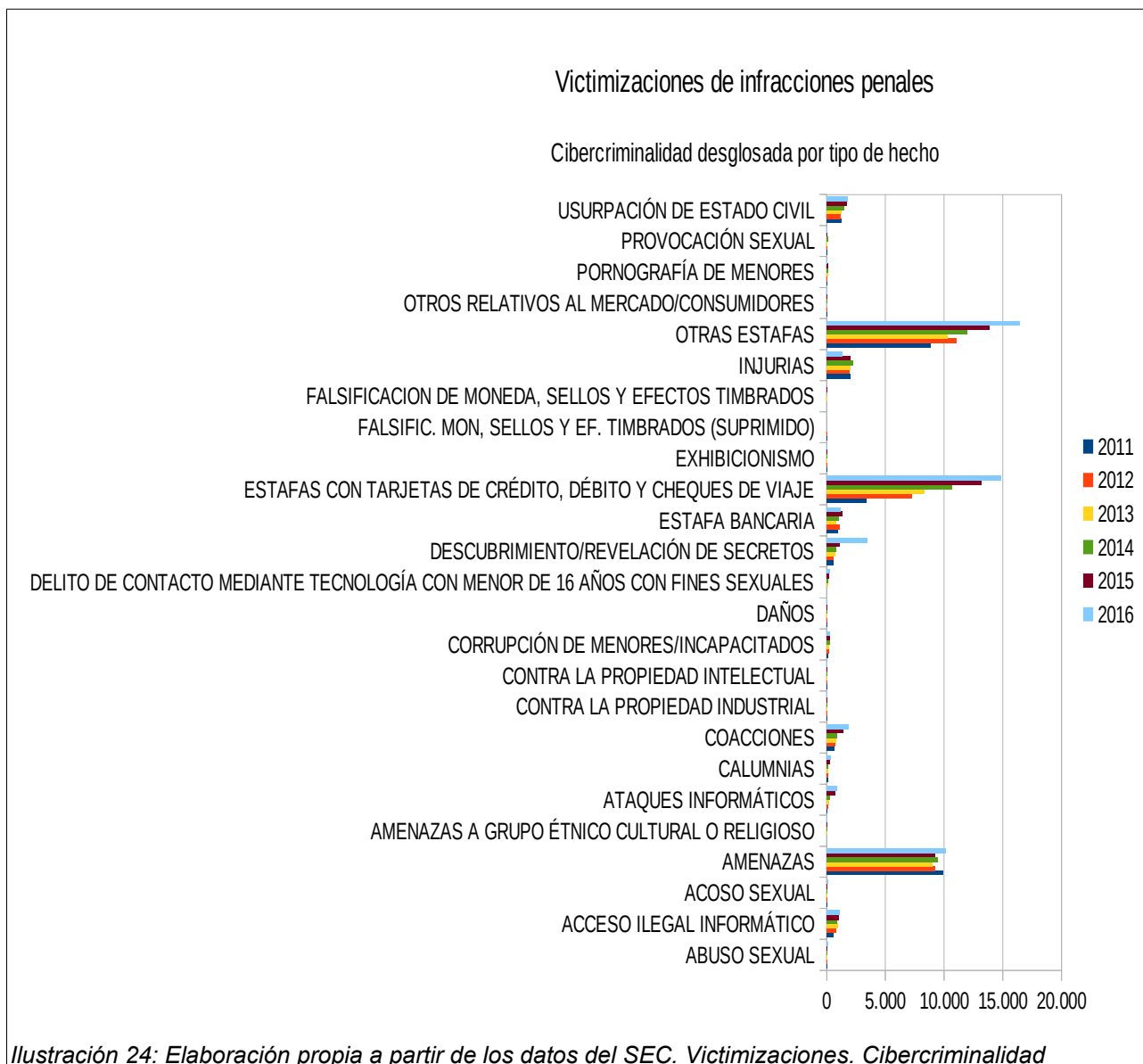


Ilustración 24: Elaboración propia a partir de los datos del SEC. Victimizaciones. Cibercriminalidad

### 8.2.2 Fiscal General del Estado

La memoria de 2017 del Fiscal General del Estado<sup>31</sup>, en su capítulo III, apartado 8 dedicado a la criminalidad informática, contiene un análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en el año 2016. Análisis que se fundamenta en las siguientes tablas donde puede observarse el importante volumen asociado a "la estafa cometida a través de las TIC":

31 [https://www.fiscal.es/memorias/memoria2017/FISCALIA\\_SITE/index.html](https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/index.html)

Delitos informáticos		Procedimientos judiciales incoados	%
Delitos contra la libertad	Amenazas/coacciones cometidos a través de las TICs (art. 169 y ss y 172 y ss)	989	12,31
	Acoso cometido a través de las TICs (art. 172 ter)	131	1,63
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	69	0,86
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	681	8,48
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	98	1,22
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	76	0,95
Delitos contra la intimidad	Ataques a sistemas informáticos/interceptación transmisión datos (arts. 197 bis y ter)	115	1,43
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	404	5,03
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICs (art. 215)	100	1,24
Delitos contra el patrimonio	Estafa cometida a través de las TICs (arts. 248 y 249)	4.930	61,36
	Descubrimiento de secretos empresariales (arts. 278 y ss)	49	0,61
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	16	0,20
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	114	1,42
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss)	54	0,67
Delitos de falsedad	Falsificación a través de las TICs	99	1,23
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	72	0,90
Otros		38	0,47
Total		8.035	100,00

Ilustración 23: Procedimientos judiciales por delitos informáticos conocidos por el Ministerio Fiscal en 2016

Delitos informáticos		Calificaciones	%
Delitos contra la libertad	Amenazas/coacciones cometidos a través de las TICs (art. 169 ss y 172 y ss)	242	14,68
	Acoso cometido a través de las TICs (art. 172 ter)	23	1,40
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	36	2,18
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	332	20,15
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	38	2,31
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	22	1,33
Delitos contra la intimidad	Ataques a sistemas informáticos/interceptación transmisión datos (arts. 197 bis y ter)	26	1,58
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	107	6,49
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICs (art. 215)	30	1,82
Delitos contra el patrimonio	Estafa cometida a través de las TICs (art. 248 y 249)	633	38,41
	Descubrimiento de secretos empresariales (art. 278 y ss)	16	0,97
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	20	1,21
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	22	1,33
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss)	32	1,94
Delitos de falsedad	Falsificación a través de las TICs	45	2,73
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	13	0,79
Otros		11	0,67
Total		1.648	100,00

Ilustración 25: Acusaciones formuladas por el Ministerio Fiscal en 2016

Delitos informáticos		Diligencias investigación	%
Delitos contra la libertad	Amenazas/coacciones cometidos a través de las TICs (art. 169 y ss y 172 y ss)	23	7,28
	Acoso cometido a través de las TICs (art. 172 ter)	0	0,00
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	3	0,95
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	3	0,95
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	5	1,58
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	3	0,95
Delitos contra la intimidad	Ataques a sistemas informáticos/interceptación transmisión datos (arts. 197 bis y ter)	11	3,48
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	20	6,33
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICs (art. 215)	8	2,53
Delitos contra el patrimonio	Estafa cometida a través de las TICs (art. 248 y 249)	144	45,57
	Descubrimiento de secretos empresariales (art. 278 y ss)	1	0,32
	Delitos contra los servicios de radiodifusión e interactivos (art. 286)	1	0,32
	Delitos de daños informáticos (arts 264, 264 bis y 264 ter)	8	2,53
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss)	2	0,63
Delitos de falsedad	Falsificación a través de las TICs	2	0,63
Delitos contra la Constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	82	25,95
Otros		0	0,00
Total		316	100,00

Ilustración 26: Diligencias de investigación del Ministerio Fiscal en 2016

## 8.3 Estudios publicados

### 8.3.1 Special Eurobarometer 464a:

#### *"La actitud de los europeos hacia la ciberseguridad"*

La Comisión Europea, en el marco de la iniciativa "Special Eurobarometer 464a", llevó a cabo en el mes de junio de 2017, una encuesta de opinión pública en los 28 países de la Unión Europea. Se tituló *"La actitud de los europeos hacia la seguridad cibernética"*<sup>32</sup> y como resultado se generó un informe, un resumen del informe y una hojas informativas por países.

La iniciativa parte de la consideración del ciberdelito como un problema sin fronteras, consistente en actos delictivos (fraude, estafa, falsificación, robo de identidad,...) que se cometen en línea mediante el uso de sistemas de información y redes de comunicaciones electrónicas. El objetivo de esta encuesta es comprender la conciencia, las experiencias y las percepciones de los ciudadanos de la UE sobre los problemas de ciberseguridad. Alrededor de 28.093 ciudadanos de la UE de diferentes categorías sociales y demográficas fueron entrevistados cara a cara en casa y en su lengua materna en nombre de la Dirección General de Comunicaciones. De ellos, 1007 entrevistados eran españoles.

Tan sólo reflejaremos aquí algunos de los resultados en España de una de las temáticas de la encuesta por su vinculación con la ingeniería social. Se trata de las preocupaciones

<sup>32</sup> <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/2012/yearTo/2018/search/SECURITY/surveyKy/2171>

de los ciudadanos por el cibercrimen y su percepción de las acciones emprendidas por las autoridades en aplicación de la normativa legal contra estas amenazas.

El primer diagrama muestra las respuestas a la cuestión sobre la frecuencia con la que el ciudadano ha sido víctima pe. de la recepción de correos electrónicos fraudulentos o llamadas de teléfono preguntando por sus detalles personales:

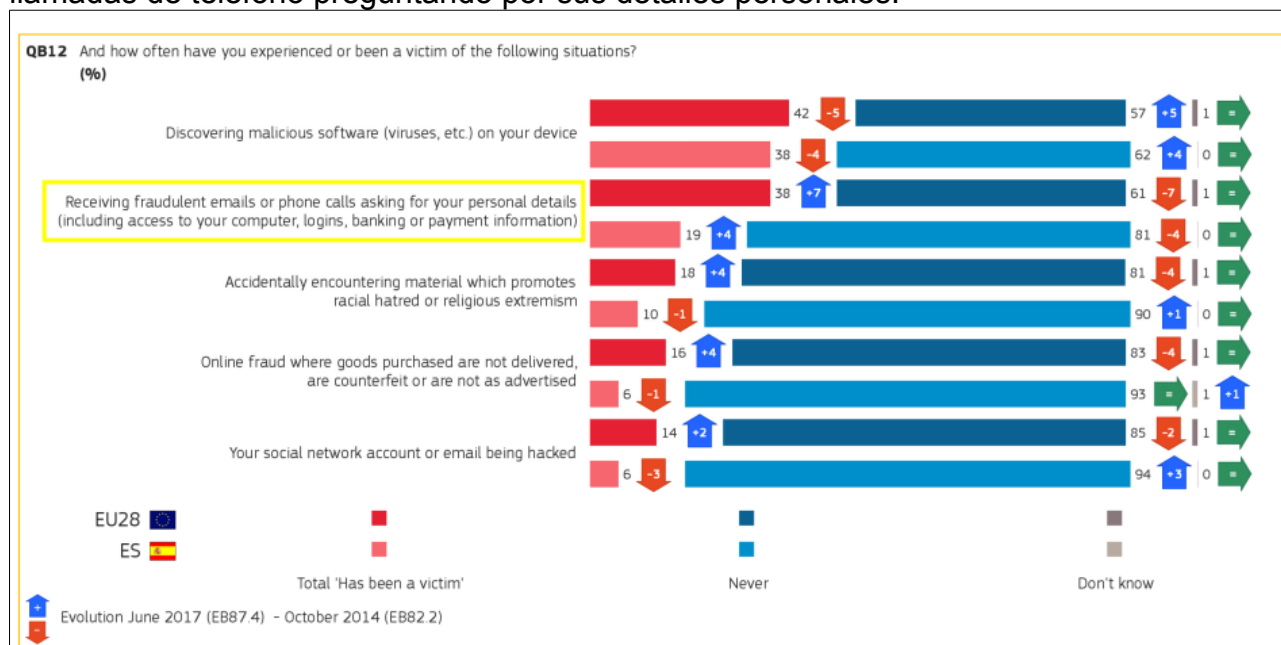


Ilustración 27: Eurobarometro. Factsheets. España. 3.QB12

En el segundo diagrama se observa que hay un equitativo reparto de opinión respecto de la actuación de la policía y demás autoridades frente al cibercrimen. Un 32% de los encuestados piensan que podrían hacer más, frente a un 35% que entienden que hacen suficiente.

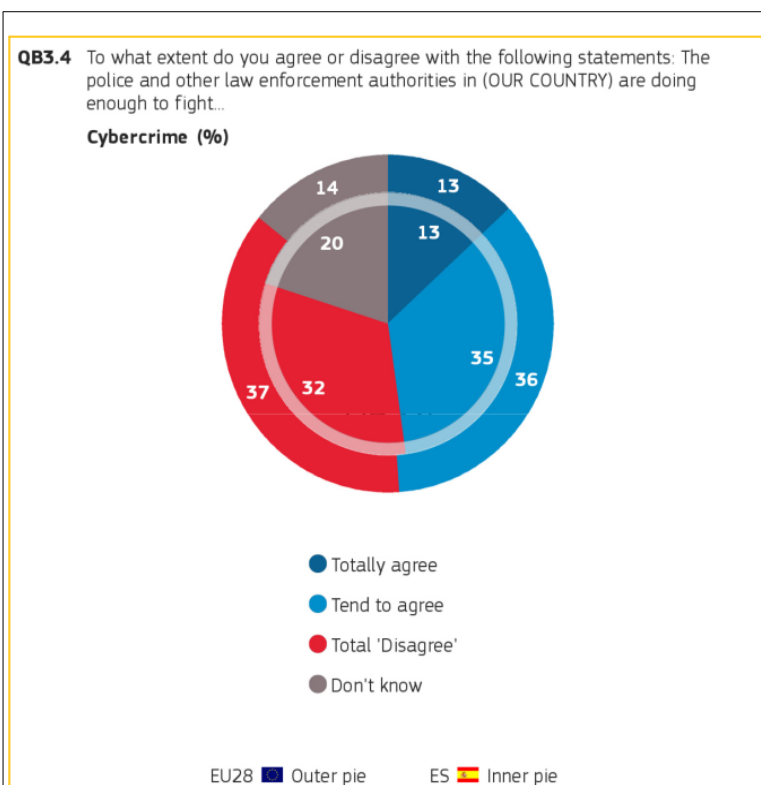


Ilustración 28: Eurobarometro. Factsheets. España. 3.QB3.4

### 8.3.2 Sobre la anatomía de los ataques de ingeniería social:

*"Una disección basada en la literatura de ataques exitosos"<sup>33</sup>*

Se trata de un interesante trabajo de investigación llevado a cabo por Jan-Willem Hendrik Bullée, Lorena Montoya, Wolter Pieters, Marianne Junger y Pieter Hartel, publicado como artículo por primera vez el 14 de julio de 2017 en la librería en línea Wiley.

El objetivo de este estudio fue explorar hasta qué punto los principios de persuasión se usan en ataques exitosos de ingeniería social. Se extrajeron 74 escenarios de 4 libros sobre ingeniería social (escritos por ingenieros sociales) y se analizaron. Cada escenario se dividió en pasos de ataque, que contenían interacciones individuales entre el delincuente y el objetivo. Para cada paso de ataque, se identificaron principios de persuasión. Los principales hallazgos que se obtuvieron fueron los siguientes:

- (a) los principios de persuasión son utilizados a menudo en ataques de ingeniería social,
- (b) la autoridad (1 de los 6 principios de persuasión) se usa considerablemente más que el resto, y
- (c) los pasos de ataque basado en la aplicación de un único principio se dan con mayor frecuencia que los de múltiples principios.

Entre las técnicas empleadas por los ingenieros sociales identificados en los escenarios, las influencias sociales basadas en los principios de persuasión fueron las más extendidas. El análisis de escenarios ilustra cómo explotar el elemento humano en seguridad. Los hallazgos respaldan la opinión de que los mecanismos de seguridad deberían incluir no solo contramedidas técnicas sino también sociales.

### 8.3.3 Todo es cuestión de Benjamins<sup>34</sup>:

*"Un estudio empírico"<sup>35</sup> sobre cómo incentivar a los usuarios a ignorar los consejos de seguridad"*

Los autores de este estudio, Nicolas Christin, Serge Egelman, Timothy Vidas y Jens Grossklags, examinaron el costo que debería asumir un atacante para pagar a los usuarios por llevar a cabo la ejecución de un código arbitrario, potencialmente malware. Contactaron con usuarios en sus casas para pedirles que descargasen y ejecutasen un programa escrito al efecto, sin contarles que hacía y sin que tuviesen forma de averiguar si era o no inofensivo. Cada semana aumentaban la recompensa por la instalación con el objetivo de descubrir si los usuarios ignorarían las recomendaciones comunes de seguridad como la de no ejecutar programas que no fuesen de confianza. Observaron que para pagos muy pequeños como 0.01 \$, el 22% de las personas que recibieron el encargo, finalmente ejecutaron el programa. Una vez que se aumentó el

<sup>33</sup> <https://onlinelibrary.wiley.com/doi/full/10.1002/jip.1482>

<sup>34</sup> Benjamin Franklin está representado en los billetes de 100\$ americanos, de ahí el argot "Benjamin" para referirse a billetes de banco.

<sup>35</sup> <http://guanotronic.com/~serge/papers/fc11.pdf>



incentivo directo a 1.00\$, esta proporción aumentó hasta el 43%. Se evidenciaba que a medida que el precio aumentaba, cada vez más usuarios que entendían los riesgos, terminaban por ejecutar el código. La conclusión de este estudio fue que por norma general los usuarios no se oponen a la ejecución de programas de procedencia desconocida, siempre que a su juicio los incentivos superen los inconvenientes.

### 8.3.4 CEFRIEL: La subestimada amenaza de la ingeniería social.

*"Tanto por el área de gobierno como el de gestión de TI"*

Este estudio fue publicado en noviembre de 2014 en slideshare.net y posteriormente redactado como artículo en ISACA Journal, es fruto del trabajo de Enrico Frumento y Roberto Puricelli, ambos ICT Security Specialist en CEFRIEL. Su objetivo era demostrar las bondades del marco de trabajo empleado por su empresa a través de los resultados de su aplicación en los distintos clientes, grandes empresas, que contrataron sus servicios cinco años atrás.

Realizaron un número significativo de evaluaciones sobre más de 12000 empleados para intentar determinar el nivel de riesgo real. En la mayoría de estas evaluaciones, se realizó una campaña de spear-phishing que se basó en ganchos genéricos (es decir, relacionados con temas generales que pueden ser atractivos para los usuarios, como ofertas especiales o descuentos para empleados). En muchos casos, los ataques se contextualizaron ligeramente para la compañía específica empleando colores, logotipos, plantillas y estilos de comunicación adecuados. En algunos casos concretos, se utilizó una referencia a una empresa específica en base a información disponible públicamente; no obstante, esto no influyó significativamente en los resultados.

La imagen muestra una comparación de los resultados de las evaluaciones. El eje X contiene el porcentaje de empleados que "hicieron clic" en el enlace del correo electrónico y el eje Y contiene el porcentaje de aquellos que además insertaron sus credenciales. Cada círculo representa una evaluación realizada en una empresa, su radio representa el tamaño de la empresa y el color representa el sector industrial al que se dedica. Los resultados promedio son bastante impresionantes y confirman que los ataques de spear-phishing funcionan bastante bien en la realidad. En estas evaluaciones, un empleado de cada tres (el 34%) siguió el enlace contenido en un

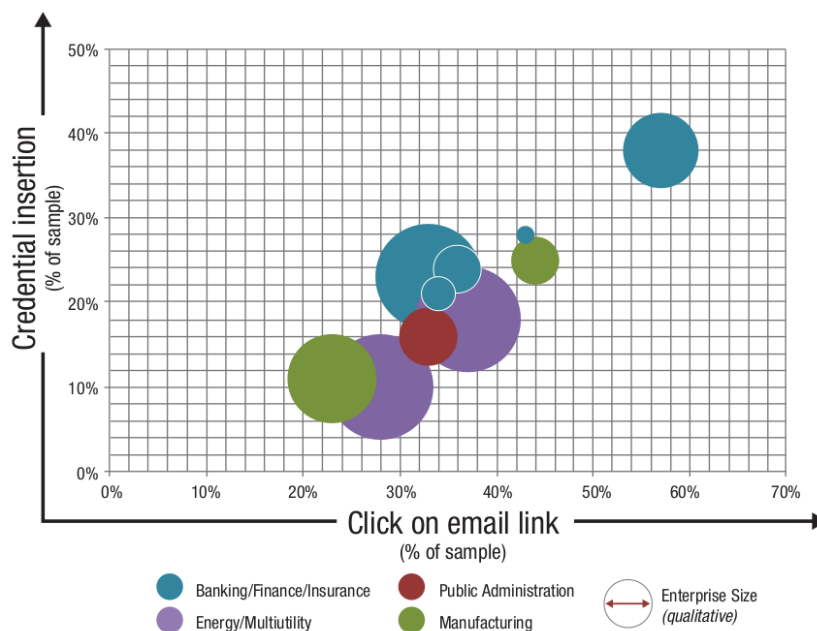


Ilustración 29: Resultados evaluaciones. Fuente: Cefriel

En estas evaluaciones, un empleado de cada tres (el 34%) siguió el enlace contenido en un

correo electrónico de phishing, y uno de cada cinco (el 21%) también insertó las credenciales de la compañía en el formulario del sitio web.

Según los autores del estudio, estos resultados son aún más impresionantes cuando se correlacionan teniendo en cuenta el factor tiempo. Según estos resultados, una campaña de phishing se caracteriza por un comportamiento impulsivo del empleado que provoca un rápido crecimiento de la tasa de éxito en las primeras fases, alcanzando una tasa efectiva del 50% en solo 20 minutos. Eso significa que el marco de tiempo disponible para una reacción efectiva del departamento de seguridad TIC es bastante breve. Especialmente en las grandes empresas, parece haber una falta de procesos formalizados que permitan aplicar contramedidas basadas en los informes de los usuarios y, con frecuencia, un nivel bajo de conocimiento del empleado con respecto a cómo informar un incidente de seguridad.

Otro punto interesante que resaltan los autores es que todos los empleados estaban sujetos a esta amenaza. No parece haber ninguna diferencia particular al analizar los resultados según la edad, la ubicación, el departamento o el rol. Incluso la gerencia y los ejecutivos a menudo son bastante vulnerables. En general, observaron que cuanto mayor es el rol en la empresa, menor es la exposición, pero el porcentaje de gerentes engañados no es marginal, lo que plantea algunos problemas que deben considerarse desde una perspectiva de gestión de riesgos.

Finalmente, a través de las técnicas de localización del rastro digital, se recopiló información sobre la configuración de seguridad de los dispositivos utilizados para explorar sitios web (las estaciones de trabajo de los usuarios), y se encontraron vulnerabilidades que introducen un alto nivel de exposición a ataques tecnológicos. Esto significa que usando una combinación de "exploits slapdash", código de malware y técnicas de ofuscación personalizadas (aunque simples), es posible eludir las contramedidas tecnológicas dentro de una empresa y obtener un acceso privilegiado a la red interna, exactamente el objetivo principal de los ciberataques modernos.

### 8.3.5 Prueba de intervenciones frente a la amenaza de la ingeniería social

En la biblioteca oficial de la UOC, ProQuest, consta un artículo titulado "A test of interventions for security threats from social engineering", extraído de la revista digital "Information Management & Computer Security", vol. 16, edición 5, año 2008 y cuyo autor es Michael Workman.

Tiene como objetivo comparar la eficacia de los protocolos recomendados frente a la ingeniería social, basándose en la teoría que usa factores de control de amenaza. Se trata de un estudio empírico para analizar las razones por las que las personas pueden verse afectadas o no por la ingeniería social.

Según cuenta el autor, se realizó un análisis factorial confirmatorio de un modelo de control de amenazas, seguido de una evaluación aleatoria de los efectos del tratamiento utilizando el modelo. Los datos se recopilaron mediante un cuestionario que contenía factores antecedentes y se observaron muestras de comportamientos de ingeniería social en el ámbito de la seguridad. Se constató que la evaluación de la amenaza (sospecha), el compromiso, la confianza y la obediencia a la autoridad eran indicadores sólidos del éxito

de la amenaza de ingeniería social, y que la eficacia del tratamiento dependía de qué factores resaltaban más en cada persona.

Este estudio encontró que el castigo como elemento de disuasión, era más beneficioso en las amenazas de ingeniería social para los empleados con mayor susceptibilidad al miedo, receptivos a figuras de autoridad; y la capacitación en ingeniería social era más beneficiosa para aquellos que tenían mayores niveles de compromiso y tendencias de confianza en los demás.

La formación no afectó el comportamiento en relación con las percepciones de gravedad y probabilidad de amenazas de ingeniería social, por tanto no predispone a los empleados a aumentar sus cautelas frente a posibles señuelos.

Ninguna de las medidas propuestas para tratar los riesgos que supone la amenaza de ingeniería social afectó a las percepciones de vulnerabilidad o gravedad de dicha amenaza. Al parecer, al menos según este estudio, las personas perciben que la ingeniería social plantea un peligro significativo y presente, independientemente de la formación que pueda ayudarles a prevenirlo.

La formación ética no tuvo impacto en el comportamiento frente a la ingeniería social en este estudio. Otra investigación (Calluzzo<sup>36</sup> y Cante, 2004; Simpson et al.<sup>37</sup>, 1994) ha llegado a conclusiones similares sobre la formación ética en otros contextos. Sin embargo, si bien este estudio sugiere que la formación ética puede no ser efectiva para ayudar a las personas a enfrentar de manera proactiva las amenazas de la ingeniería social, el autor reconoce esto como una medida productiva. Algunas investigaciones (Harrington<sup>38</sup>, 1996; Workman y Gathegi<sup>39</sup>, 2007) han demostrado que la formación ética puede ser útil para corregir comportamientos contraproducentes, como hacer trampas o incumplir normas internacionales, como robar software.

Aunque resulta evidente, la recomendación principal que emana de este estudio, dirigida a la Dirección, es que debe inculcarse a las personas el sentido de la conducta ética y de la responsabilidad, primando aquellas dignas de confianza en los procesos de selección y de evaluación del desempeño.

Finalmente, abordando el tema del miedo, se deben establecer políticas de seguridad corporativa que contemplen la clasificación de la información y las circunstancias bajo las cuales se puede divulgar información sensible. Las políticas también deben incluir los roles y responsabilidades de seguridad, los procesos y la obligación de informar sobre los incidentes sospechosos para que las personas tengan claro cómo actuar y a quien dirigirse.

---

36 Calluzzo, V.J. and Cante, C.J. (2004), "Ethics in information technology and software use", Journal of Business Ethics, Vol. 51 No. 3, pp. 301-12.

37 Simpson, P.M., Banerjee, D. and Simpson, C.L. (1994), "Softlifting: a model of motivating factors", Journal of Business Ethics, Vol. 13, pp. 431-8.

38 Harrington, S.J. (1996), "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions", MIS Quarterly, Vol. 20, pp. 257-8.

39 Workman, M. and Gathegi, J. (2007), "Punishment and ethics deterrents: a study of insider security contravention", Journal of the American Society of Information Science and Technology, Vol. 58, pp. 212-22.

### 8.3.6 ONTSI - Ciberseguridad y Confianza en los hogares españoles

El presente TFM no podía pasar por alto la opinión ciudadana, la sensación de seguridad de los "usuarios de a pie" de tecnologías de la información e internet, recabada de manera oficial por un órgano adscrito a la entidad pública empresarial Red.es. El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) presenta<sup>40</sup> una nueva oleada del Estudio sobre la Ciberseguridad y Confianza en los hogares españoles, publicado en octubre de 2017.

Ciertamente no contiene una aproximación desde el específico enfoque de la ingeniería social, pero no deja de ser un "termómetro" global respecto de la información relativa al estado de la ciberseguridad en los hogares. Recordemos que aunque el ciudadano, visto al margen de su actividad y contexto profesional, puede no ser en sí mismo objetivo de la ingeniería social; no es menos cierto que si es un medio, o mejor dicho, sus dispositivos pueden ser recursos muy apetecibles para un atacante.

El estudio analiza la adopción de medidas de seguridad y el nivel de incidencia de situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que la población tiene en Internet. Para ello se ha llevado a cabo un proceso de recogida de información basado en dos fuentes, la primera fue un cuestionario online a 3.665 hogares, y la segunda, el software Pinkerton instalado en 2.743 PC's y 922 dispositivos Android (tanto smartphones como tabletas). De esta forma se ha podido contrastar la información declarada de los cuestionarios con los datos reales recogidos por el software.

El informe sobre el estudio es extenso, 78 páginas donde en primer lugar se introduce el estudio, en segundo lugar se habla sobre las medidas de seguridad, en tercer lugar se hace mención a los hábitos de comportamiento en la navegación y usos de internet, en cuarto lugar se tratan los incidentes de seguridad, en quinto lugar se muestran las consecuencias de tales incidentes y la reacción de los usuarios, en sexto lugar se analiza la confianza en el ámbito digital en los hogares españoles, y finalmente en séptimo lugar, se redactan las conclusiones. En la siguiente imagen se puede apreciar como el informe se hace eco de la ingeniería social cuando enumera las conclusiones del mismo:



#### Conclusiones



La **ingeniería social** es otro vector utilizado por el malware. Son típicos los casos de ficheros adjuntos en correos que simulan ser fotos, documentos, facturas, multas, o el que cada año intenta suplantar a la Agencia Tributaria aprovechando la campaña de la Renta [9][10], etc. Pero el correo electrónico no es el único medio utilizado, también es bastante común el uso de redes sociales, programas de mensajería instantánea, anuncios en páginas web, etc.

7

40 <http://www.ontsi.red.es/ontsi/es/content/ciberseguridad-y-confianza-en-los-hogares-esp%C3%B1oles-octubre-2017>

Las principales conclusiones del estudio en el primer semestre de 2017, según consta en la propia web de la ONTSI, son:

- La ciberconfianza alcanza un valor mínimo histórico en el primer semestre de 2017: el 39,9 % de los usuarios tienen mucha o bastante confianza en Internet. Este dato posiblemente se halle condicionado por la cantidad de noticias relacionadas con incidencias de seguridad de que se han hecho eco los medios de comunicación.
- Aun así dos tercios (66,6 %) de los internautas consideran su equipo razonablemente protegido y la valoración de Internet como cada día más seguro se mantiene en el 42,6 % de las declaraciones.
- A pesar de que las infecciones de malware representan el riesgo en Internet más valorado por los usuarios (81,9 %), dichas infecciones siguen ocurriendo y pasando desapercibidas. Así, el 53,2 % de ordenadores españoles y el 23,6 % de dispositivos Android presentan malware sin que sus usuarios se percatasen (el total de infecciones es del 65,6 % y 26,6 % respectivamente)

## 8.4 Brechas de seguridad

### 8.4.1 La ICANN fue objeto de un ataque de spear phishing<sup>41</sup>

La ICANN<sup>42</sup> detectó e investigó una intrusión en sus sistemas que a su juicio parecía provenir de un ataque de "spear phishing", iniciado a finales de noviembre de 2014. El ataque consistió en varios mensajes dirigidos a miembros propios de la corporación, redactados en forma tal que parecían provenir de su propio dominio. Como resultado del ataque, se vieron comprometidas las credenciales de correo electrónico de varios profesionales de la ICANN.

A principios de diciembre de 2014, se descubrió que las credenciales comprometidas habían generado acceso no autorizados a los buzones de correo correspondientes además de a los siguientes sistemas de la ICANN:

- El Sistema Centralizado de Datos de Zona<sup>43</sup> (CZDS), donde el atacante obtuvo acceso a todos los archivos administrativos incluyendo las copias de los archivos de zona en el sistema, junto con la información ingresada por los usuarios (nombre, dirección de correo postal, dirección de correo electrónico, número de fax, número de teléfono, nombre de usuario y hash de la contraseña).
- El espacio Wiki del Comité Asesor Gubernamental<sup>44</sup> (GAC) en la ICANN, donde se visualizó información pública, la página de inicio de la sección exclusiva para miembros y la página del perfil de usuario de una persona.

También se logró el acceso no autorizado a cuentas de usuarios de otros dos sistemas: el blog<sup>45</sup> de la ICANN y el portal de información de WHOIS<sup>46</sup>.

41 <https://www.icann.org/news/announcement-2-2014-12-16-es>

42 Internet Corporation for Assigned Names and Numbers

43 [czds.icann.org](http://czds.icann.org)

44 Governmental Advisory Committee ([gacweb.icann.org](http://gacweb.icann.org))

45 [blog.icann.org](http://blog.icann.org)

46 [whois.icann.org](http://whois.icann.org)

### 8.4.2 Carbanak<sup>47</sup>

Carbanak es una APT dirigida principalmente a instituciones financieras que según cuenta la empresa rusa/británica Cyber Crime Kaspersky Lab, fue descubierta en 2014 por ella. Según los investigadores, el malware se introdujo en sus objetivos a través de correos electrónicos de phishing. Las cifras que se manejan sobre las cantidades de dinero que se pudieron robar a los bancos y clientes privados oscilan entre los 500 millones y el billón de dólares.

Carbanak es el nombre que los investigadores le han otorgado a la APT porque está basada en Carberp y el nombre del archivo de configuración es "anak.cfg". La principal diferencia con otros ataques APT es que los atacantes no persiguen datos sino dinero.

Los delincuentes pudieron manipular su acceso a las redes bancarias respectivas para robar el dinero de varias maneras. Una de ellas permitía enviar remotamente instrucciones a los cajeros automáticos para que dispensaran efectivo, luego las "mulas" recogerían el dinero y lo transferirían a través de la red SWIFT a las cuentas de los delincuentes. El grupo Carbanak llegó a alterar las bases de datos y aumentar los saldos de las cuentas existentes, embolsándose la diferencia sin el conocimiento del titular cuyo saldo original permanecía intacto.

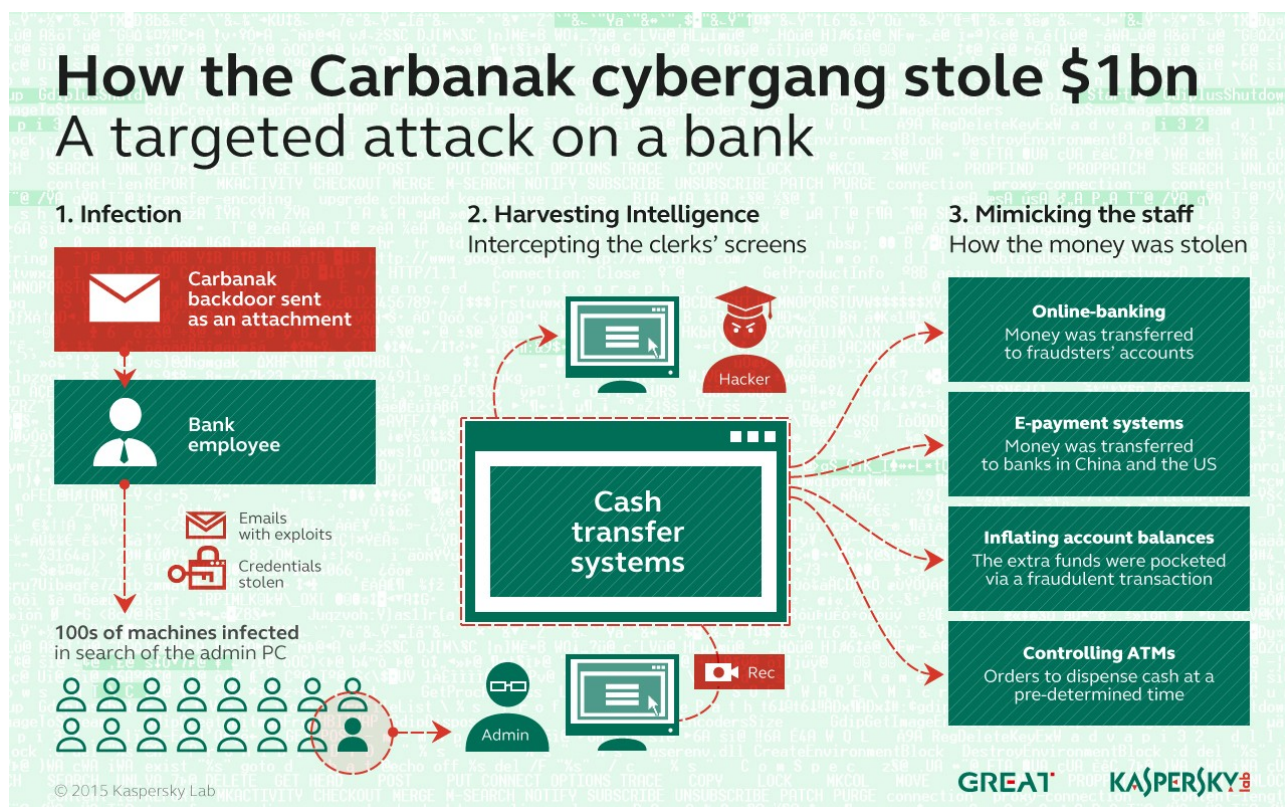


Ilustración 30: ¿Cómo robó 1 billón de dólares el cibergroupo Carbanak? Un ataque dirigido a un banco

47 <https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/>

### 8.4.3 Otras brechas conocidas

Muchos virus famosos como el “*I love you*”, el troyano *Neverquest* o *Blaster* utilizan la ingeniería social para extenderse por millones de ordenadores. Otros timos, como la *estafa de mensajes premium a través de Whatsapp*, también utilizan este método para ganarse la confianza de la víctima.

#### I love you<sup>48</sup>

ILoveYou (o VBS/LoveLetter) es un virus escrito en VBScript. En mayo de 2000 infectó aproximadamente 50 millones de computadores provocando pérdidas de más de 5.500 millones de dólares.

VBS/LoveLetter llega al usuario en un e-mail que tiene por Asunto: 'ILOVEYOU' e incluye un fichero llamado 'LOVE-LETTER-FOR-YOU.TXT.vbs'.

#### Neverquest<sup>49</sup>

Neverquest es un nuevo troyano bancario que infecta a los ordenadores a través de las redes sociales, los emails y los protocolos de envío de archivos. Puede reconocer centenares de páginas web de bancos u otros servicios financieros. Cuando el usuario intenta acceder con su ordenador infectado a una de estas websites, el troyano se activa automáticamente, robando el nombre de usuario y la contraseña.

Neverquest también ha sido diseñado para recopilar datos cuando el usuario visita otras páginas no relacionadas con las finanzas, pero que pueden ser útiles para el objetivo: Google, Yahoo, Amazon AWS, Facebook, Twitter y Skype, entre otras.

## 9 Estrategias de gestión de riesgos

No es objeto del presente TFM realizar un alegato sobre los riesgos de la información y los procesos, metodologías y buenas prácticas de gestión existentes (MAGERIT, ISO 31000, ISO 27001, ISO 27005,...). Por contra, centraremos el presente capítulo en las distintas formas que una organización puede emplear para combatir los riesgos derivados de la ingeniería social como amenaza para la seguridad de la información.

El concepto de **ciberriesgo** o **riesgo cibernético** proviene de la amenaza continua y a escala industrial sobre los activos digitales, las operaciones y la información corporativa, por parte de terceros. Para entender mejor el contexto actual, es necesario conocer los principales riesgos a los que se exponen las organizaciones, donde la ingeniería social ocupa un importante papel como una de las principales técnicas de ataque:

48 <https://es.wikipedia.org/wiki/ILoveYou>

49 <https://www.kaspersky.es/blog/neverquest-ataca-a-las-cuentas-bancarias-online/1947/>

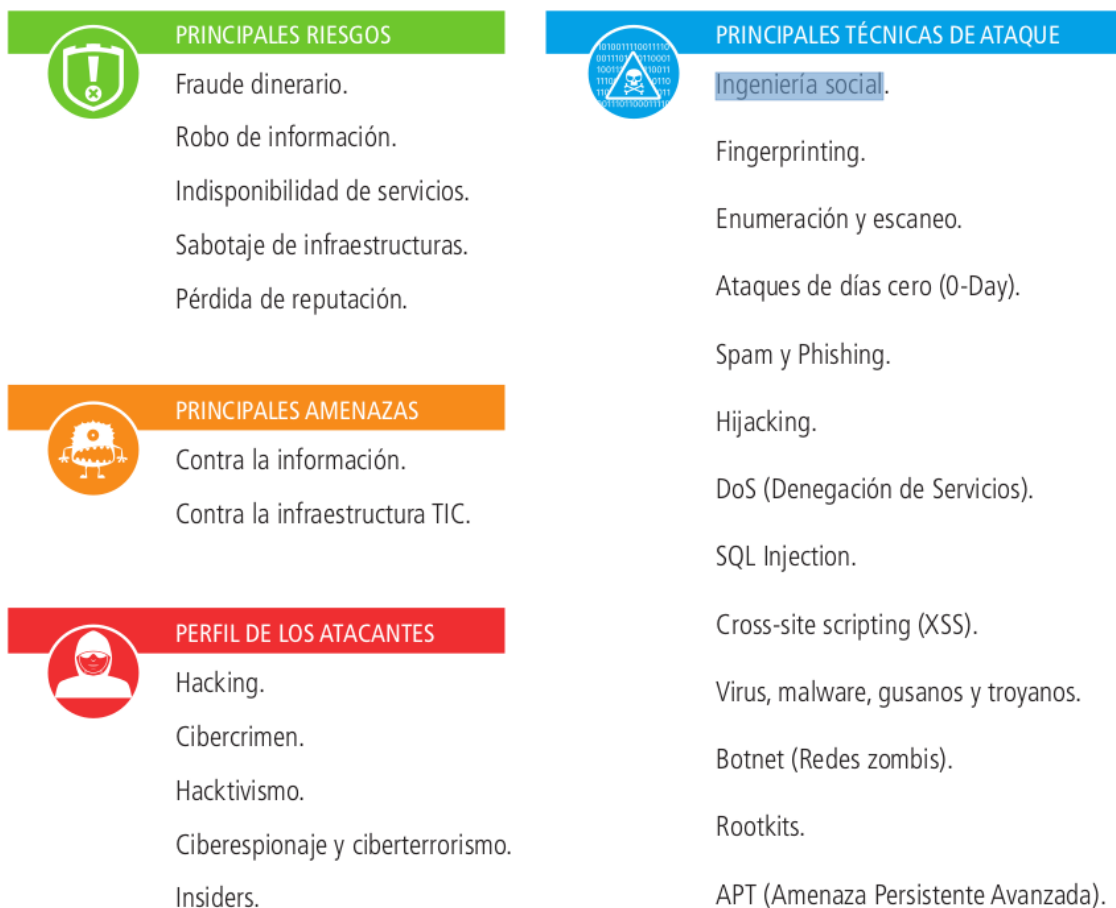


Ilustración 31: Ciberseguridad. Una guía de supervisión. Instituto de Auditores Internos

En los siguientes apartados trataremos algunas opciones de tratamiento de los riesgos derivados de la ingeniería social como amenaza para la seguridad de la información, cuyo orden de aparición no debe entenderse como un criterio de priorización de cara a su utilidad para la organización.

## 9.1 Especializar a los profesionales de ciberseguridad

El marco de trabajo en personal de ciberseguridad NICE<sup>50</sup> (Marco NICE) ayuda a identificar, reclutar, desarrollar y retener el talento en ciberseguridad. Es un recurso a partir del cual las organizaciones pueden desarrollar procedimientos o herramientas que satisfagan sus necesidades para definir u ofrecer orientación sobre los diferentes aspectos del desarrollo, planificación, capacitación y educación de los profesionales.

Esta publicación es útil como referencia fundamental para ayudar a definir las habilidades del personal según las necesidades en ciberseguridad de la organización. Proporciona a las organizaciones un léxico común y consistente que categoriza y describe el trabajo en

50 National Initiative for Cybersecurity Education



ciberseguridad por categoría, área de especialidad y rol. Proporciona un superconjunto de Conocimientos (Knowledge), Destrezas (Skills) y Habilidades (Abilities) en ciberseguridad (KSA) y Tareas para cada rol. El marco NICE promueve una comunicación sólida a nivel organizacional y sectorial como vía para la educación, capacitación y desarrollo del personal en ciberseguridad.

La publicación especial NIST 800-181 contiene una lista de destrezas - entendidas como la competencia observable para realizar un acto psicomotor aprendido-, entre las que se encuentra la identificada como S0052:

*Habilidad en el uso de técnicas de ingeniería social. (por ejemplo, phishing, cebo, tailgating, etc.).*

Además, esta destreza consta como necesaria para los siguientes roles profesionales del ámbito de la ciberseguridad: ciberinstructor y analista evaluador de vulnerabilidades.

<b>Work Role Name</b>	<b>Cyber Instructor</b>
<b>Work Role ID</b>	<b>OV-TEA-002</b>
<b>Specialty Area</b>	<b>Training, Education, and Awareness (TEA)</b>
<b>Category</b>	<b>Oversee and Govern (OV)</b>
<b>Work Role Description</b>	Develops and conducts training or education of personnel within cyber domain.
<b>Tasks</b>	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
<b>Knowledge</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
<b>Skills</b>	S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0098, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358
<b>Abilities</b>	A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Ilustración 32: KSA-T del Ciberinstructor

<b>Work Role Name</b>	<b>Vulnerability Assessment Analyst</b>
<b>Work Role ID</b>	<b>PR-VAM-001</b>
<b>Specialty Area</b>	<b>Vulnerability Assessment and Management (VAM)</b>
<b>Category</b>	<b>Protect and Defend (PR)</b>
<b>Work Role Description</b>	Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
<b>Tasks</b>	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
<b>Knowledge</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624
<b>Skills</b>	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367
<b>Abilities</b>	A0001, A0044, A0120, A0123

Ilustración 33: KSA-T del Analista Evaluador de Vulnerabilidades

## 9.2 Evaluar el factor humano

Distintos autores han tratado de documentar la necesaria evaluación del factor humano, el empleado, como paso previo a la implantación de medidas orientadas a mitigar los riesgos de seguridad de la información, considerando la trascendencia de la ingeniería social como vector de ataque en la actualidad. Por ejemplo, Tom Pendergast<sup>51</sup>, jefe de estrategia de seguridad, privacidad y cumplimiento en la compañía MediaPro<sup>52</sup>; o también Roberto Puricelli, CISM, consultor senior en seguridad de las tecnologías de las comunicaciones y la información en la compañía CEFRIEL, al que ya hemos mencionado en otra ocasión a lo largo de este trabajo. Ambos tienen artículos publicados en la revista de ISACA tratando este tema.

El señor **Pendergast** alude a investigaciones en las que se observó que los empleados hacían responsables a sus directores ejecutivos del aumento de incidentes de seguridad por la falta de inversiones y alto nivel de aceptación del riesgo; a su vez los directores responsabilizaban a sus jefes de tecnologías de la información por no adoptar medidas aplicables al elemento humano.

Pendergast enumera varias fuentes comunes en las que basarse para la elaboración de un programa de evaluación:

- varios documentos proporcionados por el Instituto Nacional de Normas y Tecnología de EEUU (NIST),
- la Organización Internacional para la estandarización (ISO),
- y el Decreto de Portabilidad de Seguro de Salud y Responsabilidad de EEUU (HIPAA),

51 <https://twitter.com/tompmmediapro>

52 <https://www.mediapro.com/>

pero afirma que solo presentan una descripción vaga de las normas y requisitos para un programa de concienciación.

En su propuesta, resulta imprescindible examinar el estado actual del conocimiento de los empleados, sus habilidades y sus actitudes sobre seguridad y privacidad (que a menudo se confunde por los empleados); debe realizarse una encuesta pre y post formación.

También considera Pendergast los datos de las herramientas de reportes de incidentes de red, como pueden ser los sistemas de la gestión de información de seguridad y gestión de eventos (SIEM) y el software de prevención de pérdida de datos (DLP). Estos datos ayudaran en entender el uso de la información y las necesidades de los empleados, facilitando la comunicación instantánea con los usuarios afectados.

Una tercera vía de evaluación del factor humano referida por este experto es la consistente en ataques simulados de ingeniería social empleando pe. técnicas de phishing. También apuesta por mejorar el rendimiento y cultura de los empleados a través de la comprensión del riesgo específico de la industria/área donde la organización desarrolla su actividad, así como el entorno único de su negocio como fuente para diseñar políticas y procedimientos adaptados a sus particulares riesgos.

Hace patente la necesidad de contar con el conjunto de factores de riesgo clave para la organización y llevar a cabo una correcta planificación para mitigarlos. Ello implica ser capaz de determinar si se está en disposición de ejecutar el plan con medios propios o por el contrario se hace necesario contratar externamente una campaña adaptiva “todo incluido” de phishing, entrenamiento, posters, juegos, animaciones y similares, a ejecutar en el transcurso de un año.

Pendergast concluye afirmando que las mejores organizaciones analizan sus factores de riesgo humano utilizando una variedad de diferentes herramientas, desarrollan un plan para cambiar el comportamiento relacionado con esos factores del riesgo, alinean sus recursos para ejecutar ese plan, y finalmente imparten educación adaptativa y flexible a las personas adecuadas, cuando y donde lo necesiten.

El señor **Puricelli** refiere que los actuales enfoques para garantizar la seguridad de las tecnologías de la información basados en la gestión de riesgos, tienden a subestimar o incluso ignorar el factor humano, tanto en los modelos de evaluación, como en las herramientas desarrolladas para aplicar esos modelos, la definición de procesos y la estructura legal. Por tanto, dado que involucrar a los empleados dentro de una evaluación de riesgos es un enfoque relativamente innovador, es de vital importancia planificar la evaluación de una manera apropiada.

En primer lugar, los departamentos de tecnologías de la información y de seguridad no son los únicos actores que deben intervenir en la definición del plan de evaluación para determinar porque las personas son objetivos y en qué grado. Por lo tanto, es necesario involucrar a todos los interesados, como al área de recursos humanos, área ético-legal y departamentos de comunicaciones, para explicar las amenazas, compartir los objetivos, definir el alcance de la evaluación y obtener un compromiso global.

Los ataques de ingeniería social suponen que un empleado es engañado para que lleve a cabo una violación de la política de seguridad definida. A pesar de que los cibercriminales sin escrúpulos intentarán engañar a los empleados, las empresas deben observar:

- Las limitaciones éticas y legales, particularmente garantizar el respeto de la relación de confianza entre el empleador y el empleado, así como evitar la invasión de la esfera personal del empleado.
- Los marcos legales laborales, que son radicalmente diferentes entre los EE.UU. y la U.E., donde los empleados están protegidos de cualquier interferencia del empleador. Por ejemplo, en Italia, la ley prohíbe a un empresario de monitorizar el comportamiento de los empleados; por lo tanto, en una evaluación, no es posible revelar los detalles de los usuarios individuales que pueden estar involucrados en un ataque.

A pesar de las limitaciones y la presencia de algún riesgo legal y ético, el interés en este tema está aumentando, incluso en Europa.

Desde 2010, la evaluación de varias grandes empresas europeas que tratan de superar las dificultades relacionadas con este tipo de actividad, ha resultado en el desarrollo de la Metodología de Evaluación de Vulnerabilidades de origen Social<sup>53</sup>. Tiene por objetivo probar el comportamiento humano contra una ejecución simulada de ataque de phishing, en la que un atacante intenta engañar a los usuarios (es decir, el personal de la empresa) para que realicen acciones que podrían poner en riesgo los activos de la compañía, por ejemplo:

1. Hacer que el empleado haga clic en un enlace dentro del correo electrónico, visitando un posible sitio web malicioso y, por lo tanto, exponiendo la organización a un ataque provocado por una infección de malware (drive-by-infection).
2. Hacer que el empleado inserte cierta información solicitada en un formulario web, pe. credenciales de la empresa.

Mediante el uso de un sitio web controlado y el seguimiento del comportamiento de los usuarios, es posible medir la tendencia de los empleados a ser víctimas de tal ataque. También es posible estimar el nivel de exposición de la empresa a ataques tecnológicos derivados de una campaña de phishing simulado, pe. identificando servicios sin parches de seguridad instalados que pueden ser explotados a través de mecanismos de rastreo de huella digital o "fingerprinting".

**Otros autores** advierten de la posibilidad de evaluar la personalidad de los empleados como mecanismo de prevención frente a potenciales ataques de ingeniería social. Recordemos que ya en el capítulo dedicado a la descripción de la ingeniería social tratamos el tema de la personalidad humana en uno de sus apartados.

Resulta evidente conocer las debilidades de un empleado una vez que éste ha sido observado, analizado y "vulnerado" por un atacante. Una organización siempre podrá reaccionar ante un incidente reconociendo con posterioridad las tendencias del empleado afectado, pero lo realmente útil sería actuar de forma proactiva (Johnston, Warkentin, McBride y Carter, 2016). Una forma de hacerlo es evaluar científicamente los tipos de personalidad y los patrones de comportamiento de las personas, tal y como se viene haciendo pe. para ubicar a un empleado en un puesto de trabajo acorde a su personalidad (Bariff y Lusk, 1977) o en un equipo de personas en busca de sinergias.

Hay varias herramientas y técnicas que se han creado a lo largo de los años para ayudar a determinar científicamente los rasgos de personalidad de los recursos humanos de una

---

53 Brenna, R.; et al.; CEFRIEL, "Social Driven Vulnerability," Technology, February 2014, [www.slideshare.net/CEFRIEL/social-driven-vulnerability-english-version](http://www.slideshare.net/CEFRIEL/social-driven-vulnerability-english-version)

organización. Una de ellas se conoce como Big Five u OCEAN (Zhuang, 2006), acrónimo inglés de los cinco rasgos principales de personalidad: Openness to experience (abierto a experiencias), Conscientiousness (meticulosidad), Extraversion (extraversión), Agreeableness (afabilidad) y Neuroticism (Neuroticismo).

Cinco grandes rasgos	Descripción del rasgo
Abierto a experiencias	Personas con mentalidad abierta, imaginación activa, preferencia por la variedad, e independencia de juicio.
Meticulosidad	Personas con conciencia compartida que tienden a distinguirse por su confiabilidad y su sentido de actitud y de responsabilidad. Tienden a ser voluntariosas, enfocadas en las tareas y orientadas a logros/resultados.
Extraversión	Personas sociables y asertivas que normalmente prefieren trabajar con otras personas.
Afabilidad	Personas que tienden a ser tolerantes, confiadas, permisivas y con capacidad para valorar y respetar las creencias y convenciones de otras personas.
Neuroticismo	Personas que pueden experimentar sentimientos negativos como inestabilidad emocional, vergüenza, culpa, pesimismo y baja autoestima.

La siguiente tabla describe cómo ciertos tipos de personalidad basados en el conjunto de rasgos OCEAN son más o menos propensos a violar la política de ciberseguridad. También tiene en cuenta otros factores, como la gravedad de la amenaza, autoeficacia, severidad de la sanción y el costo de respuesta o mitigación. Demuestra claramente la correlación entre los tipos de personalidad y la probabilidad de ser víctimas de un ataque de ingeniería social (Johnston, Warkentin, McBride y Carter, 2016).

Personas con MENOS probabilidad de violar la política de ciberseguridad	Personas con MÁS probabilidad de violar la política de ciberseguridad
<ul style="list-style-type: none"> <li>• Individuos abiertos con una baja sensación de eficacia personal.</li> <li>• Individuos abiertos con un bajo sentido de severidad de la amenaza.</li> <li>• Individuos abiertos con un bajo sentido de costo de respuesta.</li> <li>• Individuos concienzudos con un bajo sentido de severidad de la amenaza.</li> <li>• Individuos extrovertidos con un bajo sentido de severidad de sanción.</li> <li>• Individuos afables con un bajo sentido de eficacia personal.</li> <li>• Individuos afables con un bajo sentido</li> </ul>	<ul style="list-style-type: none"> <li>• Individuos abiertos en general.</li> <li>• Individuos abiertos con un bajo sentido de la severidad de sanción.</li> <li>• Individuos concienzudos con un bajo sentido de eficacia de respuesta.</li> <li>• Individuos extrovertidos con un bajo sentido de severidad de amenaza.</li> <li>• Individuos extrovertidas con un bajo sentido de vulnerabilidad a las amenazas.</li> <li>• Individuos introvertidos con un bajo sentido de costo de respuesta.</li> <li>• Individuos con un bajo sentido de</li> </ul>

<p>de severidad de sanción.</p> <ul style="list-style-type: none"> <li>• Individuos neuróticos con un bajo sentido de eficiencia personal.</li> <li>• Individuos neuróticos con un bajo sentido de severidad de sanción.</li> </ul>	<p>certeza de sanción.</p> <ul style="list-style-type: none"> <li>• Individuos neuróticos con un bajo sentido de certeza de sanción.</li> </ul>
---	---

**COBIT® 5** también considera los factores humanos y el comportamiento como habilitadores clave (aunque a menudo subestimados) para diseñar un enfoque holístico para GEIT<sup>54</sup>. Las evaluaciones dirigidas al factor humano agregan una métrica efectiva para medir el nivel de logro del objetivo de seguridad de la información. Es esencial establecer buenas prácticas con el fin de corregir, fomentar y mantener la cultura de seguridad en toda la empresa.

### 9.3 La transferencia del ciberriesgo

Transferir el riesgo a un tercero es una de las cuatro prácticas de tratamiento del mismo reconocidas por los estándares internacionales como ISO 27001, las otras son mitigarlo, asumirlo o eliminarlo. La forma habitual de transferencia de riesgo es a través de la contratación de un seguro para el activo/s en cuestión, y otra posibilidad sería subcontratar el servicio concreto afectado por el riesgo. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

Actualmente, las encuestas afirman que en el mercado actual el daño a la reputación y a la propia marca son considerados los principales riesgos para muchas compañías y startups, ya que consecuentemente la cuenta de resultados puede verse gravemente afectada.

Además, el marco económico y los cambios de normativas que obligan a bruscas adaptaciones, son también una preocupaciones importante de empresarios y profesionales.

La siguiente figura muestra la relación impacto/probabilidad de los ciberataques, dentro de los riesgos globales considerados por el World Economic Forum. Como puede observarse, el WEF sitúa a este riesgo entre los más significativos.



54 GEIT: Governance of Enterprise IT

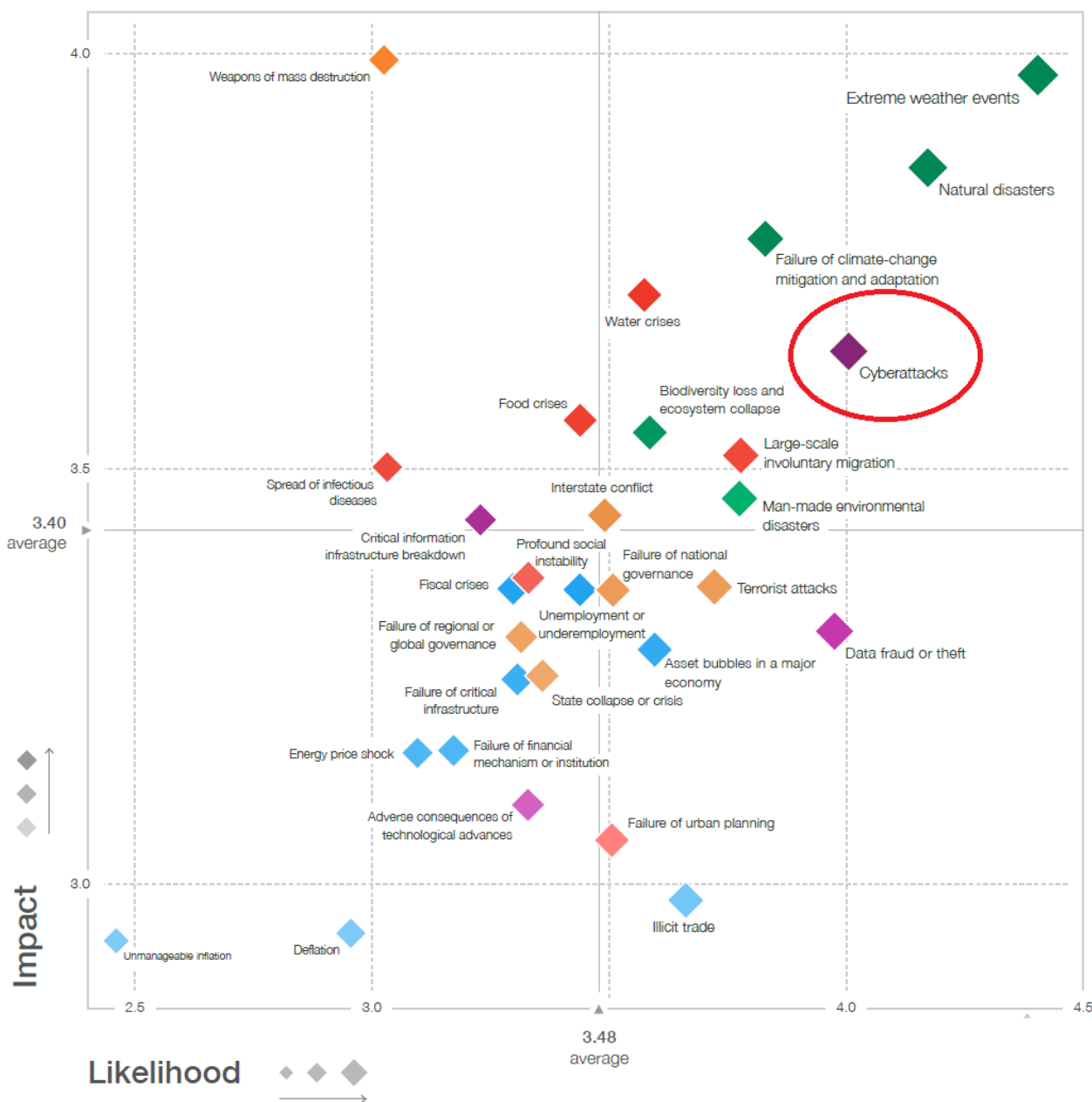


Ilustración 34: CCN-CERT IA-09-18 Ciberamenazas y tendencias 2018

Algunas aseguradoras están empezando a ofrecer servicios para dar cobertura a los ciberriesgos. Este es el caso de Thiber<sup>55</sup> que presentó en abril de 2016 un amplio documento<sup>56</sup> con el objetivo de concienciar a grandes y pequeñas empresas de que los daños causados por los ciberriesgos han venido para quedarse. En él se presenta un concepto de ciberseguro frente al riesgo tecnológico para el mercado español, describiendo sus ventajas y resaltando las múltiples barreras por las que el producto, a

55 <http://www.thiber.org/2016/04/29/ciberseguros-la-ultima-linea-de-defensa-contra-amenazas-ciberneticas-en-espana/>

56 <http://www.thiber.org/ciberseguros.pdf>

pesar de estar en crecimiento, no llega a consolidarse como un punto obligatorio dentro del plan de empresa.

Los ciberseguros representarían una capa de protección extra que debería mejorar sustancialmente la salud de la empresa y su propia gestión. El documento centra la atención en cómo debe resolverse la transferencia de los riesgos entre la empresa y el asegurador (o reasegurador).



\* En función del asegurador / negociación

Ilustración 35: Cobertura de un producto típico de ciberriesgos. Fuente: AON

## 10 Pautas para combatir la ingeniería social.

En 2008, Workman M., Bommer, W.H. and Straub, D.<sup>57</sup>, ya indicaron que no es suficiente con la aplicación de medidas de seguridad automatizadas para solucionar el problema de la ingeniería social, aunque estas sean obligatorias para los usuarios. Las principales razones que establecían eran financieras (son muy costosas), situacionales (distintas necesidades en distintos momentos), tecnológicas (incompatibilidades) y culturales.

Recientemente, el 15 de enero de 2018, la empresa de seguridad centrada en los datos Digital Guardian, publicaba en su web un oportuno artículo dedicado a la ingeniería social titulado "Ataques de ingeniería social: técnicas comunes y cómo prevenir un ataque"<sup>58</sup>. En él, 28 expertos en seguridad de la información opinaban sobre cómo prevenir los ataques de ingeniería social más comunes, obviamente acercando las soluciones de sus

57 Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: an empirical test of the threat control model", Journal of Computers in Human Behavior, Vol. 24 No. 6, pp. 2799-816.

58 <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack>



compañías a los lectores, aunque no por ello menos interesante. Resultaría excesivamente extenso hacer mención, inclusive de manera resumida, a cada una de las intervenciones; no obstante, baste mencionar que entre los expertos se encontraba Kevin Mitnick<sup>59</sup>, "el hacker más famoso del mundo".

Organizaciones europeas importantes como ENISA, cuenta en su web con un glosario para el tema "CSIRTs in Europe" que alberga una resumida entrada para el concepto "Ingeniería Social<sup>60</sup>". En ella se aportan unas breves recomendaciones que pueden servir de introducción a este capítulo:

*Cualquier organización debe identificar sus activos críticos e implementar las políticas y protocolos de seguridad adecuados. Cuando sea necesario, estos deben ser reforzados mediante el uso de la tecnología.*

*Sin embargo, la contramedida más eficiente para los ataques de ingeniería social sigue siendo de sentido común. En esta línea, ENISA recomienda lo siguiente:*

- *campañas frecuentes de sensibilización: carteles, presentaciones, correos electrónicos, notas informativas;*
- *formación del personal y ejercicios prácticos;*
- *pruebas de penetración para determinar la susceptibilidad de una organización a ataques de ingeniería social, informando y actuando sobre los resultados.*

Este capítulo vamos a tratarlo con distintos enfoques, dependiendo del público objetivo, de ahí los siguientes apartados.

## 10.1 Pautas para la víctima potencial

Europol cuenta con una excelente infografía<sup>61</sup> para situaciones en las que los cargos intermedios de servicios financieros o de compras son el objetivo principal de las estafas de fraude dirigidas a los empleados. Con pérdidas que en algunos casos alcanzan varios millones de euros, el coste profesional y humano de estos crímenes es inmenso. Los empleados deben ser conocedores de las técnicas empleadas por los atacantes, de las señales que avisan de potenciales ataques y del comportamiento que deben seguir para hacer frente a los estafadores. Por tanto, el mensaje que debe trasladarse a un empleado para evitar convertirse en una víctima de la ingeniería social debe darle a conocer los siguientes elementos fundamentales.

<sup>59</sup> <https://www.mitnicksecurity.com/>

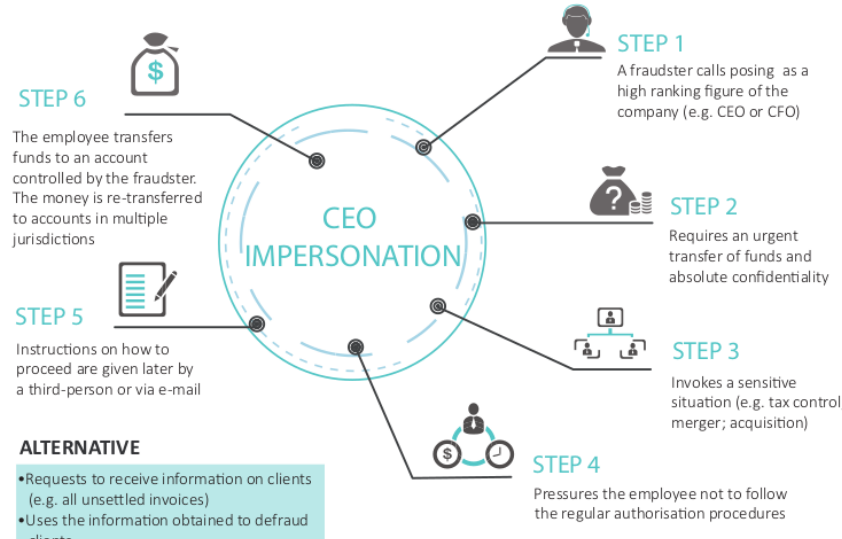
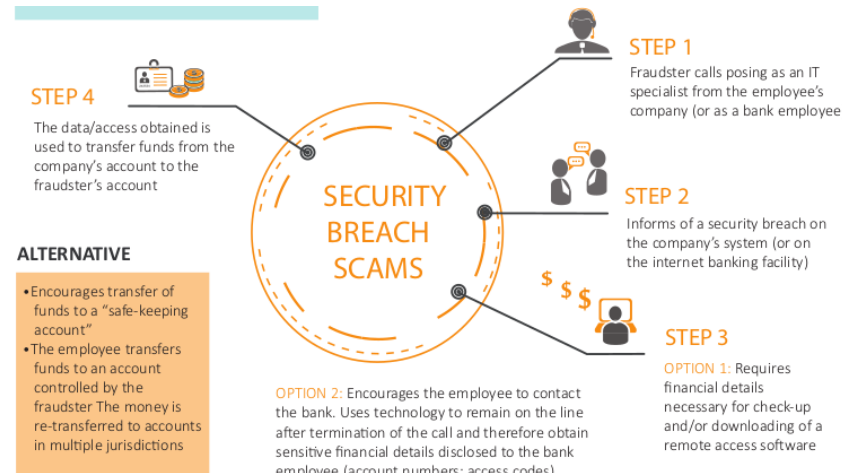
<sup>60</sup> <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering>

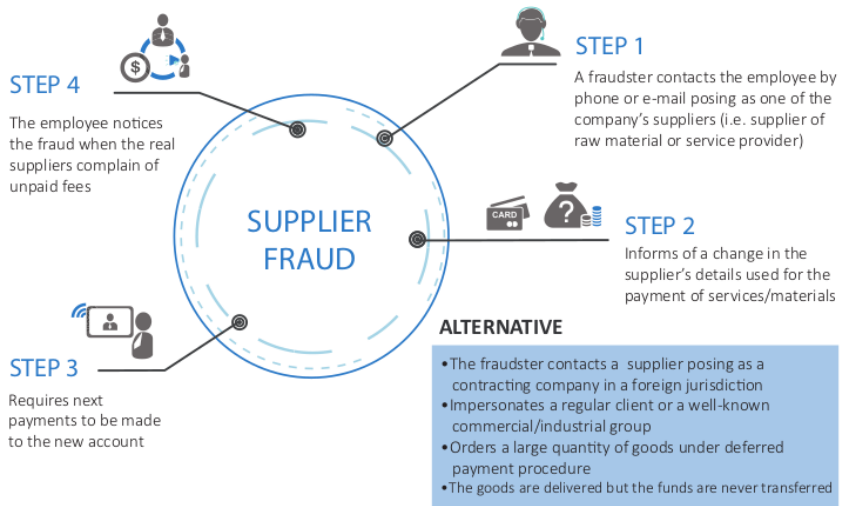
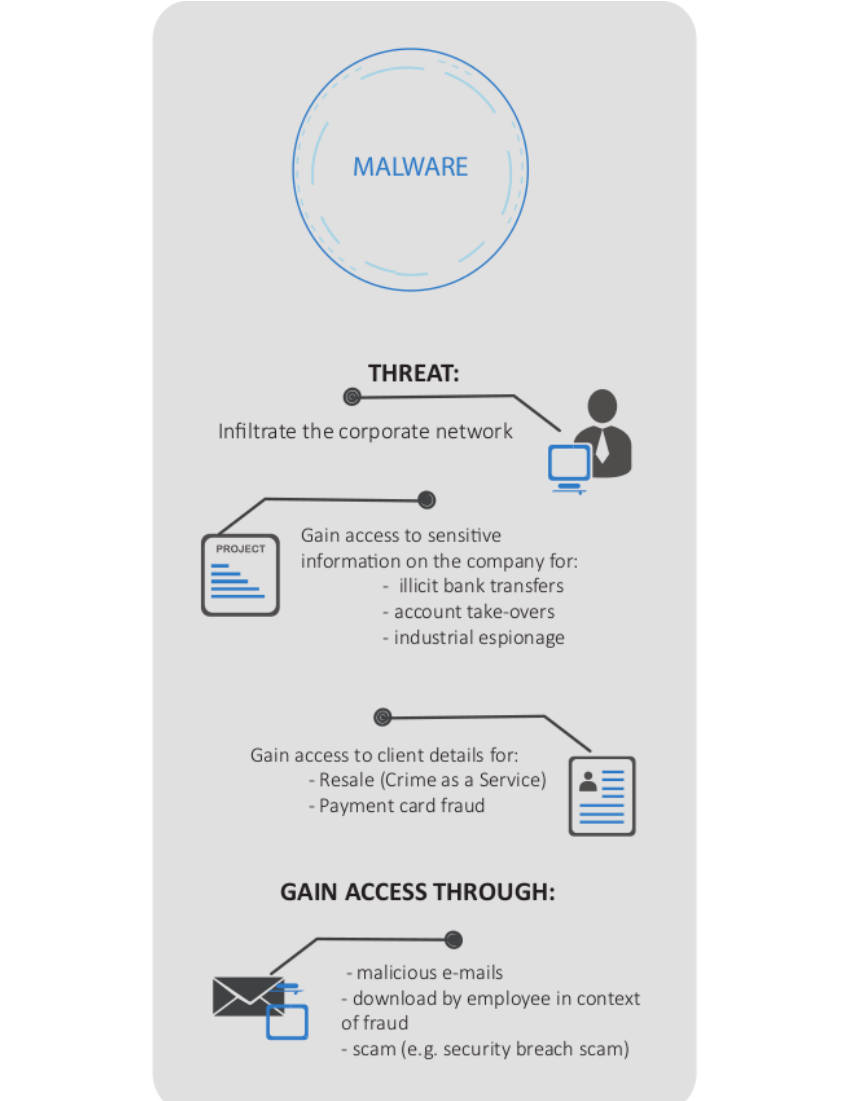
<sup>61</sup> <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees>

### 10.1.1 Conoce las formas de ocultar la identidad que usan los estafadores

- Usan documentos falsificados con el logotipo / las firmas legítimas de la compañía obtenidos en línea.
- Usan direcciones de correo electrónico que imitan a las reales.
- Disfrazan el origen de las llamadas telefónicas a través de aplicaciones que falsifican la identidad del llamante, mostrando el número oficial del servicio o de la persona a la que suplantan.
- Usan VOIP y servidores proxy para reducir los riesgos de detección.
- Utilizan los servicios de centros de llamadas ilegales con sede fuera de la UE.

### 10.1.2 Conoce los tipos de estafas y sus señales:

Estafas	Señales
 <p><b>CEO IMPERSONATION</b></p> <p><b>STEP 1</b> A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)</p> <p><b>STEP 2</b> Requires an urgent transfer of funds and absolute confidentiality</p> <p><b>STEP 3</b> Invokes a sensitive situation (e.g. tax control; merger; acquisition)</p> <p><b>STEP 4</b> Pressures the employee not to follow the regular authorisation procedures</p> <p><b>STEP 5</b> Instructions on how to proceed are given later by a third-person or via e-mail</p> <p><b>STEP 6</b> The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions</p> <p><b>ALTERNATIVE</b></p> <ul style="list-style-type: none"> <li>• Requests to receive information on clients (e.g. all unsettled invoices)</li> <li>• Uses the information obtained to defraud clients</li> </ul>	<p><b>SUPLANTACIÓN DE ALTO CARGO</b></p> <ul style="list-style-type: none"> <li>• Contacto directo de un alto funcionario con el que normalmente no estás en contacto.</li> <li>• Solicitud inusual en contradicción con los procedimientos internos.</li> <li>• Solicitud de confidencialidad absoluta.</li> <li>• Amenazas o adulaciones inusuales / promesas de recompensa.</li> </ul>
 <p><b>SECURITY BREACH SCAMS</b></p> <p><b>STEP 1</b> Fraudster calls posing as an IT specialist from the employee's company (or as a bank employee)</p> <p><b>STEP 2</b> Informs of a security breach on the company's system (or on the internet banking facility)</p> <p><b>STEP 3</b> <b>OPTION 1:</b> Requires financial details necessary for check-up and/or downloading of a remote access software</p> <p><b>STEP 4</b> The data/access obtained is used to transfer funds from the company's account to the fraudster's account</p> <p><b>OPTION 2:</b> Encourages the employee to contact the bank. Uses technology to remain on the line after termination of the call and therefore obtain sensitive financial details disclosed to the bank employee (account numbers; access codes)</p> <p><b>ALTERNATIVE</b></p> <ul style="list-style-type: none"> <li>• Encourages transfer of funds to a "safe-keeping account"</li> <li>• The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions</li> </ul>	<p><b>ESTAFA DE VIOLACIÓN DE SEGURIDAD</b></p> <ul style="list-style-type: none"> <li>• Uso de un tono particularmente alarmante por parte de un oficial de TI / seguridad.</li> <li>• Solicitud para descargar software externo (por ejemplo, software de acceso remoto).</li> <li>• Oferta de una cuenta de custodia.</li> </ul>

Estafas	Señales
 <p><b>SUPPLIER FRAUD</b></p> <p><b>STEP 1</b> A fraudster contacts the employee by phone or e-mail posing as one of the company's suppliers (i.e. supplier of raw material or service provider)</p> <p><b>STEP 2</b> Informs of a change in the supplier's details used for the payment of services/materials</p> <p><b>STEP 3</b> Requires next payments to be made to the new account</p> <p><b>STEP 4</b> The employee notices the fraud when the real suppliers complain of unpaid fees</p> <p><b>ALTERNATIVE</b></p> <ul style="list-style-type: none"> <li>• The fraudster contacts a supplier posing as a contracting company in a foreign jurisdiction</li> <li>• Impersonates a regular client or a well-known commercial/industrial group</li> <li>• Orders a large quantity of goods under deferred payment procedure</li> <li>• The goods are delivered but the funds are never transferred</li> </ul>	<p><b>FRAUDE DE PROVEEDOR</b></p> <ul style="list-style-type: none"> <li>• Cambio repentino en los detalles de contacto / pago de un proveedor internacional (normalmente se anunciaría unas semanas / meses por adelantado).</li> <li>• Cambio que ocurre poco después de que se aprobara una orden importante o poco antes de la fecha límite para el pago.</li> </ul>
 <p><b>MALWARE</b></p> <p><b>THREAT:</b> Infiltrate the corporate network</p> <p>Gain access to sensitive information on the company for:</p> <ul style="list-style-type: none"> <li>- illicit bank transfers</li> <li>- account take-overs</li> <li>- industrial espionage</li> </ul> <p>Gain access to client details for:</p> <ul style="list-style-type: none"> <li>- Resale (Crime as a Service)</li> <li>- Payment card fraud</li> </ul> <p><b>GAIN ACCESS THROUGH:</b></p> <ul style="list-style-type: none"> <li>- malicious e-mails</li> <li>- download by employee in context of fraud</li> <li>- scam (e.g. security breach scam)</li> </ul>	<p><b>MALWARE</b></p> <ul style="list-style-type: none"> <li>• Correos electrónicos no solicitados con saludos genéricos.</li> <li>• Correo electrónico no solicitado que contiene enlaces / URL sospechosos.</li> </ul>

Estafas	Señales
<b>SEÑALES COMUNES</b> <ul style="list-style-type: none"><li>• Llamada / correo electrónico no solicitado que solicita información sobre los procedimientos internos para el pago o la adquisición.</li><li>• Llamada / correo electrónico no solicitado solicitando información financiera (números de cuenta, códigos de acceso).</li><li>• Sensación de emergencia.</li><li>• Presión.</li></ul>	

### 10.1.3 Reacciona o actúa siguiendo las siguientes recomendaciones:

- Tenga en cuenta los riesgos y disemine la información dentro de su compañía.
- Tenga cuidado al usar las redes sociales: al compartir información sobre su lugar de trabajo y sus responsabilidades, aumenta los riesgos de convertirse en un objetivo.
- Evite compartir información confidencial sobre la jerarquía, seguridad o procedimientos de la compañía.
- Nunca abra enlaces sospechosos o archivos adjuntos recibidos por correo electrónico. Tenga especial cuidado cuando verifique sus buzones personales en los ordenadores de la compañía.
- Si recibe un correo electrónico o llamada sospechosa, siempre informe a su departamento de TI; ellos son los que están a cargo de tales asuntos. Pueden verificar el contenido del correo sospechoso y bloquear al remitente si es necesario.
- Siempre revise cuidadosamente las direcciones de correo electrónico cuando se trata de información delicada / transferencias de dinero. Los defraudadores a menudo usan correos de imitación donde solo un carácter difiere del original.
- Si recibe una llamada o un correo electrónico que lo alertan de una violación de seguridad, no proporcione información de inmediato ni proceda con una transferencia. Siempre comience llamando a la persona de nuevo usando un número de teléfono que se encuentre en sus propios registros o en el sitio web oficial de la compañía; no use el número proporcionado por correo o por la persona que llama. Si se contactó con usted por teléfono, vuelva a llamar usando otro teléfono (los estafadores usan la tecnología para permanecer en línea después de colgar).
- En caso de duda sobre una orden de transferencia, siempre consulte a un colega, incluso si le pidieron discreción.
- Considere asignar responsabilidad a un empleado a quien otros puedan consultar en caso de duda.
- Si un proveedor le informa sobre un cambio en los detalles de pago, contacte con él siempre para confirmar la nueva información. Tenga en cuenta que el número de correo electrónico / teléfono provisto en la factura podría haber sido modificado.
- Aplicar estrictamente los procedimientos de seguridad vigentes para pagos y adquisiciones. No se salte ningún paso y no ceda a la presión.

- Siempre contacte a la policía en caso de intento de fraude, incluso si no fue víctima de la estafa.

## 10.2 Pautas para la empresa/organización

A continuación expondremos las pautas a seguir por una organización, estructurando las mismas en seis bloques: buenas prácticas, estándares de seguridad, auditoría, medición, formación y cultura en ciberseguridad.

### 10.2.1 Buenas prácticas recomendadas

Es posible encontrar en la web determinados documentos de autor que tratan el tema de la ingeniería social orientando a las organizaciones sobre las contramedidas que deben adoptar según la técnica empleada por el atacante. Este es el caso del artículo titulado "**Social Engineering: Manipulating the Source**<sup>62</sup>", redactado por Jared Kee con el asesoramiento de Brent Deterding y ubicado en el SANS Institute InfoSec Reading Room que nos servirá de introducción del presente apartado. Las buenas prácticas recomendadas -contramedidas- se dividen en aquellas dirigidas a mitigar los ataques telefónicos, las útiles frente a los ataques en línea (email o web), las dedicadas a evitar el buceo en contenedores, aquellas orientadas a luchar contra la ingeniería social inversa y finalmente las que persiguen frenar los intentos de persuasión en persona. Dado que el autor se ha reservado todos sus derechos, animamos a realizar una rápida lectura del documento que no por antiguo (data de 2008) deja de tener vigencia.

Otros documentos públicos en formato informe, como el "**2018 Data Breach Investigations Report**<sup>63</sup>" de Verizon, contemplan capítulos específicos dedicados a los ataques de ingeniería social. Entre las recomendaciones que recoge destacan las siguientes:

- Considere que algunas personas harán clic en un archivo adjunto más rápido que Harry Turner<sup>64</sup>. Tal vez debería entregarles tabletas o portátiles con un sistema operativo que se ejecute en un espacio aislado (sandbox), permitiendo únicamente la ejecución de código firmado.
- Reduzca el impacto de un dispositivo de usuario comprometido mediante la segmentación de clientes de activos críticos, y use una autenticación fuerte para acceder a otras zonas de seguridad de su red, evitando "keyloggers". Si usa el correo electrónico en la nube, requiera un segundo factor.
- Entrene al personal de soporte y a los usuarios finales. Ponga a prueba su capacidad para detectar una campaña de ataque, identificar posibles puestos de usuario infectados, determinar la actividad del dispositivo después de un compromiso y confirmar la existencia de fuga de datos. Practique, practique y

62 <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914>

63 <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

64 [telegraph-office.com/pages/turner.html](https://www.telegraph-office.com/pages/turner.html)

practique para adquirir la habilidad de reaccionar de manera rápida y eficiente y así limitar el impacto de un phishing exitoso.

- Brinde formación específica para cada tipo de rol desempeñado por los usuarios, considerando sus privilegios o capacidades de acceso a los datos. Eduque a los empleados con acceso a los datos de otros empleados (pe. a sus declaraciones de impuestos) o con la capacidad de transferir fondos, probablemente sean objetivos. Aumente su nivel de escepticismo; no es paranoia si alguien realmente quiere obtener los datos de su organización.

Vamos a volver a hacer referencia a uno de los autores que ya hemos mencionado en capítulos anteriores, se trata de Richardus Eko y su trabajo "Social Engineering Framework". Recordemos que establecía cuatro etapas de la ingeniería social: preparación, apretón de manos, ataque y post-acción. Pues bien, su marco de trabajo también contempla una estrategia de mitigación de riesgos y seguridad que hemos decidido ubicar bajo este apartado de buenas prácticas. Él lo denomina **Marco de Trabajo para Construir "Firewalls" Humanos** y consta de tres líneas de actuación: personas y cultura, políticas y procesos, y herramientas y tecnología.

La siguiente figura ilustra y explica gráficamente cada una de ellas:

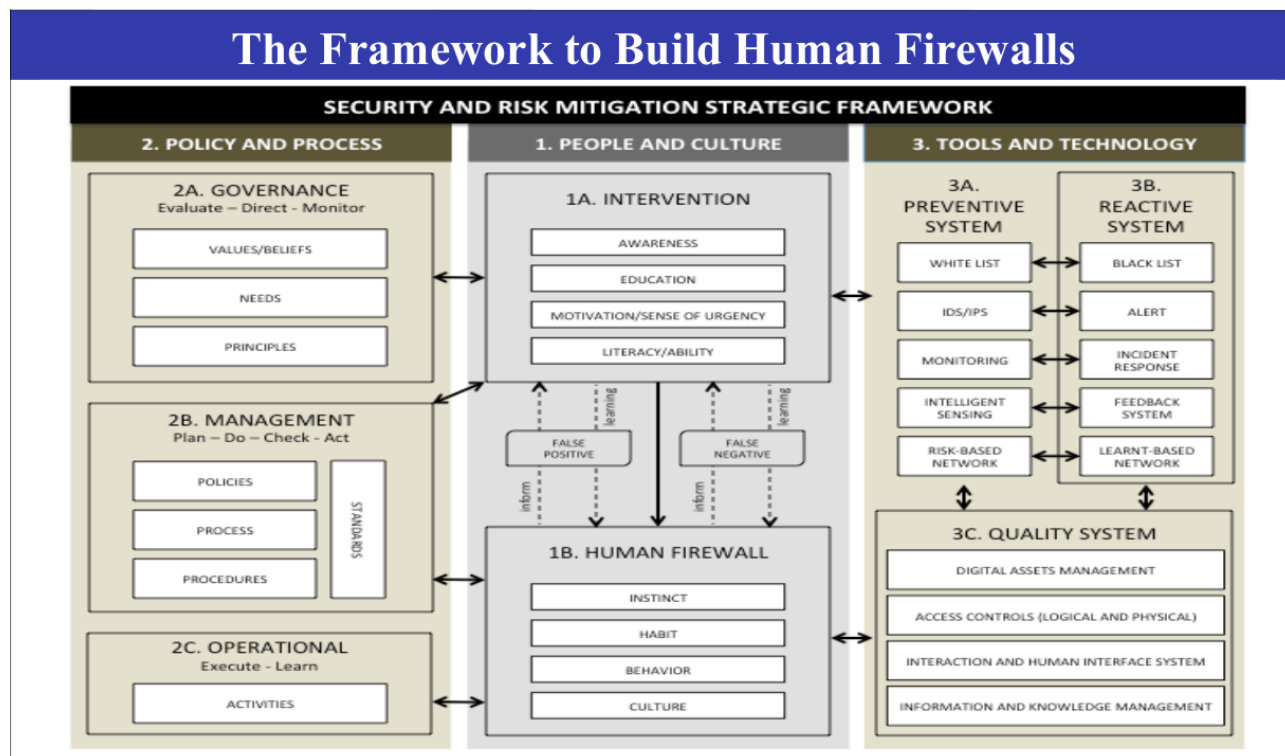


Ilustración 36: Marco de Trabajo para Construir "Firewalls" Humanos. Reproducido con autorización.

## 10.2.2 Estándares de seguridad

Una buena política de seguridad de la información es aquella que nace de la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en estándares. **La norma ISO/IEC 27001:2013**, que contiene los requisitos que debe cumplir un sistema de gestión de seguridad de la información, contempla específicamente controles y objetivos de control de referencia relativos a los recursos humanos.

Se distinguen requisitos a tres niveles, muchos de los cuales son de aplicación directa de cara a la mitigación de los ataques de ingeniería social:

- Durante el proceso de selección previo a la contratación
  - Una verificación curricular.
  - Garantías de confianza para ocupar un rol específico de seguridad.
  - Especificación del acuerdo contractual con el detalle de todos los términos y condiciones, pe. acuerdo de confidencialidad, responsabilidades y derechos respecto de la propiedad intelectual y la protección de datos personales, criterios sobre el manejo de información, acciones disciplinarias,...
- Durante la relación laboral con los empleados
  - La Gerencia será responsable de asegurar que los empleados sean informados de sus roles y responsabilidades, estén motivados en el cumplimiento de la política de seguridad, estén concienciados al respecto, reciban formación continua,...
  - Disponer de un procedimiento disciplinario, aplicarlo con garantías y emplearlo tanto con carácter disuasorio como incentivador.
- Tras la finalización del contrato de trabajo
  - Comunicar las responsabilidades legales y los acuerdos de confidencialidad aplicables después de la finalización de la relación laboral.
  - Incluir en los contratos tales responsabilidades y deberes.
  - Informar del fin del contrato del empleado a los departamentos de la organización y empresas colaboradoras para las que resulte de interés.

Así pues, la política de seguridad debe contemplar expresamente una directriz orientada a la gestión de los recursos humanos, que dé origen a un programa de trabajo para consolidar los requisitos expresados al respecto en el SGSI.

Otro estándar de aplicación a la organización para mitigar los ataques de ingeniería social es **la norma ISO/IEC 27032:2012**<sup>65</sup> a la que ya hacíamos referencia en el capítulo dedicado a la descripción de la ingeniería social. Fue preparada por el Comité Técnico Conjunto ISO / IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad de TI. En su introducción se describe el ciberespacio como un entorno complejo

65 <https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27032:ed-1:v1:en>

resultante de la interacción de personas, software y servicios en Internet, respaldado por dispositivos físicos de tecnologías de la información y comunicación distribuidos por todo el mundo y por redes conectadas. Continúa afirmando la norma que existen problemas de seguridad que no están cubiertos por la seguridad de la información actual, la seguridad de Internet, la seguridad de la red y las mejores prácticas de seguridad de las TIC, ya que existen lagunas entre estos dominios, así como la falta de comunicación entre organizaciones y proveedores en el ciberespacio. Esto se debe a que los dispositivos y las redes conectadas que han respaldado el ciberespacio tienen múltiples propietarios, cada uno con sus propias preocupaciones comerciales, operativas y regulatorias. El diferente enfoque puesto por cada organización y proveedor en el Ciberespacio en dominios de seguridad relevantes, donde se toma poca o ninguna aportación de otra organización o proveedor, ha resultado en un estado fragmentado de seguridad para el Ciberespacio.

Como tal, la primera área de enfoque de este Estándar Internacional es abordar los problemas de Ciberseguridad que se concentran en cerrar las brechas entre los diferentes dominios de seguridad en el Ciberespacio. En particular, esta ISO brinda orientación técnica para abordar riesgos comunes de Ciberseguridad, que incluyen:

- ataques de ingeniería social;
- piratería informática;
- la proliferación de software malicioso ("malware");
- spyware; y
- otro software potencialmente no deseado.

### 10.2.3 Auditorías

**La ingeniería social, vista como un recurso, se puede utilizar para evaluar el elemento humano** y concretamente la concienciación del usuario sobre la seguridad de la información; como resultado se pueden revelar debilidades en el comportamiento como el incumplimiento de los procedimientos estándar.

La ingeniería social puede usarse para dirigirse a individuos o grupos específicos de alto valor en la organización, como los ejecutivos. Tiene sentido principalmente cuando la organización conoce la existencia de una amenaza o entiende que la pérdida de información de una persona o grupo específico de personas podría tener un impacto significativo. Por ejemplo, se podría montar un ataque de ingeniería social usando técnicas de phishing, dirigido a individuos específicos, aprovechando la información disponible públicamente como sus títulos, áreas de interés, etc.

La selección individual de personas objetivo de evaluación también tiene sus riesgos; el éxito del ingeniero social, bien consiguiendo acceso a algún sistema o bien obteniendo información confidencial, podría avergonzar a esas personas. Por ello es importante que los resultados de las pruebas de ingeniería social se utilicen para mejorar la seguridad de la organización y no para individualizar ni hacer patentes las debilidades de las personas. Los evaluadores deben generar un informe final detallado que identifique las tácticas utilizadas, tanto las exitosas como las fallidas. Con este nivel de detalle se ayudará a la organización en la adaptación de sus programas de capacitación en seguridad.



El Instituto de Auditores Internos, en su guía para la supervisión de la ciberseguridad, propone una lista de 20 controles de seguridad críticos, como un **conjunto recomendado de acciones de ciberdefensa**, orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. Entre ellos se encuentra el CSC 7 que podemos vincular directamente con la ingeniería social:

<b>CSC 7</b>	<b>PROTECCIÓN DEL CORREO ELECTRÓNICO Y DEL NAVEGADOR</b>	Minimizar la posibilidad de que los atacantes manipulen a los empleados a través de su interacción con el correo electrónico y el navegador.
--------------	--	--

*Ilustración 37: CSC7-Control y objetivo de control de auditoría (IAI)*

Dicho control pasa por utilizar clientes de correo y navegadores actualizados y evitar que el usuario pueda añadir extensiones, así como cambiar su configuración. La configuración debe ser la más restrictiva posible para que el usuario pueda trabajar, deshabilitando los plugins innecesarios.

Con este enfoque tan técnico, resulta evidente que el control adolece de la parte meramente social o psicológica que caracteriza a la ingeniería social. Este hecho puede compensarse con otro control de la lista, concretamente el CSC 17:

<b>CSC 17</b>	<b>VERIFICACIÓN DE LAS HABILIDADES DE SEGURIDAD Y FORMACIÓN ADECUADA</b>	Identificar los conocimientos específicos, habilidades y capacidades necesarias en la organización para la defensa de los activos críticos de la compañía, y desarrollar y evaluar un plan para identificar gaps y remediar con políticas, formación y programas de sensibilización.
---------------	--	--

*Ilustración 38: CSC17-Control y objetivo de control de auditoría (IAI)*

Se basa en que cada puesto funcional tiene que tener una formación específica en seguridad. Deben identificarse posibles carencias y formar a los empleados. Igualmente, la organización debería tener un programa de concienciación dirigido a todos los empleados, adecuado a las funciones que realizan.

Entre las **herramientas a disposición de los auditores para llevar a cabo ataques autorizados de ingeniería social**, podemos encontrar las siguientes:

- Basadas en software: Existen algunas herramientas muy utilizadas por los ingenieros sociales para ayudarlos a manejar los ataques, que por supuesto pueden ser utilizadas por los auditores en la evaluación de los empleados. Determinar qué herramientas son las más efectivas depende en gran medida del tipo y el escenario de ataque que se persigue. A continuación se enumeran algunas de las herramientas más conocidas, no obstante cabe mencionar que también hay muchos sitios web que ofrecen ayuda para que los ingenieros sociales realicen sus actividades.
  - Kali Linux (antiguo BackTrack): una distribución de software Linux que ayuda a recopilar información y a utilizarla para pruebas de penetración y auditorías de ingeniería social.

- BasKet: funciona como un bloc de notas orientado a la organización de enormes cantidades de datos de distinto tipo (urls, textos, imágenes,...). Datos que pueden haber sido recopilados por ejemplo para ataques de ingeniería social.
- Dradis: una aplicación web autónoma que proporciona un repositorio centralizado de información. Herramienta de código abierto para la generación de informes y colaboración destinada principalmente a profesionales de seguridad de la información.
- Búsqueda avanzada de Google: un motor de búsqueda con numerosas funciones para buscar información con características específicas.
- Redes sociales (Facebook, Twitter, LinkedIn, MySpace, etc.): una red de medios sociales que consiste en enormes datos de todos los miembros registrados en el servicio.
- Common User Passwords Profiler (CUPP online): una herramienta especial diseñada para ayudar a las personas a adivinar las contraseñas más probables utilizadas por alguien.
- Maltego: servicio que tiene el potencial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo, etc.
- Conjunto de herramientas de ingeniería social (SET): Es una herramienta de código abierto impulsada por Python destinada a pruebas de penetración en torno a la Ingeniería Social. Ver anexo II.
- Basadas en el uso del teléfono: Desde el comienzo de la tecnología, el teléfono se ha utilizado para "piratear". Ya sea con exploits como el famoso teléfono phreaker Captain Crunch o los famosos Phreakers telefónicos The Badir Brothers, el teléfono ha sido ampliamente utilizado como una herramienta para los ingenieros sociales.
  - Los teléfonos desechables (burner phones): no dejan rastro del usuario y se compran con dinero en efectivo o una tarjeta regalo. Actualmente hay aplicaciones para iOS y Android (teléfonos inteligentes) para crear números desechables. Una de esas aplicaciones se llama "BURNERAPP" y se puede utilizar para vincular muchos números de teléfono en un mismo dispositivo. Esta aplicación es excelente para crear rápidamente un nuevo número, pero no es tan segura como tener un teléfono físico desechable real.
  - La suplantación del identificador de llamada: La identificación de llamadas se emplea con normalidad tanto en hogares como empresas. El principio básico detrás de la suplantación de identificador de llamadas es cambiar la información que se muestra en la pantalla del dispositivo que recibe la llamada. Esta técnica puede usarse en un ataque de ingeniería social para mostrar que una llamada proviene de una oficina remota, de un departamento dentro de la propia oficina, de un socio empresarial, de una compañía de suministros (teléfono, agua, Internet, etc.), de un superior, etc. Herramientas típicas son: SpoofCard, Asterix, SpoofApp, Voicemail,...
- Basadas en otros dispositivos:
  - Las cámaras y las grabadoras pueden ser una herramienta útil para los ingenieros sociales cuando es necesario capturar información rápidamente, ya sea mediante fotos, vídeos o audios. Es recomendable que el dispositivo empleado no de señales sonoras o visuales que desvelen su actividad, que su

tamaño le permita camuflarse o que tenga conectividad inalámbrica. Herramientas útiles para usar junto con esto son servicios como Skype que permiten al ingeniero social transmitir directamente desde el teléfono a la web. Esto permite que otros vean lo que hace el ingeniero social y registre la información para un estudio posterior.

- Los dispositivos de seguimiento GPS, con funciones como alertas de viaje instantáneas, informes históricos, conducción peligrosa y una duración de la batería extremadamente larga, son características muy interesantes para un ingeniero social.
- Los dispositivos para forzar cerraduras como los cuchillos Shove (ganzúas), las llaves bumping (maestras) o las cuñas.

Otro mecanismo de auditoría, o más bien de análisis de riesgos, es la denominada **retro-ampliación inversa del diagrama DAIS**, una metodología iterativa y evolutiva que permite determinar elementos críticos en una organización desde la visión de la ingeniería social. La retro-ampliación inversa es un método correctivo que trabaja con los diagramas DAIS tras perpetrarse un ataque. Sin embargo, también puede ser aplicado como una estrategia preventiva partiendo de potenciales ataques finales que se podrían llevar a cabo en una organización, y cuyo denominador común es el uso de la ingeniería social. Partiendo del ataque final del diagrama DAIS, el experto en seguridad deberá analizar e identificar todas las posibles acciones de la ingeniería social predecesoras que han conducido a dicho ataque final. Cada una de estas acciones es considerada entonces como un factor de riesgo. A partir de esto, por cada acción predecesora se aplica de manera recursiva la misma idea.

Tras el proceso de ampliación del DAIS, y mediante la visualización del nuevo diagrama, se pueden identificar gráficamente aspectos relevantes en relación con el ataque sobre el que se está trabajando, básicamente tendremos identificados los factores de riesgo tanto humanos como tecnológicos. Sin embargo, el nuevo diagrama nos permite obtener mayor información; en concreto, podemos emplear dicha representación del ataque para obtener los siguientes datos útiles: acciones críticas, conjunto de acciones mínimas, probabilidad de éxito y nivel de riesgo. Esta forma de análisis incluso nos permitiría establecer un conjunto de diagramas DAIS que podríamos definir como patrones tipo de la ingeniería social.

Retomando el caso real de modificación de nota en las calificaciones de un alumno, presentado en el capítulo dedicado al "Proceso de la Ingeniería Social", a título meramente ilustrativo incluiremos a continuación el diagrama DAIS normalizado y acto seguido el normalizado y extendido, remitiendo al material de la UOC para cualquier necesidad de información adicional:

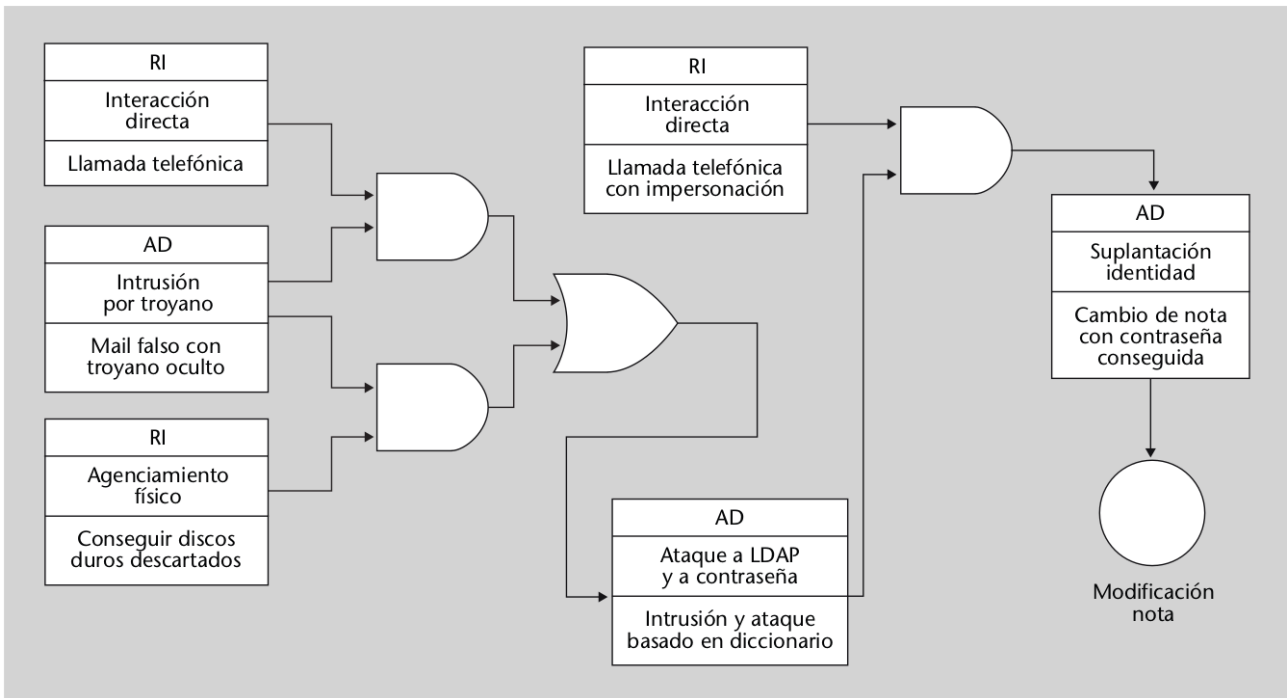


Ilustración 39: Retroampliación inversa. Diagrama DAIS normalizado. Material UOC.

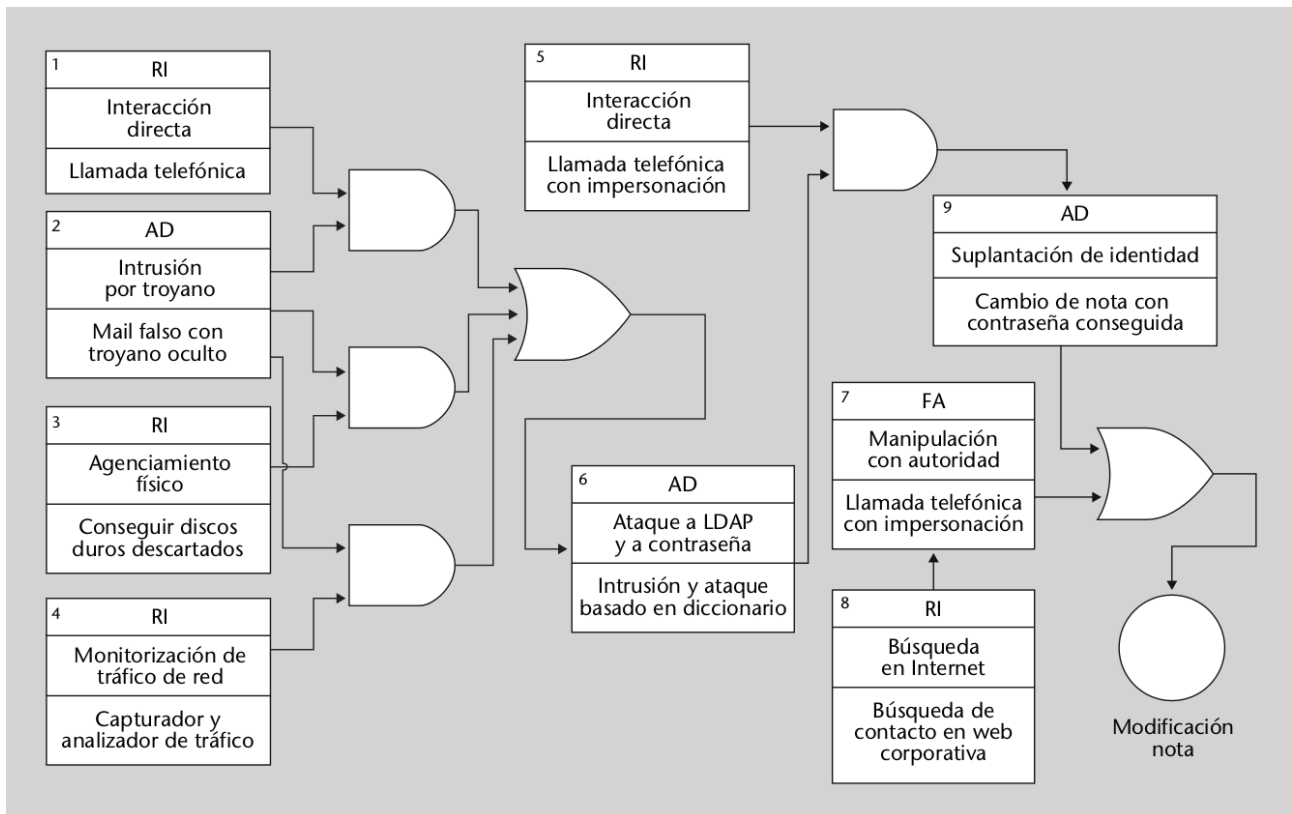


Ilustración 40: Retroampliación inversa. Diagrama DAIS normalizado y ampliado. Material UOC.

Tras la obtención del diagrama DAIS ampliado, podemos deducir directamente que las acciones críticas son la 2, 6, 7 y 9. Por otro lado, los conjuntos mínimos de acciones para alcanzar el objetivo son {1,2,5,6,9}, {2,3,5,6,9}, {2,4,5,6,9} y {7,8}.

#### 10.2.4 Formación

Tanto las respuestas innatas como las aprendidas por las personas, tratadas en capítulos anteriores, pueden ser superadas mediante la formación y sensibilización (Johnston, Warkentin, McBride, y Carter, 2016).

Haciendo un símil entre la seguridad de la información de una organización y la economía personal de un empleado, si éste acostumbrara a dejar su billetera abierta y desatendida, debería ser concienciado para que este hábito fuera considerado como un riesgo. Para el caso, el resultado más eficaz se obtendría provocando un pequeño susto en el empleado, por ejemplo tomando prestada una de sus tarjetas de crédito. La sensación y el impacto que este hecho genera en el empleado cuando se percata del "robo", hará que recuerde durante más tiempo el riesgo al que pueden estar sometidos los activos y aplicará las medidas de seguridad necesarias.

El cibercrimen con origen en la ingeniería social es una amenaza que, como hemos mencionado en anteriores ocasiones, puede ser fácilmente cometido por personas sin conocimientos técnicos, y tener una valoración cuantitativa del riesgo podría:

- Generar un mayor compromiso de la dirección y consecuentemente una mayor partida presupuestaria para contrarrestarlo.
- Permitir priorizar los objetivos en los que basar un plan de formación. Además, la repetición de la evaluación antes y después de los programas de formación puede ayudar a evaluar su efectividad.

Los programas de concienciación tradicionales a veces fallan porque los usuarios pueden carecer de motivación para aprender y pueden dejar de prestar atención a las diferentes señales de comunicaciones falsas o simuladas por formar parte de sus hábitos diarios.

Encontrar la forma correcta de crear conciencia es un factor clave. Los intentos más prometedores están relacionados con el uso de elementos visuales, como video, infografías o píldoras de información para estimular a las personas. Además, la gamificación es una de las tendencias más prometedoras. Las recompensas, el reconocimiento social y la retroalimentación directa durante la vida laboral diaria pueden ayudar.

#### Plan de concienciación personalizado

Pero demos un paso más. Si es posible evaluar el factor humano como ha quedado patente en el capítulo dedicado a las estrategias de gestión de riesgos, también debería ser posible personalizar un programa de concienciación y/o formación basándonos en los datos obtenidos (resultados de un phishing de verificación, tipo de personalidad de los empleados, experiencias comunes, etc.) Esta cuestión está bastante bien tratada por Michael Alexander en su artículo "Methods for Understanding and Reducing Social

Engineering Attacks<sup>66</sup> publicado en abril de 2016 en SANS Institute InfoSec Reading Room.

Alexander afirma que los paquetes de formación contratados tan sólo son útiles par pasar evaluaciones de cumplimiento, no llegando a ser efectivos. No obstante, a medida que los atacantes se vuelven más sofisticados y selectivos como ocurre con el spear phishing o las amenazas avanzadas persistentes, este enfoque inadecuado. La sensibilización y/o la formación en seguridad debe volverse tan sofisticada como los ataques, de modo que si un ataque se dirige a un individuo en particular en función de su posición en la empresa o sus privilegios de acceso, la capacitación debe tratar por separado a este tipo de personas, entrando en detalles específicos sobre cómo pueden ser atacadas. En este sentido Alexander plantea varios ejemplos:

- Un administrador de sistemas es probable que sea atacado para adquirir sus privilegios de acceso de una manera muy diferente a la que se utilizaría para un empleado con funciones de asistente administrativo.
- Un empleado con la capacidad de saldar pagos pendientes puede ser atacado de manera diferente que un director financiero porque el primero tiene la capacidad de crear e imprimir cheques o conoce cierta información sensible relacionada con cuentas bancarias, mientras que el segundo se dedica más a temas de estrategia y procedimientos.

Este experto continúa expresando la necesaria consideración de las características y tendencias innatas de la personalidad de los empleados para la elaboración de un programa de formación. Cita a Lewis (2010) para reflejar el más que probable éxito de un ataque man-in-the-middle que suponga la suplantación de un sitio web comúnmente visitado por un empleado objetivo, de modo que éste proporcione información confidencial sin percatarse de la ilegitimidad de la web. Y cita a Bullée, Montoya, Pieters, Junger y Hartel (2015) para afirmar lo anterior es aplicable incluso a quienes hayan superado una acción formativa tipo en materia de seguridad.

Ante este panorama, y otros no descritos, si bien puede ser poco práctico capacitar a todos los empleados para afrontar todas las amenazas potenciales, si es posible modularizar la capacitación basada en ciertos vectores, como el nivel de acceso, el uso de Internet o incluso los tipos de personalidad.

Alexander propone una solución basada en un programa interno de capacitación y concienciación en seguridad de la información con las siguientes características:

- Ha de considerar todos los factores que afectan a la organización.
- Debe tener en cuenta los factores conductuales y de personalidad de los empleados.
- Tienes que ser planificado, diseñado, implementado y medido.
- Y debe estar incorporado a los procesos cotidianos de la organización hasta que se convierta en parte de la cultura de la organización.

En la siguiente tabla vamos a reflejar los detalles de esta solución para una mejor estructuración y comprensión:

---

66 <https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972>

**Fase de planificación**

1. Establecer los objetivos de la capacitación, considerando que deben ser realistas, alcanzables y medibles. Ejemplos:
  - Asegúrese de que todos los empleados aprendan las políticas y procedimientos de seguridad para el final del segundo trimestre.
  - Reducir el uso de Internet por motivos personales en un 30%.
  - Reducir el número de incidentes relacionados con la seguridad debido a ingeniería social en un 30% para el final del tercer trimestre.
2. Planificar las pruebas de personalidad, considerando el tiempo para investigar y seleccionar la mejor prueba de personalidad para la organización. Ejemplos:
  - El método OCEAN (Johnston, Warkentin, McBride, y Carter, 2016).
  - El método Myers-Briggs, The Caliper Profile y DISC.
3. Determinar el formato y el método de ejecución de la capacitación, considerando factores como las aulas disponibles, los materiales didácticos, la ubicación de los empleados, el tamaño de la organización, los idiomas necesarios, etc.
4. Diseñar un plan de proyecto para determinar todas las tareas relevantes, las fechas de inicio y finalización planificadas para cada tarea, dependencias y la fecha de finalización proyectada de la capacitación.

**Fase de evaluación de la personalidad**

1. El diseño del programa en sí no puede comenzar hasta que se complete la prueba de personalidad por lo que deben comenzar lo antes posible.
2. Completadas las pruebas, deben analizarse los resultados para categorizar a los empleados según el tipo de personalidad (Johnston, Warkentin, McBride y Carter, 2016).
3. Se creará un programa de capacitación personalizado para cada categoría.

**Fase de diseño del programa de capacitación y concienciación**

1. El diseño debe enfocarse en las fortalezas potenciales y, más importante aún, en las debilidades de cada tipo de personalidad.

Por ejemplo, si un empleado en particular evidencia su pertenencia al tipo de personalidad extrovertida y se sabe que ello supone automáticamente un bajo sentido de gravedad de amenaza, éste tiene más probabilidades de violar las políticas de seguridad de la organización. Esta categoría ha de ser entrenada para comprender completamente todas las amenazas conocidas y las consecuencias de las mismas.

**Fase de desarrollo del programa**

1. Tanto el proceso de planificación, como los materiales didácticos han de estar elaborados.
2. Las aulas deben estar reservadas y los horarios deben estar concretados.
3. Se debe realizar una prueba de los materiales en un pequeño grupo interfuncional de empleados. Los comentarios recogidos deben evaluarse e incorporarse a los materiales en caso de pertinencia.
4. Determinar los criterios de éxito para que, cuando se midan los resultados, la gerencia sepa si el programa ha valido la pena.

#### Fase de ejecución del programa

1. Suponiendo que todas las fases anteriores se hicieron correctamente, la implementación de la capacitación debería realizarse sin problemas.
2. La ejecución del programa evolucionará con el tiempo (Gupta, n.d.).
3. La cultura corporativa debería comenzar a cambiar.
4. Se deben implementar políticas y cronogramas para garantizar que la conciencia de seguridad se arraigue en la mentalidad de cada empleado y se convierta en una parte natural de los procesos de la organización.

#### 10.2.5 El Plan de Cultura de Ciberseguridad.

Como comentábamos en el capítulo de introducción de este trabajo, el desarrollo de una Cultura de CiberSeguridad (CCS/CSC) es importante para gestionar el riesgo asociado al factor humano, al tiempo que permite la adopción y el uso de nuevas tecnologías por parte de las empresas. Nos encontramos ante el reto de modelar la ciberseguridad en la organización desde un punto de vista integral que permita dar una solución global como suma de distintas soluciones parciales.

Una buena forma de acercamiento a la cultura de ciberseguridad es a través de la publicación de ENISA titulada *Cultura de Ciberseguridad en las Organizaciones*<sup>67</sup>, basada en múltiples disciplinas, incluidas las ciencias de la organización, la psicología, el derecho y la ciberseguridad. Este informe se complementa con el conocimiento y las experiencias recopiladas de los programas existentes de CSC implementados dentro de las organizaciones, y contiene buenas prácticas, herramientas metodológicas y una orientación paso a paso para aquellos que buscan comenzar o mejorar el propio programa de Cultura de Ciberseguridad de su organización.

El concepto de cultura de ciberseguridad se refiere al conocimiento, creencias, percepciones, actitudes, suposiciones, normas y valores de las personas con respecto a la ciberseguridad y cómo se manifiestan en su comportamiento con las tecnologías de la información. CSC abarca temas comunes, incluidos la concienciación en ciberseguridad y los marcos de seguridad de la información, pero es más amplio en alcance y aplicación, preocupándose de hacer que las consideraciones de seguridad de la información sean una parte integral del trabajo, hábitos y conducta de los empleados, incrustándolas en sus acciones cotidianas.

Entre los factores que destacan la necesidad de un plan de cultura en ciberseguridad en las organizaciones están los siguientes:

- El comportamiento de la organización frente a la ciberseguridad depende directamente de las creencias, valores y acciones llevadas a cabo por sus empleados
- Las campañas de concienciación sobre ciberamenazas no son, en sí mismas, una protección suficiente contra la constante evolución de los ciberataques.

67 <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>



- Las medidas técnicas de ciberseguridad no tienen razón de ser por sí mismas, concebidas de forma aislada, sino que necesitan operar en armonía con otros procesos comerciales para evitar que los empleados se encuentren ante la disyuntiva de elegir entre "hacer su trabajo" o "cumplir con las políticas de seguridad".
- Finalmente, el plan pretende responder a la consideración de que los humanos representan el eslabón más débil en las cadenas de ciberseguridad, transformándolos en robustos servidores humanos frente a los ciberataques.

La consideración de afrontar concienzudamente las recomendaciones y el marco de trabajo que propone la guía de implementación de un CSC en la organización excede el alcance del presente trabajo fin de máster, por ello reduciremos los elementos a los imprescindibles.

El primero será el Marco de Implementación paso a paso centrado en actividades específicas, su implementación y medición de impacto. Tiene un enfoque iterativo porque después ejecutar cada actividad de CS, se mide su impacto, se consideran los resultados obtenidos y se revisa el enfoque. Después de esto, se pueden elegir nuevas actividades o se pueden cambiar los métodos de entrega/distribución. Esto también brinda la oportunidad de considerar y modificar los objetivos iniciales y / o el público objetivo.

Marco de trabajo para que las organizaciones implementen un programa de CSC	
Paso 1: configure su grupo de trabajo principal de CSC	Tendrá la tarea de: <ul style="list-style-type: none"> <li>• formación de política y estrategia de CSC;</li> <li>• generación de conocimiento para garantizar un enfoque basado en evidencia para CSC;</li> <li>• así como supervisar la implementación o las actividades de CSC.</li> </ul>
Paso 2: Comprenda su negocio y evalúe los riesgos.	Hable con los empleados para identificar: <ul style="list-style-type: none"> <li>• las culturas, creencias y prácticas existentes de su organización; y</li> <li>• lo puntos de alineación/desalineación entre los procesos de negocio y las medidas de seguridad.</li> </ul> Este producto debe conducir y dar forma a todos los pasos subsiguientes de este Marco.
Paso 3: defina los objetivos principales, los criterios de éxito y las audiencias objetivo.	<ul style="list-style-type: none"> <li>• Defina los objetivos principales de su programa de CSC.</li> <li>• Priorice los problemas más importantes a tratar y defina los criterios de éxito.</li> <li>• Identifique a los empleados objetivo actuales de su programa CSC.</li> </ul>
Paso 4: calcule su situación actual y haga un análisis de brechas con respecto a su situación objetivo.	Calcular su CSC en base al reflejo del comportamiento actual de los empleados. Esto es un requisito previo para cuantificar el impacto de sus actividades de CSC.

<p>Paso 5: Seleccione una o más actividades para cerrar la brecha entre el estado actual y su estado objetivo.</p>	<ul style="list-style-type: none"> <li>• Haga una lluvia de ideas sobre una variedad de actividades basadas en su público objetivo.</li> <li>• Cree o compre cualquier material / herramienta para implementarlas.</li> </ul>
<p>Paso 6: ejecute las actividades que seleccionó.</p>	<ul style="list-style-type: none"> <li>• Ejecute cada actividad individualmente para poder determinar el impacto de cada una.</li> <li>• Ejecute actividades de forma conjunta si desea determinar su impacto combinado.</li> </ul>
<p>Paso 7: Recalcule la situación actual y analice los resultados.</p>	<ul style="list-style-type: none"> <li>• Vuelva a calcular su situación actual (desde el paso 4) para identificar el impacto de su actividad de CSC.</li> <li>• Si aplica, analice los resultados para identificar las variaciones en el impacto dentro de su público objetivo.</li> </ul>
<p>Paso 8: Revise y considere sus resultados antes de decidir sobre la próxima acción.</p>	<ul style="list-style-type: none"> <li>• Si necesita revisar sus procesos comerciales en función de su capacidad / incapacidad para influir en su CSC, <u>regrese al paso 2</u> y continúe.</li> <li>• Si decide cambiar su público objetivo o modificar sus objetivos, <u>regrese al paso 3</u> y proceda.</li> <li>• Si sus actividades de CSC lograron sus objetivos, o si desea enfocarse en un aspecto diferente del CSC en su organización, <u>regrese al paso 4</u> y continúe.</li> <li>• Si sus actividades de CSC no alcanzaron su objetivo establecido, <u>vuelva al paso 5</u> y refine su actividad de CSC o seleccione una actividad diferente y vuelva a ejecutarla.</li> </ul>

El segundo será definir los requisitos organizativos para garantizar el éxito del CSC. Ello supone la creación de un entorno laboral receptivo así como la creación de una equipo de trabajo sólido y cohesionado para la implantación del CSC.

El tercero será establecer los elementos y recursos necesarios para construir con éxito un programa de CSC y medirlo. Algunas actividades clave que resultarían de utilidad al equipo de trabajo podrían ser:

Online	Híbridas	Offline
<p>Emails, vídeos, juegos, seminarios web, cursos de formación online, intranet de la organización, redes sociales,...</p>	<p>Ejecuta escenarios, ensayos, entornos protegidos y ejercicios de juegos de guerra. Historias de buenas prácticas de los</p>	<p>Sesiones de capacitación individuales o de grupo, folletos, carteles, talleres, eventos, lecturas de expertos externos,...</p>

	empleados. Ofrecimiento de incentivos. Hojas de consejos. Preguntas frecuentes. Simulacros de ataques,...	
--	---	--

La medición del impacto de las actividades dependerá del análisis de brechas ejecutado y de la efectividad de las métricas definidas.

El cuarto consiste en la utilización de buenas prácticas. Se trata de aprovechar las iniciativas CSC ya desplegadas de otras organizaciones, poniendo el foco en los diferentes públicos objetivo, tanto personal experto como perfiles operacionales.

Y el quinto elemento a considerar de nuestra selección son los factores organizativos que afectan a las culturas de ciberseguridad. Las organizaciones pueden tomar medidas para dar forma tanto a su CSC como a una cultura organizacional más amplia (cultura corporativa) que puede influir enormemente en CSC. Aquí, las colaboraciones dentro de la organización son esenciales ya que la comunicación abierta facilitará el desarrollo de un CSC. Todos los integrantes de una empresa deben participar aportando experiencias en sus áreas profesionales, identificando dónde se cruzan los riesgos de ciberseguridad con las funciones del negocio, y detectando soluciones o ideas potencialmente conflictivas. No obstante, ciertos puestos y departamentos ejecutivos tienen un papel clave que desempeñar en el desarrollo del CSC: dirección gerencia, responsables de seguridad de la información, cargos intermedios, miembros del departamento de tecnologías de la información, abogados, responsables de recursos humanos y encargados de la comunicación interna.

Una vez expuesto el marco de trabajo para la implementación de un CSC, aprovecharemos para traer a colación una "herramienta" diseñada por INCIBE que ayudará enormemente al equipo de trabajo. Se trata del "kit de concienciación<sup>68</sup>", un programa de trabajo a caballo entre un plan de concienciación/formación y un plan de ciberseguridad que está compuesto por las siguientes seis fases:

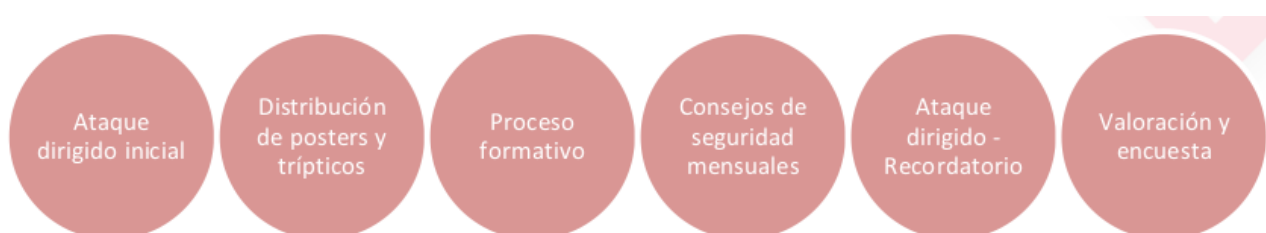


Ilustración 41: INCIBE. Fases del kit de concienciación

68 <https://www.incibe.es/protege-tu-empresa/kit-concienciacion>

El kit incorpora múltiples recursos gráficos, elementos interactivos y una programación detallada para su puesta en marcha:

1. Manual de implantación: contiene información sobre los materiales además de una programación para su distribución dentro de una empresa.
2. Ataques dirigidos: La conciencia empieza con uno o dos ejercicios que van a permitir evaluar el nivel de concienciación en seguridad de los empleados a la vez que despertamos su interés por aprender más. Estos ejercicios toman la forma de ataques sorpresa.
3. Pósteres y trípticos: Con estos elementos principalmente gráficos se pretende concienciar a los empleados para que se consideren una parte activa de la seguridad de nuestra empresa. Deben ser distribuidos en lugares de paso frecuente.
4. Proceso formativo: Una vez despertado el interés, se plantea realizar un proceso formativo combinando la distribución de material para su lectura y visualización con la opcional organización de charlas. Esta fase consta de cuatro bloques temáticos o píldoras: la información, los soportes, el puesto de trabajo y los dispositivos móviles.
5. Consejos de seguridad mensuales: A modo de resumen se incluyen unos ficheros con gráficos que contienen consejos temáticos para reforzar lo aprendido. Estos materiales se pueden enviar por correo, publicar en un blog interno o distribuirse de forma impresa.
6. Encuesta de satisfacción: Cuando haya terminado la concienciación en su empresa puede remitirse a INCIBE la experiencia y opinión mediante la encuesta de satisfacción.

## 10.3 Pautas para los estados

### 10.3.1 Medición

En el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se llevó a cabo el seminario nº 3 dedicado al *fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia*. En él se reconocía la necesidad de adoptar medidas eficaces para conocer mejor la escala, las raíces y el modus operandi en la comisión de delitos conexos, elaborar estrategias eficaces de prevención, mejorar el intercambio de información, y reforzar los marcos nacionales y la cooperación internacional entre Estados Miembros.

Destaca por tanto la necesaria medición de la ciberdelincuencia como elemento previo a la adopción de contramedidas. Uno de los enfoques utilizados para medir las nuevas formas y dimensiones de la delincuencia, incluida la ciberdelincuencia, se basa en una combinación de indicadores, como por ejemplo:

- información sobre los infractores,
- información sobre los flujos existentes en los mercados ilícitos e
- información sobre el número de delitos cometidos, los daños y pérdidas causados, y los flujos financieros ilícitos resultantes.

En el caso de la ciberdelincuencia se destaca la posibilidad de utilización de diversas fuentes de datos con ese fin, algunas de las cuales son:

- las estadísticas de delitos registrados por la policía,
- las encuestas entre particulares y empresas,
- las iniciativas de denuncia de las víctimas,
- la información de ciberseguridad obtenida por medios tecnológicos,
- las técnicas de rastreo de URL,
- o el secuestro de redes zombi o “botnets”.

De todo ello se pueden obtener beneficios importantes. Por ejemplo, de los datos de las encuestas que incluyen información sobre pérdidas financieras derivadas de la ciberdelincuencia pueden obtenerse estimaciones sobre su impacto; del análisis de los mercados de la ciberdelincuencia puede estimarse la naturaleza y la dimensión de algunas formas de delitos cibernéticos. Un enfoque de este tipo se centra en el análisis de foros en línea que funcionan como “redes sociales” para delincuentes, que tienen por objeto la venta y la compra de bienes sociales, así como el intercambio de información sobre actividades delictivas.

Las nuevas tecnologías de investigación también ofrecen la posibilidad de rastrear los servicios ocultos en Tor. Estas tecnologías pueden facilitar la identificación y clasificación sistemática del número y el tipo de páginas de la Internet profunda relacionadas con temas como la venta de drogas ilícitas, la pornografía infantil, la venta de armas o instrumentos para cometer delitos cibernéticos.

Por último, la caracterización de los autores de estos delitos ayuda a comprender la naturaleza y el modus operandi de las organizaciones delictivas en cuestión. Es probable que no exista un “perfil” estándar en este sentido. Un número relativamente reducido de programadores y piratas informáticos altamente cualificados pueden impulsar la innovación en el terreno de la ciberdelincuencia y ofrecer sus aptitudes como un servicio delictivo. Sin embargo, la facilidad de acceso a los exploits y los programas maliciosos implica que en muchos casos los autores ya no requieren conocimientos avanzados. Por otra parte, es posible que algunas formas de ciberdelincuencia dependan cada vez más de la presencia de un gran número de “soldados rasos”, pe. mulas.

### 10.3.2 Regulación

La Oficina de las Naciones Unidas contra la Droga y el Delito<sup>69</sup> (UNODC, de sus siglas en inglés) promueve la creación de capacidad a largo plazo y sostenible en la lucha contra el

69 <https://www.unodc.org/unodc/es/index.html>

ciberdelincuencia mediante el apoyo a las estructuras y acciones nacionales. Específicamente, la UNODC recurre a su experiencia especializada en respuesta a los sistemas de justicia penal para proporcionar asistencia técnica en creación de capacidad, prevención y sensibilización, cooperación internacional y recopilación de datos, investigación y análisis sobre ciberdelincuencia.

En su resolución 65/230, la Asamblea General solicitó a la Comisión de Prevención del Delito y Justicia Penal que estableciera un Grupo Intergubernamental de Expertos de Composición Abierta, para realizar un estudio exhaustivo del problema de la ciberdelincuencia y las respuestas a este fenómeno por los Estados Miembros, la comunidad internacional y el sector privado. El estudio debería promover el intercambio de información sobre legislación nacional, mejores prácticas y asistencia técnica y la cooperación internacional, con miras a examinar opciones para fortalecer las legislaciones existentes y proponer nuevas respuestas jurídicas nacionales o internacionales u otras respuestas al delito cibernético.

Pues bien este Grupo se reunió por primera vez en Viena en el año 2011, donde revisó y adoptó una colección de temas y una metodología para el estudio. Posteriormente se celebraron otras sesiones en 2013, 2017 y en 2018, ésta última tuvo lugar del 3 al 5 de abril de 2018, también en Viena, Austria. El informe emanado, UNODC / CN.5 / 2018/4<sup>70</sup>, es un estupendo documento guía para los Estados con recomendaciones de gran trascendencia respecto del tratamiento del ciberdelito que debe realizarse en la legislación, marcando las pautas a seguir en base al conocimiento de la cibercriminalidad.

A modo ilustrativo, a continuación expondremos algunas de las recomendaciones que contiene tanto para la legislación como para la tipificación de delitos:

- Legislación y marcos

*a) Los Estados Miembros deberían velar por que sus disposiciones legislativas resistan el paso del tiempo frente a futuros avances tecnológicos promulgando leyes cuya formulación sea neutral tecnológicamente y que penalicen las actividades consideradas ilícitas en lugar de los medios utilizados. Asimismo, los Estados Miembros deberían considerar la posibilidad de adoptar una terminología coherente para describir las actividades cibernéticas delictivas y facilitar, en la medida de lo posible, una interpretación precisa de las leyes pertinentes por parte de los organismos encargados de hacer cumplir la ley y el poder judicial.*

(...)

*c) Con el fin de prevenir y eliminar los refugios para los delincuentes, los Estados Miembros deberían cooperar entre sí en la mayor medida posible en la investigación, la reunión de pruebas, el enjuiciamiento, el fallo y, en caso necesario, la eliminación de contenidos ilícitos de Internet...*

(...)

---

<sup>70</sup> <https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html>

k) Los Estados Miembros deberían apoyar a la UNODC en la creación de un proyecto o programa educativo<sup>71</sup> destinado a concienciar sobre la ciberdelincuencia y las respuestas apropiadas a ese fenómeno entre las autoridades judiciales y fiscales, los expertos en ciencia forense digital de los Estados Miembros y las entidades privadas, y utilizar instrumentos de creación de capacidad o una plataforma electrónica de gestión de los conocimientos con el fin de sensibilizar a la sociedad civil sobre las repercusiones de la ciberdelincuencia.

(...)

- Tipificación de delitos

De conformidad con el plan de trabajo, el presente párrafo contiene una recopilación de las sugerencias formuladas por los Estados Miembros en la reunión en relación con el tema 3 del programa, titulado “Tipificación”...

(...)

d) Los Estados Miembros deberían tipificar los delitos cibernéticos básicos que afectan a la confidencialidad, la integridad y la disponibilidad de las redes de computadoras y los datos informáticos, teniendo en cuenta las normas internacionales reconocidas ampliamente.

e) Los actos cibernéticos considerados infracciones leves y no delitos deberían tratarse en reglamentos civiles y administrativos en lugar de en la legislación penal.

f) En la medida en que aún no lo hayan hecho, los Estados Miembros deberían considerar la posibilidad de tipificar como delito las siguientes conductas:

i) las formas de actividad cibernética delictiva nuevas y emergentes, como el uso indebido delictivo de criptomonedas, los delitos cometidos en la web oscura y la Internet de las cosas, el phishing, y la distribución de programas maliciosos y otros programas informáticos utilizados para cometer actos delictivos;

ii) la divulgación de información personal y la “porno venganza”;

iii) el uso de Internet para cometer actos relacionados con el terrorismo;

iv) el uso de Internet para incitar a cometer delitos motivados por prejuicios y al extremismo violento;

v) la prestación de apoyo técnico o asistencia para la comisión de un acto cibernético delictivo;

vi) la creación de plataformas en línea ilícitas o la publicación de información para cometer delitos cibernéticos;

vii) la obtención de acceso por medios ilícitos a sistemas informáticos o la piratería de dichos sistemas;

viii) la interceptación o el daño ilícitos de datos informáticos y el daño ilícito a sistemas informáticos;

ix) la interferencia ilícita en los datos y sistemas informáticos;

71 <https://www.unodc.org/elearning/index.html>

- x) el uso indebido de dispositivos;*
- xi) la falsificación y el fraude informáticos;*
- xii) el abuso y explotación sexuales de menores;*
- xiii) la infracción de la propiedad intelectual;*
- xiv) el abuso y explotación sexuales de menores, y la inducción de menores al suicidio;*
- xv) la influencia ilícita sobre infraestructuras de información esenciales.*



## 11 Conclusiones

Desde el plano personal, una vez afrontado el reto de investigar y documentar cuanto ha resultado interesante en relación a la ingeniería social y sus metodologías, con el conocimiento de los distintos informes, artículos e incluso libros puestos a disposición pública por sus autores, estoy en disposición de realizar las siguientes afirmaciones:

1. Se trata de un técnica de ataque suficientemente estudiada tanto en el plano académico como en el plano empresarial. Este hecho parece ser consecuencia de la relevancia que la misma tiene en la seguridad de la información en general y la ciberseguridad en particular, por ser uno de los vectores de ataque más empleados.
2. Tiene un fuerte impacto en la economía de los ciudadanos y de las organizaciones, además de en la reputación. Por un lado supone un coste a considerar como parte del presupuesto planificado para cada ejercicio fiscal debido a la presencia cada vez más común de incidentes de seguridad originados en la ingeniería social. Y por otro, mueve ingentes cantidades de dinero negro en los mercados sumergidos, bien por la compraventa de información robada, bien por la contratación de servicios de ataque.
3. Fruto de los estudios y las incidencias, se ha producido el nacimiento en algunos casos y la evolución en otros, de una industria o nicho de mercado orientado a su gestión como riesgo: desarrollo de estándares internacionales que contemplan expresamente la ingeniería social, creación de herramientas software específicas para evaluar su afección dentro de la organización, diseño y entrega de programas de concienciación y formación, especialización de los perfiles profesionales dedicados a la seguridad de la información, evolución de los seguros que ofrecen las compañías para externalizar el riesgo, etc.
4. Los estados están tomando medidas para mitigar en lo posible los riesgos cibernéticos a través de iniciativas legislativas, como la modificación del código penal, e iniciativas administrativas, como la creación de autoridades de control y centros de operaciones de seguridad y respuesta a incidentes. Aunque en gran medida también sean los propios estados, directa e indirectamente, quienes propicien la evolución de las amenazas por sus luchas de poder y aspiraciones de control.
5. Cada vez se hace más necesario disponer de un plan de cultura en ciberseguridad entre los planes estratégicos de soporte al negocio de una organización de tamaño medio o grande. Los departamentos de seguridad deben crecer en paralelo a los servicios ofrecidos y con los niveles adecuados de gestión o incluso gobierno en las organizaciones.

Volviendo la vista a los objetivos planteados inicialmente de cara al desarrollo de este TFM, en una primera valoración general, podría afirmarse que eran demasiado ambiciosos. En defensa de los mismos hemos de dejar patente que ante la posibilidad de desarrollar un trabajo poco acotado, en un tema poco conocido por el autor, procedía manifestar esta actitud y elevar las expectativas como elemento motivador para lograr resultados. Con la experiencia adquirida, la evolución natural del trabajo debería ser el desarrollo específico de los objetivos de cara a una organización concreta:

- 7 *"Desarrollar los ítems de un plan de cultura de ciberseguridad, acotando el alcance al contexto de la ingeniería social, y trabajando el conocimiento, las creencias, las percepciones, las actitudes, las suposiciones, las normas y los valores de las personas"* y
- 8: *"Diseñar e implementar objetos de aprendizaje con herramientas abiertas que faciliten la implantación de los ítems del plan de cultura de ciberseguridad"*.

Ciertamente existen empresas dedicadas casi exclusivamente a ello, en las que la empresa cliente podría apoyarse, sin embargo lo recomendable sería partir de la propuesta del departamento de seguridad interno. El conocimiento de la organización en la que se pretende aplicar el plan de cultura en ciberseguridad resulta clave para garantizar su éxito.

Considerando que la metodología definida durante la fase inicial del TFM se ha seguido adecuadamente, un análisis crítico de la misma podría enmarcarse en la asignación de tiempos a cada tarea. Obviamente es fácil afirmar esto a posteriori, cuando se tiene una visión clara sobre los recursos que más trabajo ha costado localizar y/o documentar, y cuales ha resultado menos complejos. Determinados capítulos, la mayoría, han supuesto un esfuerzo mayor de lo estimado como consecuencia del interés en dejar constancia de todo aquello que parecía ser trascendente, lo que ha redundado en una menor dedicación al cumplimiento de las últimas tareas.

## 12 Glosario

### 12.1 Términos

**Adware:** (Software publicitario) es cualquier programa que automáticamente muestra u ofrece publicidad no deseada, ya sea incrustada en una página web mediante gráficos, carteles, ventanas flotantes, o durante la instalación de algún programa al usuario, con el fin de generar lucro a sus autores.

**Air Gap:** Bloquear el hardware para impedir que los empleados accedan a ciertos sitios web, instalen aplicaciones o conecten dispositivos USB. En muchos casos, las grandes empresas requieren que los empleados lleven portátiles y dispositivos separados para uso personal y comercial. Esto se conoce como un modelo de seguridad "espacio de aire", y si bien este enfoque mejora la seguridad, la productividad se ve severamente afectada.

**Baiting:** Hostigar, cebar, azuzar. Técnica de ingeniería social.

**Botnet:** Término derivado de las palabras robot y network.

**Bullying:** Es cualquier forma de maltrato psicológico, verbal o físico producido entre estudiantes de forma reiterada a lo largo de un tiempo determinado tanto en el aula, como a través de las redes sociales, con el nombre específico de ciberacoso.

**Bump Key:** Llave bumping. El método Bumping es una técnica para abrir cerraduras sin forzarlas haciendo uso de una llave maestra.

**Ciberdelito:** (Delito informático) es toda aquella acción antijurídica y culpable a través de vías informáticas o que tiene como objetivo destruir y dañar por medios electrónicos y redes de Internet.

**Cracker:** Se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad.

**Crawler:** Es un programa informático que inspecciona las páginas del World Wide Web de forma metódica y automatizada.

**Figón de paquetes O Sniffer:** Es un programa de captura de las tramas de una red de computadoras.

**Flame o Flaming:** Es un malware modular descubierto en 2012 que ataca ordenadores con el sistema operativo Microsoft Windows.

**Grooming:** Es una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las preocupaciones de el menor y poder abusar sexualmente de él.

**Gusano:** Es un malware que tiene la propiedad de duplicarse a sí mismo.

**Hacker:** Es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

**Malware:** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información.

**Mantrap:** Un portal de mantrap, air lock, sally o access control es un sistema de control de acceso de seguridad física que comprende un espacio pequeño con dos juegos de puertas entrelazadas, de modo que el primer conjunto de puertas debe cerrarse antes de que se abra el segundo conjunto.

**Pirata:** Es quien adopta por negocio la reproducción, apropiación y distribución con fines lucrativos y a gran escala de distintos medios y contenidos (soporte lógico, videos, música) de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador.

**Shove Knife:** Cuchillo de empuje o ganzúa. Alambre fuerte y doblado por una punta, a modo de garfio, con que, a falta de llave, pueden correrse los pestillos de las cerraduras.

**Syn Flood:** Una inundación SYN es una forma de ataque de denegación de servicio en el que un atacante envía una sucesión de solicitudes SYN al sistema del objetivo en un intento de consumir suficientes recursos del servidor para que el sistema no responda al tráfico legítimo.

**Tailgaiting:** Chupar rueda, ir a rebufo. Técnica de ingeniería social.

**Wetware:** Es un término obtenido de la idea relacionada a la computación del hardware o el software, pero aplicada a formas de vida biológicas.

**Whaling:** Nueva modalidad de fraude derivada del "phishing", cuyo propósito es captar "peces pequeños" para redes zombi. La "caza de ballenas" está dirigida hacia usuarios acaudalados e influyentes.

## 12.2 Acrónimos

**APT:** Advanced Persistent Threat

**APWG:** Anti-Phishing Working Group

**BEC:** Business Email Compromise

**CaaS:** Crime-as-a-Service

**CEO:** Chief Executive Officer

**CERT:** Computer Emergency Response Team

**CP:** Código Penal

**CSC:** Cyber Security Culture

**CSIRT:** Computer Security Incident Response Team

**CVV:** Card Verification Value

**EC3:** European Cybercrime Centre

**ECTEG:** European Cybercrime Training and Education Group

**ENISA:** European Union Agency for Network and Information Security

**GDPR:** General Data Protection Regulation

**IAI:** Instituto de Auditores Internos

**ICANN:** Internet Corporation for Assigned Names and Numbers

**IOCTA:** Internet Organised Crime Threat Assessment

**IoT:** Internet of Things

**IP:** Internet Protocol

**ISACA:** Information Systems Audit and Control Association

**IT:** Information technology

**NIS:** Network and information systems

**NIST:** National Institute of Standards and Technology

**OEDI:** Observatorio Español de Delitos Informáticos

**ONTSI:** Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información

**OSINT:** Open-source intelligence

**P2P:** Peer to peer, or people to people

**PIN:** Personal identification number

**SANS:** Instituto organizado como una cooperativa de investigación y educación, especializado en seguridad de la información

**SEC:** Sistema Estadístico de Criminalidad

**SGSI:** Sistema de Gestión de Seguridad de la Información

**SIEM:** Gestión de eventos e información de seguridad.

**SWIFT:** Society for Worldwide Interbank Financial

**Tor:** The Onion Router

**VoIP:** Voice-over-Internet Protocol

**VPN:** Virtual private network

**WEF:** World Economic Forum

## 13 Bibliografía

### LIBROS

- European Union Agency for Network and Information Security (2018). *ENISA Threat Landscape Report 2017*. Heraklion, Greece. ISBN 978-92-9204-250-9, ISSN 2363-3050, DOI 10.2824/967192
- European Union Agency for Network and Information Security (2017). *Cyber Security Culture in organisations*. Heraklion, Greece. ISBN: 978-92-9204-245-5, DOI: 10.2824/10543
- Newhouse, William et al. (agosto de 2017). *NIST Special Publication 800-181. National Initiative for Cybersecurity Education (NICE) - Cybersecurity Workforce Framework*. Gaithersburg, Maryland. EE.UU. MD 20899-2000, DOI: 10.6028/NIST.SP.800-181
- Scarfone, Karen et al. (septiembre de 2008). *NIST Special Publication 800-115. Technical Guide to Information Security Testing and Assessment*. Gaithersburg, Maryland. EE.UU. MD 20899-8930.
- Comisión técnica. Martínez, Isarel et al. (2016). *Buenas prácticas en gestión de riesgos: Ciberseguridad. Una guía de supervisión (La fábrica de pensamiento)*. Madrid: Instituto de Auditores Internos de España. ISBN: 978-84-945594-2-6
- Comisión Europea (2017). *Europeans' attitudes towards cyber security*. Special Eurobarometer 464a – Wave EB87.4 – TNS opinion & social. ISBN: 978-92-79-71901-1. DOI: 10.2837/82418
- European Union Agency for Law Enforcement Cooperation - Europol (2017). *Internet Organised Crime threat assessment (IOCTA) 2017*. ISBN 978-92-95200-80-7. ISSN 2363-1627. DOI 10.2813/55735
- Madrigal, Consuelo. *Fiscal General del Estado (2016). <<Memoria enviada al Gobierno de S.M.>>*. Madrid. España. Edita: Centro de Estudios Jurídicos. Ministerio de Justicia. NIPO: 056-15-002-7. ISSN: 1889-7118. Depósito legal: M-27317-2016.
- THIBER, the Cyber Security Think Tank (2016). *<<CIBERSEGUROS: la transferencia del ciberriesgo en España>>*. Madrid. España. ISBN 978-84-608-7693-9
- Mitnick, Kevin D. et al. (2003). *<<The art of the deception. Controlling the Human Element of Security>>*. Nueva York: John Wiley & Sons, Inc. ISBN: 076454280X (ISBN13: 9780764542800)

### ARTÍCULOS

- Robles, Sergi y Castillo Sergio (2011). *<<Ingeniería Social>>*. Asignatura "Vulnerabilidades de Seguridad" del MISTIC de la UOC (módulo 5, PID\_00178969). Barcelona. España.

- Pendergast, Tom (2016). <<How to Audit the Human Element and Assess Your Organization's Security Risk>>. ISACA Journal (núm. 5, pág. 20-24). Illinois. USA.
- Puricelli, Roberto (2015). <<The Underestimated Social Engineering Threat in IT Security Governance and Management>>. ISACA Journal (núm. 3, pág. 24-28). Illinois. USA.
- Shenk, Jerry (2017). <<Countering Impersonation, Spearphishing and Other Email-Borne Threats: A Review of Mimecast Targeted Threat Protection>>. SANS Institute InfoSec Reading Room. Europa, Medio Oriente y África (Autor: Pensilvania).
- Alexander, Michael (2016). <<Methods for Understanding and Reducing Social Engineering Attacks>>. SANS Institute InfoSec Reading Room. Europa, Medio Oriente y África.
- Kee, Jared (2008). <<Social Engineering: Manipulating the Source>>. SANS Institute InfoSec Reading Room. Europa, Medio Oriente y África.
- Workman, Michael (2008). <<A test of interventions for security threats from social engineering>>. Information Management & Computer Security (Vol. 16, Iss. 5, pág. 463-483). Bradford. Inglaterra.
- Eko, Richardus (2017). <<Social Engineering Framework: Understanding the Deception Approach to Human Element of Security>>. IJCSI International Journal of Computer Science Issues (volume 14, issue 2). Jakarta. Indonesia. DOI: 10.20943/01201702.816
- Winder, Davey (2017). <<Social engineering>>. PC Pro; London (Iss. 277).
- Bąkowski, Piotr (2013). <<Cyber security in the European Union>>. Servicio Europeo de Investigación Parlamentaria. Bruselas. Bélgica.
- López, Oscar David y Restrepo, Wilmar Dario (2013). <<Análisis y desarrollo de estrategias para la prevención del uso de la ingeniería social en la sociedad de la información>>. Ing. USBMed (Vol. 4, No. 2 pág. 16-22). ISSN: 2027-5846.
- Miró, Fernando (2013). <<LA RESPUESTA PENAL AL CIBERFRAUDE: Especial atención a la responsabilidad de los muleros del phishing>>. Revista Electrónica de Ciencia Penal y Criminología. ISSN 1695-0194.
- Faralado, Patricia (2010). <<La respuesta española al cibercrimen. Algunas reflexiones.>>. Gaceta penal y procesal penal: Análisis de la sentencia sobre la constitucionalidad de los decretos legislativos nº 982, 983 y 988. (Tomo 14, pág. 431 - 453). España. ISBN/ISSN/DL: 0002386
- Salvador, Luis de (2011). <<Ingeniería social y operaciones psicológicas en internet>>. Instituto Español de Estudios Estratégicos - IEEE.es (documento 74). España.
- Hendrik, Jan-Willem et al. (2017). <<On the anatomy of social engineering attacks - A literature-based dissection of successful attacks>>. John Wiley & Sons, Ltd.. Netherlands. DOI: 10.1002/jip.1482

## PRESENTACIONES E INFORMES

- Puricelli Roberto y Frumento, Enrico (2014). <<An innovative and comprehensive Framework for Social Vulnerability Assessment>>. DeepSec Conference. Vienna, Austria.
- Social-Engineer, LLC (2017). <<*The 2017 Social Engineering Capture the Flag Report*>>. DEF CON 25 SECTF, DerbyCon VII SECTF.
- Beek, Christiaan et al. (2018). <<Alerta sanitaria. El sector de la asistencia sanitaria en el punto de mira de la ciberdelincuencia>>. McAfee - Inter Security. Madrid. España.
- McFarland, Charles et al. (2015). <<*El comercio clandestino de datos: El mercado de la información digital robada*>>. McAfee. Madrid. España.
- @nms\_george (2013). <<*Ingeniería Social: explotando a los humanOS*>>. Eset latinoamerica: concurso de investigación en seguridad de la información.
- M<sup>3</sup>AAWG (2014). <<*The Network Operators' Perspective*>>. Messaging, Malware and Mobile Anti-Abuse Working Group. Email Metrics Program: Report #16 – 1 st Quarter 2012 through 2 nd Quarter 2014. San Francisco. EE.UU.
- M<sup>3</sup>AAWG y London Action Plan (2015). <<*Operación Safety Net. Mejores prácticas recomendadas para enfrentar amenazas en línea, móviles y telefónicas*>>.
- Christin, Nicolas et al. (2010). <<*It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice*>>.
- Ureña, Alberto et. al. (2017). <<*Estudio sobre la Ciberseguridad y confianza en los hogares españoles*>>. ONTSI. Red.es. ISSN 2386-3684. Madrid. España.
- Verizon. <<*2018 Data Breach Investigations Report*>> (11 th edition).
- CCN-CERT IA-16/17. <<*Ciberamenazas y Tendencias Edición 2017*>>
- CCN-CERT IA-09/18. <<*Ciberamenazas y Tendencias Edición 2018*>>
- Agencia Española de Protección de Datos (2018). <<*Protección de datos y prevención de delitos*>>
- INTECO. Cuaderno de notas del OBSERVATORIO (2012). <<*¿Qué son las Amenazas Persistentes Avanzadas (APTs)?*>>
- INTERPOL (2013). <<*Social engineering fraud: questions and answers*>>
- Naciones Unidas. 13er Congreso sobre prevención del delito y justicia penal (2015). <<*Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional*>>
- Naciones Unidas. Consejo Económico y Social (2018). <<*Informe de la reunión del Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético*>>. Viena. Austria.
- Universidad de Piura (2016). <<*Delitos informáticos: Delitos en y desde la red*>>



- Anti-Phishing Working Group - APWG (2017). <<Phishing Activity Trends Report - 1 st Half 2017>>.
- Anti-Phishing Working Group - APWG (2017). <<Phishing Activity Trends Report - 4 th Quarter 2017>>.

## PÁGINAS WEBS

- *Toma conciencia para evitar los ataques de ingeniería social* (17/02/2016) [en línea]. León: INCIBE. [Consulta: febrero de 2018] <https://www.incibe.es/protege-tu-empresa/blog/toma-conciencia-evitar-ataques-ingenieria-social>
- *La ingeniería social en la empresa: aprovechando la naturaleza humana* (12/05/2014) [en línea]. León: INCIBE. [Consulta: febrero de 2018] <https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas>
- *Pasos que sigue un ciberdelincuente para alcanzar a su presa* (09/12/2015) [en línea]. León: INCIBE. [Consulta: febrero de 2018] <https://www.incibe.es/protege-tu-empresa/blog/pasos-que-sigue-un-ciberdelincuente-para-alcanzar-a-su-presa>
- *¿Cómo combatir la ingeniería social? Este empresario nos lo cuenta* (08/08/2016) [en línea]. León: INCIBE. [Consulta: febrero de 2018] <https://www.incibe.es/protege-tu-empresa/blog/combater-ingenieria-social-este-empresario-nos-cuenta>
- *Historias reales: Espiaron nuestros correos con los clientes y ¡casi nos timan!* (11/07/21014) [en línea]. León: INCIBE. [Consulta: febrero de 2018] <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-empresas-espiaron-correos-clientes-fraude-scam>
- *Kit de concienciación* (2013). [en línea]. León: INCIBE. [Consulta: marzo de 2018] <https://www.incibe.es/protege-tu-empresa/kit-concienciacion>
- *Psicohacking* (14/03/2018) [en línea]. León: OSI - INCIBE. [Consulta: marzo 2018] <https://www.osi.es/es/actualidad/blog/2018/03/14/psickohacking>
- *El robo de identidad y sus consecuencias* (02/06/2011) [en línea]. León: OSI - INCIBE. [Consulta: marzo 2018] <https://www.osi.es/es/actualidad/blog/2011/06/02/el-robo-de-identidad-y-sus-consecuencias>
- *Social Lab, el wargame de la ingeniería social* (22/11/2012) [en línea]. León: OSI - INCIBE. [Consulta: marzo 2018] <https://www.osi.es/es/actualidad/blog/2012/11/22/social-lab-el-wargame-de-la-ingenieria-social>
- *¿Qué hacen los ciberdelincuentes con los datos robados?* (26/10/2015). [en línea]. León: INCIBE. [Consulta: marzo de 2018] <https://www.incibe.es/protege-tu-empresa/blog/que-hacen-los-ciberdelincuentes-con-los-datos-robados>
- *How to avoid losing a lot of money to CEO Fraud* (10/02/2016). [en línea]. ENISA. [Consulta: mayo de 2018] <https://www.enisa.europa.eu/publications/info-notes/how-to-avoid-losing-a-lot-of-money-to-ceo-fraud>
- *What is "Social Engineering"?* (fecha de publicación desconocida). [en línea]. ENISA. [Consulta: mayo de 2018] <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering>

- Sistema de Gestión de Seguridad de la Información según la norma ISO/IEC 27001:2013. [en línea]. International Organization for Standardization. [Consulta: mayo 2018] <https://www.iso.org/standard/54534.html>
- Gestión de la Ciberseguridad según la norma ISO/IEC 27032:2012. [en línea]. International Organization for Standardization. [Consulta: mayo 2018] <https://www.iso.org/standard/44375.html>
- Social Engineering (fecha de publicación desconocida). [en línea]. KnowBe4. [Consulta: abril 2018] <https://www.knowbe4.com/what-is-social-engineering/>
- Phishing con BackTrack 5 (2011). [en línea]. Los Indestructibles. [Consulta: marzo 2018] <https://losindestructibles.wordpress.com/2011/10/01/phishing-con-backtrack-5/>
- Ingeniería Social: Camuflando un payload (2017). [en línea]. Hacking Ético. [Consulta: marzo 2018] <https://hacking-etico.com/2017/07/27/ingenieria-social-camuflando-un-payload/>
- Los delitos informáticos: Marco teórico y Legal (fecha publicación desconocida). [en línea]. SI & SL – Seguridad Informática & Software Libre. [Consulta: marzo 2018] <https://www.siysl.net/los-delitos-informaticos-marco-teorico-y-legal/>
- Los delitos informáticos. Tratamiento internacional (2016). [en línea]. La Razón - La Gaceta Jurídica. [Consulta: marzo 2018] [http://www.la-razon.com/index.php?url=/la\\_gaceta\\_juridica/delitos-informaticos-Tratamiento-internacional\\_0\\_2450155056.html](http://www.la-razon.com/index.php?url=/la_gaceta_juridica/delitos-informaticos-Tratamiento-internacional_0_2450155056.html)
- Los 10 delitos digitales que marcarán la ciberseguridad en 2017 (2017). [en línea]. Noticias Jurídicas. [Consulta: marzo 2018] <http://noticias.juridicas.com/actualidad/noticias/11587-los-10-delitos-digitales-que-marcaran-la-ciberseguridad-en-2017/>
- Procesos policiales y judiciales para identificar autores de delitos en redes sociales (2014). [en línea]. Lefebvre - El Derecho. [Consulta: marzo 2018] [http://tecnologia.elderecho.com/tecnologia/ciberseguridad/Procesos-policiales-judiciales-identificacion-calumniosos\\_11\\_675055001.html](http://tecnologia.elderecho.com/tecnologia/ciberseguridad/Procesos-policiales-judiciales-identificacion-calumniosos_11_675055001.html)
- Aproximación a los delitos cometidos a través de las TIC (2014). [en línea]. Aspectos profesionales. [Consulta: mayo 2018] <http://www.aspectosprofesionales.info/2014/03/aproximacion-los-delitos-telematicos.html>
- Clasificación de los delitos informáticos (2016). [en línea]. Carely Berenice Carrasco García: Taller de legislación informática. [Consulta: abril 2018] <https://carebcarrasco.wordpress.com/2016/06/13/clasificacion-de-los-delitos-informaticos/>
- Metodología jurídica penal para hacer frente al crecimiento del ciberdelito. ¿cuál sería el tratamiento jurídico penal dada la dificultad para apreciar la autoría delictiva? (2012). [en línea]. Lefebvre - El Derecho. [Consulta: abril 2018]. [http://tecnologia.elderecho.com/tecnologia/ciberseguridad/ciberterrorismo-ciberdelito-tecnologia-ciberdelincuente\\_11\\_478180004.html](http://tecnologia.elderecho.com/tecnologia/ciberseguridad/ciberterrorismo-ciberdelito-tecnologia-ciberdelincuente_11_478180004.html)

- Social Engineering Attacks: Common Techniques & How to Prevent an Attack (2018). [en línea]. Digital Guardian. [Consulta: mayo 2018] <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack>
- “ICANN Targeted in Spear Phishing Attack. Enhanced Security Measures Implemented” (2014). [en línea]. ICANN, [Consulta: abril 2018] <https://www.icann.org/news/announcement-2-2014-12-16-en>
- COBIT ® 5 (2012). [en línea]. ISACA. [Consulta: abril 2018]. USA [www.isaca.org/cobit](http://www.isaca.org/cobit)
- Etc, etc, etc.

## 14 Autorizaciones de reproducción de contenidos

A continuación se exponen algunas de las principales autorizaciones de reproducción y/o transformación de contenidos con derechos de autor que han sido incluidos en el presente trabajo fin de máster, normalmente en forma de resumen. La única intención de estas referencias es la de reflejar, a nuestro juicio, los mejores trabajos en cada área tratada, para contribuir en la lucha contra los ataques de ingeniería social.

Algunas de las autorizaciones incluidas forman parte de la política editorial de las fuentes de información empleadas y otras son respuestas personales de los autores.

### SANS Web Site

#### Preguntas frecuentes

<https://www.sans.org/about/faq>

Can I use material from SANS web site or a SANS published work in a dissertation, research paper, or other scholarly work?

You may use SANS copyrighted material in a scholarly work as long as it is properly referenced (you must give the material a footnote or endnote citing SANS and the source). Under US Copyright Law, you do not need permission to include small amounts of copyrighted material in a learning exercise. However, your paper may not be copied for distribution outside your classroom without violating copyright law.

### ENISA

Documento: Cyber Security Culture in organisations

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2017

*Reproduction is authorised provided the source is acknowledged.*

ISBN 978-92-9204-245-5 DOI 10.2824/10543

### INCIBE

Aviso Legal: Propiedad intelectual, industrial y frames

<https://www.incibe.es/aviso-legal>

Todos los elementos que forman el sitio Web, así como su estructura, diseño, código fuente, así como los logos, marcas y demás signos distintivos que aparecen en la misma, son titularidad de INCIBE o de sus colaboradores y están protegidos por los correspondientes derechos de propiedad intelectual e industrial.

Igualmente están protegidos por los correspondientes derechos de propiedad intelectual e industrial las imágenes y otros elementos gráficos contenidos en los portales.

INCIBE prohíbe expresamente la realización de “framings” o la utilización por parte de terceros de cualesquiera otros mecanismos que alteren el diseño, configuración original o contenidos de nuestros portales.

El uso de los contenidos deberá respetar su licenciamiento particular. De tal modo su uso, reproducción, distribución, comunicación pública, transformación o cualquier otra actividad similar o análoga, queda totalmente prohibida salvo que medie previa y expresa autorización de INCIBE.

*INCIBE autoriza la reproducción total o parcial de los textos y contenidos proporcionados por el portal, siempre que concurren todas y cada una de las siguientes condiciones:*

*Se mantenga la integridad de los contenidos, documentos o gráficos.*

*Se cite expresamente a INCIBE como fuente y origen de aquellos.*

*El propósito y la finalidad de tal uso sea compatible con los fines de la Web y/o la actividad de INCIBE.*

*No se pretenda un uso comercial, quedando expresamente prohibidas su distribución, comunicación pública, transformación o descompilación.*

Cualquier otro uso habrá de ser comunicado y autorizado por INCIBE, previa y expresamente.

Respecto a las citas de productos y servicios de terceros, INCIBE reconoce a favor de sus titulares los correspondientes derechos de propiedad industrial e intelectual, no implicando su sola mención o aparición en la Web la existencia de derechos ni de responsabilidad alguna sobre los mismos, como tampoco respaldo, patrocinio o recomendación.

INCIBE declara su respeto a los derechos de propiedad intelectual e industrial de terceros; por ello, si considera que nuestros portales pudieran estar violando sus derechos, rogamos se ponga en contacto con INCIBE.

## CCN-CERT

Documento: CCN-CERT-IA-16-17 Ciberamenazas y Tendencias. Edición 2017

*Asunto:* CCN-CERT-IA 16-17 Ciberamenazas y Tendencias 2017

*Fecha:* Mon, 28 May 2018 15:15:02 +0200

*De:* FORMACION CCN <formacion@ccn.cni.es>

*Organización:* CCN

*Para:* rmarinj@uoc.edu

*Buenas tardes, Rafael.*

*Mediante el presente correo electrónico se le autoriza el empleo de la información recogida en el informe `CCN-CERT-IA-16-17 Ciberamenazas y Tendencias. Edición 2017`, para la elaboración de su proyecto final de máster. No obstante, la información sustráida de dicho informe ha de ser debidamente citada en su trabajo.*

*Sin otro particular, reciba un cordial saludo.*

--

Centro Criptológico Nacional  
formacion@ccn.cni.es

## SOCIAL ENGINEERING

Documento: The 2017 Social Engineering Capture the Flag Report

<https://www.social-engineer.org>

Asunto: Re: The 2017 Social Engineering Capture the Flag Report

Fecha: Tue, 15 May 2018 19:03:11 +0000

De: Cat Murdock <cat@social-engineer.com>

Para: Rafael Marín Jiménez <rmarinj@uoc.edu>

Rafael,

As long as you professionally and properly cite the report and it's author, Social-Engineer, you may reference it as a source for you TFM.

Hope this helps!

Cat Murdock  
Social Engineer PenTester  
(570)234-3735 ext. 216  
cat@social-engineer.com

**From:** Rafael Marín Jiménez <rmarinj@uoc.edu>  
**Sent:** Monday, May 14, 2018 10:22:40 AM  
**To:** Cat Murdock  
**Subject:** The 2017 Social Engineering Capture the Flag Report

Dear Cat

My name is Rafael Marín, I'm a student of the [Universidad Oberta de Catalunya](#) (Spain) in the [Inter-University Master in Information and Communication Technologies Security](#) (MISTIC). I'm currently working on my final master's degree project (TFM), which aims to carry out a study on social engineering methodologies.

During my research I learned about the existence of the website <https://www.social-engineer.org> and browsing it I have located the SECTF event. I was particularly interested in "The 2017 Social Engineering Capture the Flag Report" which I would like to mention briefly in my TFM as an example of the possibilities of information gathering offered by social engineering.

Since this report is fully protected by copyright, I have taken the liberty of writing to this e-mail address at the bottom of the report, with the intention of requesting the relevant authorisation.

You should be aware that the TFM does not pursue any financial gain on my part, and that the source of the information will obviously be duly mentioned.

Previously I tried to contact the Social-Engineer.com team through the address [sectf@social-engineer.com](mailto:sectf@social-engineer.com)

engineer.org and the website contact form. Nobody answered.

Awaiting news from you, I bid you farewell.  
Rafael Marin

-----  
Asunto: RE: Contact  
Fecha: Tue, 22 May 2018 02:29:34 -0400  
De: logan@social-engineer.org  
Para: rmarinj@uoc.edu

Yes as long as you give full credits to the source we are good

Good luck!

Chris "loganWHD"

[www.twitter.com/humanhacker](http://www.twitter.com/humanhacker)

[www.social-engineer.org](http://www.social-engineer.org)

---

**From:** rmarinj@uoc.edu <noreply@social-engineer.org>  
**Sent:** Sunday, May 6, 2018 12:45 PM  
**To:** logan@social-engineer.org  
**Subject:** Contact

**Name:** Rafael Marín  
**Email:** [rmarinj@uoc.edu](mailto:rmarinj@uoc.edu)  
**Message:**

Good afternoon

---

My name is Rafael Marín, I am a student of the Universidad Oberta de Catalunya (Spain) in the Inter-University Master in Information and Communication Technologies Security (MISTIC). I am currently working on my final master's degree project (TFM), which aims to carry out a study on social engineering methodologies.

During my research I learned about the existence of the website <https://www.social-engineer.org> and browsing it I have located the SECTF event. I was particularly interested in the "The 2017 Social Engineering Capture the Flag Report" which I would like to mention briefly in my TFM as an example of the possibilities of information gathering offered by social engineering.

Since this report is fully protected by copyright, I have taken the liberty of writing to this e-mail address at the bottom of the report, with the intention of requesting the relevant authorisation.

You should be aware that the TFM does not pursue any financial gain on my part, and that the source of the information will obviously be duly mentioned.

---

Awaiting news from you, I bid you farewell.  
Rafael Marin

Sent from <https://www.social-engineer.org>

## RICHARDUS EKO INDRAJIT

Documento: Social Engineering Framework: Understanding the Deception Approach to Human Element of Security

Asunto: Re: Social Engineering Framework: Understanding the Deception Approach to Human Element of Security

Fecha: Mon, 14 May 2018 00:43:14 +0700

De: Richardus Eko Indrajit <eko.indrajit@gmail.com>

Para: Rafael Marín Jiménez <rmarinj@uoc.edu>

CC: Richard Ekoji <indrajit@post.harvard.edu>

Dear Rafael,

Of course, you can use it for your reference.

It is truly an honour for me.

I wish you luck with your endeavour.

By the way, I will be visiting Barcelona on the 26 of May 2018.

I am free to meet you should you need my assistance.

Warm regards,

Eko Indrajit

On Mon, May 14, 2018 at 12:08 AM Rafael Marín Jiménez <[rmarinj@uoc.edu](mailto:rmarinj@uoc.edu)> wrote:

Good afternoon Prof. Richardus Eko Indrajit

My name is Rafael Marín, I'm a student of the [Universidad Oberta de Catalunya](#) (Spain) in the [Inter-University Master in Information and Communication Technologies Security](#) (MISTIC). I'm currently working on my final master's degree project (TFM), which aims to carry out a study on social engineering methodologies.

During my research I learned about the existence of the "Social Engineering Framework: Understanding the Deception Approach to Human Element of Security" article (<https://doi.org/10.20943/>, <http://www.> - IJCSI Open Access Publications) and I would like to mention briefly it in my TFM.

I have taken the liberty of writing to this e-mail address at the top of the article, with the intention of requesting the relevant authorisation.

You should be aware that the TFM does not pursue any financial gain on my part, and that the source of the information will obviously be duly mentioned.

Awaiting news from you, I bid you farewell.

Rafael Marín

## SERGI ROBLES



Documento: "Ingeniería Social", módulo 5 de la asignatura "Vulnerabilidades de Seguridad" del MISTIC

--- Mensaje original de Sergi Robles <Sergi.Robles@uab.cat> para Rafael Marín Jiménez (rmarinj@uoc.edu) enviado el 26.02.2018 15:47

Hola Rafael,

En realidad son los apuntes de un módulo de la asignatura de Vulnerabilidades de Seguridad. Lo puedes encontrar en la biblioteca de la UOC. Te paso el enlace:

[http://openaccess.uoc.edu/webapps/o2/bitstream/10609/55581/6/Vulnerabilitats%20de%20seguretat\\_M%C3%B2dul5\\_Enginyeria%20social.pdf](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/55581/6/Vulnerabilitats%20de%20seguretat_M%C3%B2dul5_Enginyeria%20social.pdf)

Si el enlace no te funciona, busca el libro "Vulnerabilidades de Seguridad" y accede al módulo 5.

Saludos,

Sergi.

On 22/02/18 20:05, Rafael Marín Jiménez wrote:

> Buenos días Sergi

>

> He localizado en la biblioteca de la UOC un libro titulado "Ingeniería Social

> <http://uoc.summon.serialssolutions.com/#!/search?bookMark=ePnHCXMw42JgAfZbUzkZhDxBm4OAZfvhtYkKkAFgHgaWkqJSYLGn6-Ya4uyhW5qfHA-eEyyOB51ynFwWDxZJKY0P8HSJB58-bmgJvtGcJPUA2BQqJQ>

> del que eres coautor y que debería estar disponible en línea, pero actualmente no es así. Me preguntaba si puedes remitirme algún otro enlace o una versión accesible offline.

> Voy a comenzar el TFM y versa sobre ese tema, por ello pretendo recopilar información al respecto.

>

> Gracias por adelantado.

> RMJ

-----  
Sergi Robles (<http://deic.uab.es/~sergi>)

Dept. of Information and Communications Engineering

Universitat Autònoma de Barcelona

Tel.: +34 93581 2395

Skype: SergiRobles

## 15 Anexos

### 15.1 Anexo I: Phishing

El phishing suele ser el primer paso en la mayoría de los ciberataques antes de obtener un punto de apoyo en un sistema o de robar datos. Los ejemplos de cómo se usa el phishing como vector de ataque se ilustran en la siguiente figura:

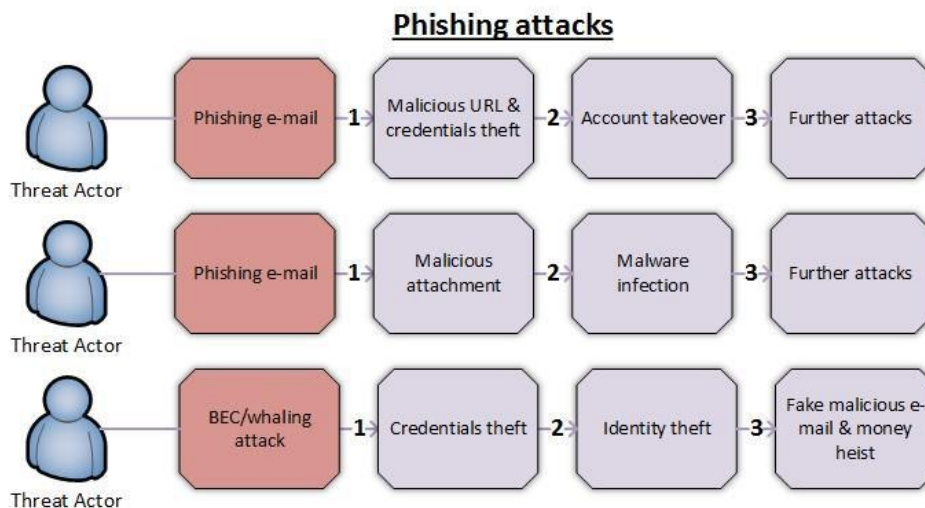


Ilustración 42: ENISA. Phishing como vector de ataque

Los primeros dos actores de amenaza, por url y por adjunto malicioso, son descritos con mayor detalle en la siguiente figura:

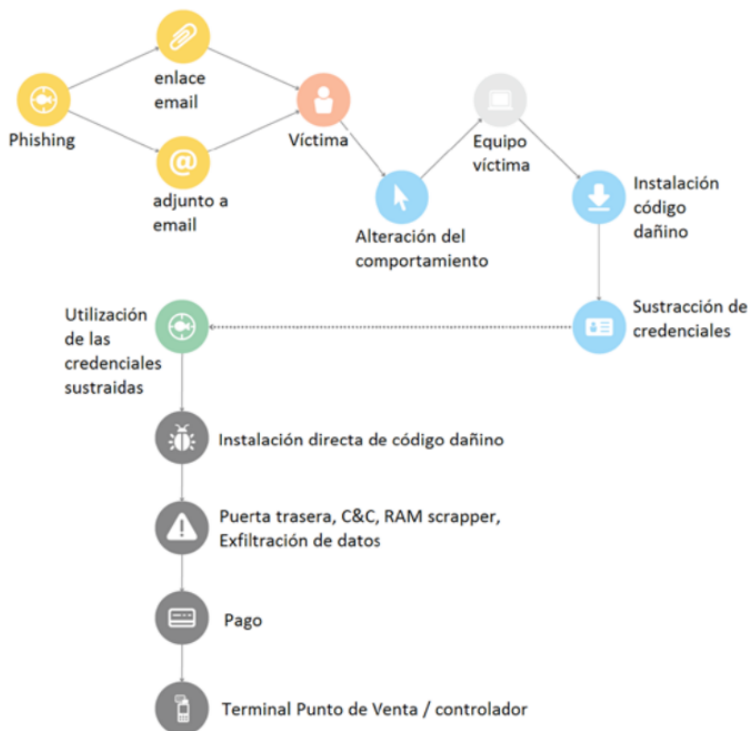


Ilustración 43: Itinerario dañino más frecuente seguido por los atacantes

Ejemplos de incidentes de seguridad relacionados con este vector de ataque:

- Los correos electrónicos que simulan provenir de un banco entregaron el Troyano Trickbot bancario a través de un archivo adjunto malicioso<sup>72</sup>. Este es un escenario muy común de entrega de malware y ransomware. Los correos electrónicos suelen estar muy bien contruidos y son convincentes, por lo que a menudo logran engañar a la gente.
- Las estafas de soporte técnico se basan en la ingeniería social: utilizan mensajes de error falsos para engañar a los usuarios para que llamen a líneas directas y paguen por servicios de soporte técnico innecesarios o por la descarga de malware. Una de las últimas tendencias en esta área es el uso de sitios web que abren automáticamente la aplicación predeterminada de llamada telefónica de un dispositivo móvil con el número de teléfono listo para marcarse<sup>73</sup>.
- Se encontró una aplicación falsa de WhatsApp con 1 millón de descargas en Play Store<sup>74</sup> de Google. La aplicación maliciosa parece haber sido desarrollada por WhatsApp Inc, el legítimo propietario de la aplicación, pero en realidad no fue así. El agente de amenazas detrás de la aplicación logró engañar a los usuarios al agregar un espacio oculto (en Unicode) al final del nombre de la compañía, enmascarando la aplicación como una aplicación de WhatsApp Inc. Se han usado técnicas de engaño similares en los ataques de phishing<sup>75</sup>.

Podemos encontrar un buen resumen sobre el phishing en el "ENISA Threat Landscape Report 2017", liberado en enero de 2018. En este documento, además de definir esta técnica, se explican los factores que contribuyen a su éxito como son: los ataques dirigidos, la entrega de malware, la capacidad de convicción de su redacción combinada con la sensación de urgencia, la capacidad de evadir la detección o el abuso de los servicios legítimos. A efectos del presente TFM, consideramos relevante recuperar del mencionado informe las acciones de mitigación específicas, a saber:

- Las organizaciones deben educar a su personal para identificar correos electrónicos falsos y maliciosos y mantenerse alertas. También deberían lanzar internamente ataques de phishing simulados para probar tanto su infraestructura como la receptividad de su personal.
- Las organizaciones deben usar pasarelas de correo electrónico de seguridad especializadas para filtrar el spam, que está estrechamente relacionado con las campañas de phishing.
- No haga clic en enlaces ni descargue archivos adjuntos si no está absolutamente seguro del origen de un correo electrónico.

72 <https://myonlinesecurity.co.uk/more-fake-natwest-emails-deliver-trickbot-banking-trojan/>

73 <https://cloudblogs.microsoft.com/microsoftsecure/2017/11/20/new-tech-support-scam-launches-communication-or-phone-call-app/?source=mmpc>

74 [https://www.theregister.co.uk/2017/11/03/fake\\_whatsapp\\_app](https://www.theregister.co.uk/2017/11/03/fake_whatsapp_app)

75 <https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers>

- No haga clic en los enlaces aleatorios y especialmente en los enlaces cortos que se encuentran en las redes sociales.
- Evite compartir información personal en las redes sociales, pe. tiempo de ausencia de la oficina o del hogar, información de vuelo, etc. considerando que los atacantes los utilizan activamente para recopilar información sobre sus objetivos.
- Verifique el nombre de dominio de los sitios web que visita para detectar errores tipográficos, especialmente para sitios web sensibles, pe. sitios web bancarios. Los atacantes generalmente registran dominios falsos que se parecen a los legítimos y los utilizan para "engañar" a sus objetivos. Buscar solo una conexión https no es suficiente.
- No haga clic en "habilitar contenido" (que habilita macros) en documentos de Microsoft Office. Las macros se aprovechan para descargar e instalar malware.
- Habilite la autenticación de dos factores cuando corresponda. La autenticación de dos factores puede evitar el robo de la cuenta de usuario.
- Use una contraseña sólida y única para cada servicio en línea. Reutilizar la misma contraseña en varios servicios es un problema serio de seguridad y debe evitarse en todo momento. El uso de credenciales sólidas y únicas en cada servicio en línea limita el riesgo de un posible robo de la cuenta solo al servicio afectado.
- En caso de enviar dinero a una cuenta, revise la información bancaria del destinatario a través de un medio diferente. Los correos electrónicos sin encriptar y sin firmar no deberían ser confiables, especialmente para casos de uso confidenciales como estos.
- Considere aplicar soluciones de seguridad que usan técnicas de aprendizaje automático para identificar sitios de phishing en tiempo real.

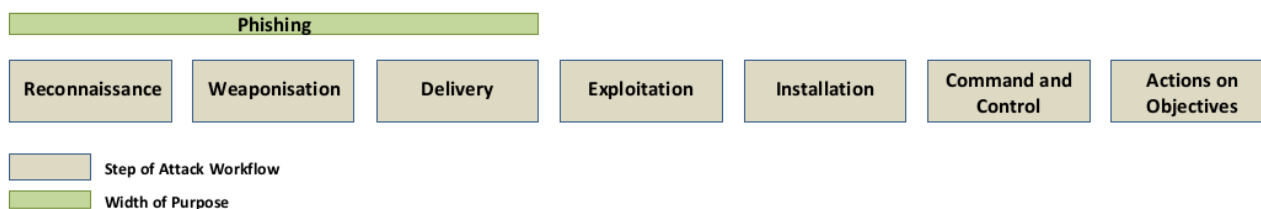


Ilustración 44: Posición del phishing en la "kill chain"

Para profundizar en el phishing como técnica de ataque basada en la ingeniería social, más concretamente para conocer las recomendaciones y soluciones de lucha contra esta técnica, se recomienda encarecidamente consultar los documentos técnicos e informes de los patrocinadores de APWG<sup>76</sup>. Se trata de las principales empresas del sector cuya actividad está orientada a la ciberseguridad y por tanto con una amplia experiencia y conocimientos.

<sup>76</sup> <https://www.antiphishing.org/resources/technical-whitepapers/>

## 15.2 Anexo II: Conjunto de herramientas de ingeniería social (SET)

La profundidad con la que se han tratado los distintos capítulos recogidos en el presente TFM aconseja no extender más su contenido. En este sentido, se ha decidido limitar la información del anexo II a una referencia a la web de descarga y al manual de usuario de "Social Engineer Toolkit" (SET) que en el momento de esta redacción se encuentra en su versión 6.0.

Software:	<a href="https://www.trustedsec.com/social-engineer-toolkit-set/">https://www.trustedsec.com/social-engineer-toolkit-set/</a> <a href="https://github.com/trustedsec/social-engineer-toolkit/">https://github.com/trustedsec/social-engineer-toolkit/</a>
Manual:	<a href="https://github.com/trustedsec/social-engineer-toolkit/blob/master/readme/User_Manual.pdf">https://github.com/trustedsec/social-engineer-toolkit/blob/master/readme/User_Manual.pdf</a> Preparado por: David Kennedy (Hacker, TrustedSec)

En palabras de la web de su fundador:

*<< Social-Engineer Toolkit (SET) fue creado y escrito por el fundador de TrustedSec. Es una herramienta de código abierto impulsada por Python destinada a pruebas de penetración en torno a la Ingeniería Social.*

*Se ha presentado en conferencias a gran escala, incluidas Blackhat, DerbyCon, Defcon y ShmooCon. Con más de dos millones de descargas, es el estándar para las pruebas de penetración de ingeniería social y cuenta con un gran respaldo dentro de la comunidad de seguridad.*

*Tiene más de 2 millones de descargas y está destinado a aprovechar los ataques tecnológicos avanzados en un entorno de tipo de ingeniería social. TrustedSec cree que la ingeniería social es uno de los ataques más difíciles de proteger y ahora uno de los más frecuentes. El kit de herramientas ha aparecido en varios libros, incluido el best seller número uno en libros de seguridad durante 12 meses desde su lanzamiento, "Metasploit: The Penetrations Tester's Guide", escrito por el fundador de TrustedSec, así como por Devon Kearns, Jim O'Gorman y Mati Aharoni. >>*