Trabajo de Fin de Grado

Grado en Ingeniería en Tecnologías Industriales

Las tecnologías de Internet, un riesgo para empresas y ciudadanos

MEMORIA

Autor: Berta de Moragas Jover i Carla Pascual Garcia
Director: Ramon Salvador Valles

Convocatoria: 06 2019

Escola Tècnica Superior
d'Enginyeria Industrial de Barcelona

Resumen

El desarrollo de las tecnologías de Internet ha creado un escenario en el que la mayoría de acciones y situaciones dependen y se realizan a través de ellas. No obstante, el uso de estas tecnologías supone un riesgo tanto para las empresas como para los ciudadanos. Estos riesgos nos llegan a través de los contenidos que nos encontramos en la web, por medio de herramientas de mensajería y redes sociales, en la descarga de archivos, en operaciones bancarias fraudulentas…

Este proyecto se centra en el estudio de casos reales en los que Internet ha sido un medio a través del que, empresas y ciudadanos, se han visto afectados de forma negativa.

El estudio de los riesgos de Internet se ha clasificado en ocho categorías: (1) suplantación de identidad, (2) privacidad, (3) política de *cookies*, (4) ciberataques (5) *phising*, (6) reputación *online*, (7) ciberdelincuencia y (8) *big data*. Esta clasificación se ha establecido tras haber realizado unas primeras búsquedas y observar que estas son las más comunes.

Tras examinar una serie de noticias y sucesos, se han seleccionado tres casos para cada una de las ocho categorías. Todos los eventos han sido estudiados de forma exhaustiva: se ha resumido cada suceso, se han estudiado sus consecuencias y, posteriormente, se han planteado y definido posibles soluciones. Finalmente, se ha establecido un conjunto de consecuencias y soluciones comunes para cada categoría, que permiten generalizar y establecer un comportamiento común para cada uno de los tipos de riesgos de Internet estudiados.

Como se verá más adelante, hemos aprendido y concluido que existen muchos tipos distintos de riesgos, y en todos los casos, no sólo la persona/empresa principal sale perjudicada por los escándalos, sino que, a su vez, todo su entorno. Por ejemplo, en el caso de afectación a una empresa toda la sociedad e incluso otras empresas que tengan una relación con ella, por pequeña que pueda ser, pueden verse afectadas. A su vez, en el caso de afectación a un individuo o grupo de individuos, todo aquel ciudadano/ empresa con el que éste mantenga relación, se verá afectado.

Sumario

Glosario

SUPLANTACIÓN DE IDENTIDAD

"Se produce cuando una persona malintencionada se apropia indebidamente de otra identidad digital y actúa en su nombre para conseguir información personal, publicar para desprestigiar, extorsionar o chantajear, etc. También se produce cuando una persona crea una cuenta o perfil con los datos de otra y se hace pasar por ella actuando en su nombre.

Las consecuencias de ser victima de suplantación de identidad incluyen: mostrar una imagen distorsionada de sí mismo en Internet; ser victima de burlas, insultos o amenazas, tener un descredito frente a otros; sufrir una perdida económica, etc." [1]

PRIVACIDAD EN INTERNET

"Condición de las informaciones que hacen referencia o pertenecen a una persona física o jurídica según la cual no se pueden hacer publicas sin su consentimiento." [2]

COOKIE

"Una *cookie* es un fichero de texto inofensivo que se almacena en el navegador cuando visita casi cualquier página web. La utilidad de la cookie es que la web sea capaz de recordar su visita cuando vuelva a navegar por esa página. [3]

Existen diferentes tipos de *cookies*:

- ***Cookies* técnicas:** Son las más elementales y permiten, entre otras cosas, saber cuándo está navegando un humano o una aplicación automatizada, cuándo navega un usuario anónimo y uno registrado, tareas básicas para el funcionamiento de cualquier web dinámica.
- ***Cookies* de análisis:** Recogen información sobre el tipo de navegación que está realizando, las secciones que más utiliza, productos consultados, franja horaria de uso, idioma, etc.
- ***Cookies* publicitarias:** Muestran publicidad en función de su navegación, su país de procedencia, idioma, etc."

CIBERATAQUES

"Conjunto de acciones ofensivas contra sistemas de información como bases de datos, redes computacionales, etc. hechas para dañar, alterar o destruir instituciones, personas o empresas.

El ciberataque puede dirigirse tanto a los equipos y sistemas que operan en la red anulando los servicios que prestan, como a los datos e información que se almacenan en bases de datos, robándolos o usándolos para espionaje." [4]

PHISING

"Se trata de un tipo de estafa que intenta obtener de la víctima sus datos, contraseñas, cuentas bancarias, números de tarjetas de crédito o del documento nacional de identidad, etc. mediante engaño para utilizarlos en el robo de fondos de sus cuentas.

A la persona que pone en práctica este delito se le conoce como *phisher*. Generalmente el *phisher* se hace pasar por una empresa o entidad pública y solicita los datos personales del usuario con la excusa de comprobarlos o actualizarlos. Esta petición de datos se realiza a través de un mensaje de teléfono móvil, una llamada telefónica, una ventana emergente durante la navegación por Internet o bien en un correo electrónico." [5]

REPUTACIÓN *ONLINE*

"Se conoce con ese nombre al prestigio o estima sobre una marca o una persona en Internet. No está completamente bajo el control de esta persona u organización, ya que todos los usuarios de Internet pueden contribuir a fabricarla aportando sus comentarios y opiniones." [6]

CIBERDELINCUENCIA

"Se dice de aquella actividad que por medio de la red (sea pública o privada) o a través de un sistema informático "tenga como objetivo atentar a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos"." [7]

BIG DATA

"El término se refiere a conjuntos de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad)

dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos y estadísticas convencionales o paquetes de visualización, dentro del tiempo necesario para que sean útiles." [8]

ROOTKIT

"Programa diseñado para proporcionar a los hackers acceso administrativo a su equipo sin su conocimiento." [9]

TRIPADVISOR

"Sitio web que proporciona a los viajeros la sabiduría de las masas para ayudarles a decidir dónde alojarse, cómo volar, qué actividades hacer y dónde comer. Además, TripAdvisor compara los precios de más de 200 sitios web de reserva para que los viajeros puedan encontrar el precio más bajo de su hotel ideal." [10]

INTERNET

"Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial." [11]

RIESGO

"Contingencia o proximidad de un daño." [12]

RED SOCIAL

"Plataforma digital de comunicación global que pone en contacto a gran número de usuarios." [13]

FACEBOOK

"Red social donde los usuarios registrados pueden participar e interactuar con personas o páginas en función de sus intereses. En esta plataforma el usuario dispone de un espacio para construir su propio perfil e introducir información personal." [14]

GOOGLE STREET VIEW

"Representación virtual de nuestro entorno en Google Maps que engloba millones de imágenes panorámicas. El contenido de Street View procede de dos fuentes: Google y sus colaboradores." [15]

VERIZON

"Empresa creada en el año 2000 por Bell Atlantic Corp y GTE Corp. Hoy en día, Verizon es una compañía de tecnología de comunicaciones global que ofrece la promesa del mundo digital a millones de clientes todos los días." [16]

AUTENTICACIÓN DE DOBLE FACTOR

"Capa adicional de seguridad que se ha diseñado con el objetivo de garantizar que el usuario sea la única persona que pueda acceder a su cuenta, aunque otra persona conozca su contraseña." [17]

VIRUS

"Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada." [18]

MALWARE

"Es el software que tiene como objetivo infiltrarse en el ordenador sin el conocimiento de su dueño y con finalidades muy diversas que pueden ir desde mostrarnos publicidad, bloquearnos el ordenador, dañar archivos, robarnos datos…" [19]

BOTNETS

"Son programas nocivos diseñados para tomar el control remoto de redes de ordenadores." [20]

Prefacio

Origen del proyecto

La idea de realizar este proyecto surgió al deparar en el desconocimiento que existe por parte de la inmensa mayoría de la población sobre todo lo que rodea a las tecnologías de Internet. Es por ello, y porque existen infinidad de riesgos que pueden afectar de muchas maneras distintas y pueden traer un gran número de consecuencias negativas, que surgió la necesidad de estudiar algunos de los principales riesgos. Se pretende entonces, acabar con el desconocimiento de cómo afrontar la situación si alguien se ve afectado por un escándalo como los que se van a estudiar, o aprender a prevenirlo.

Motivación

Este proyecto se nos ha presentado como una oportunidad para poder conocer mejor el mundo de Internet el cual es la base del mundo y sociedad en la que vivimos. Internet va a seguir creciendo de forma exponencial, por ello, concienciarnos y poder profundizar en una temática tan interesante y sobretodo útil como son los peligros y riesgos que corremos al usar Internet y estar conectados a las redes, fue considerada como una oportunidad, y no dudamos en aceptar y realizar nuestro trabajo de final de grado sobre ello.

1. Introducción

En la actualidad una gran parte de la población tiene integrado el uso de Internet en su día a día. Las oportunidades que nos brinda para facilitar muchas de las actividades humanas, y contribuir al propio desarrollo de los usuarios, son innegables, pero no se debe pasar por alto que esta herramienta también puede conllevar una serie de riesgos.

Las tecnologías de Internet pueden suponer ciertos tipos de riesgos para las empresas. Por una parte, pueden disminuir su poder de mercado. Por otra, aquellas empresas que no las utilicen, pueden cambiar adversamente la relación entre sus costes y los de sus rivales. Además, el uso de Internet expone a las empresas a la posibilidad de sufrir ciberataques, significando para ellas una gran pérdida económica. Asimismo, Internet puede significar un gran peligro para la sociedad, especialmente por lo que hace a los datos personales y confidencialidad de información de todos los ciudadanos que, alguna vez, hayan introducido datos en la red.

1.1. Objetivos del proyecto

En este proyecto como objetivo principal se quiere analizar cada uno de los sucesos y sus consecuencias con el fin de poder establecer una clasificación y, a partir de ello, encontrar posibles soluciones comunes o maneras de evitar todos los riesgos que el uso de las tecnologías de Internet conlleva.

A su vez, como fin secundario, se pretende poder llegar a concienciar de lo importante que es hacer un uso adecuado de las tecnologías de Internet para que estas resulten beneficiosas para la población y no jueguen en su contra, causando serios problemas como los que se estudiaran a lo largo del proyecto. Por ello, se tratará de buscar las medidas que permitan evitar que los usuarios se encuentren con problemas en la red.

1.2. Alcance del proyecto

El proyecto incluye la definición y descripción de cada una de las noticias, así como su análisis que permite establecer las consecuencias y soluciones de las mismas. Cada riesgo se limita a un estudio de tres noticias. Una vez se han analizado por separado se establecen consecuencias y soluciones comunes para cada uno de los riesgos descritos y, finalmente, se mencionan las leyes que se aplican en Europa y España para casos como los tratados.

2. Estado del Arte

Para enfocar el trabajo se ha querido realizar un análisis de 4 estudios o artículos en los que sus autores han escrito y tratado el tema de la seguridad en Internet. Se ha decidido realizar dicha tarea con el fin de ver cuales son los riesgos más comunes en Internet para empresas y usuarios, y posteriormente poderlo contrastar con las noticias que tienen afectación a gran escala, que se analizaran en el siguiente apartado.

Para cada uno de los artículos se ha procedido a realizar una tabla analítica con la que se ha podido valorar y analizar como debe hacerse la clasificación de los riesgos para el estudio que se realizará más adelante.

A continuación, se muestran los distintos artículos analizados.

En el primero de ellos se clasifican los tipos de amenazas a las que se puede ver sometido un usuario al navegar por la red, además de analizar y caracterizar a los intrusos y ataques que enfrentan los dispositivos y servicios de IT. A su vez se proponen precauciones a tomar con el fin de evitar o reducir dichos ataques. [21]

	Ataques											Precauciones						
	Físico	Reconocimiento	Denegación de servicio	Acceso	Privacidad			Contraseña	Delitos cibernéticos	Ataques destructivos	Ataques de control de supervisión y adquisición de datos						Privacidad	Cantidad de infromación
M. Abomhara y G.M.Kølen	Afecta componentes de hardware	Descubrimiento y asignación no autorizados de sistemas, servicios o vulnerabilidades.	Intento de hacer que una máquina o recurso de red no esté disponible para los usuarios previstos.	Personas no autorizadas obtienen acceso a redes o dispositivos a los que no tienen derecho de acceso.	Minería de datos: permite a los atacantes descubrir información que no se anticipa en ciertas bases de datos.	Ciberespionaje: uso de técnicas de craqueo y software malicioso para espiar u obtener información secreta de individuos, organizaciones o el gobierno	Eavedropping: escuchar una conversación entre dos partes.	Seguimiento: los movimientos de un usuario pueden ser rastreados por el número de identificación único (UID) del dispositivo. El seguimiento de la ubicación de un usuario facilita su identificación en situaciones en las que	Intentos para duplicar una contraseña de usuario válida.	Internet y los objetos inteligentes se utilizan para explotar a los usuarios y los datos para obtener beneficios materiales, como el robo de propiedad intelectual, el robo de identidad, el robo de marca y el fraude	El espacio se utiliza para crear una interrupción y destrucción a gran escala de la vida y la propiedad.	Ataques de control de supervisión y adquisición de datos	Confidencialidad	Integridad	Autentificación y autorización	Disponibilidad	Responsabilidad	En los dispositivos; a la hora de comunicar o usar redes sociales, mensajería etc; almacenamiento; identidad; localización	La cantidad de datos almacenados en dispositivos e internet también debe ser limitada

Figura 2.1: Tabla resumen artículo 1

El segundo artículo defiende a partir de un estudio realizado cuales son los métodos preventivos que actualmente los ciudadanos del mundo que hacen uso de las tecnologías de internet aplican con el fin de no sufrir ataques. Y, a su vez menciona y estudia qué impide que dichas personas tomen ciertas medidas. [22]

	Métodos preventivos				¿Qué impide que las personas tomen medidas?			
Ruogu Kang1, Laura Dabbish1,2, Nathaniel Fruchter1, Sara Kiesler.	Usar wifi privado ante wifi público.	Usar mecanismos de protección de datos: contraseñas, usar códigos encriptados, tener en cuenta certificaciónes y pasos de verificacion implementados por sitios web.	Uso de antivirus.	Reducir el uso o tener cuentas privadas en las redes sociales.	Falta de conciencia y preocupación de los peligros de Internet.	Tomar medidas de protección implica sacrificar la eficacia o la conveniencia.	Poca utilidad de las herramientas o el software de protección de la privacidad.	Sentimiento de impotencia y falta de conocimiento sobre los procedimientos para tomar medidas de protección.

Figura 2.2: Tabla resumen artículo 2

El tercer artículo resume los ataques más comunes que se dan en Internet y se describe en que consiste cada uno de ellos. [23]

	Ataques									
	Virus	Inyectores en el sistema de arranque	Espionaje	Hackeo	Gusano informatico o worm	Troyanos	Suplantación de identidad	Negación de servicio	Bombardeo de correos y spam	Phishing
Olalekan Adeyinka	Son programas que infectan y se propagan por los archivos del dispositivo, que se ejecutan cuando se abre el archivo. Pueden eliminar información o insertar frases en el documento.	Son un tipo de virus, cada vez que el dispositivo se enciende, este virus se va propagando.	Se refiere al acceso a las comunicaciones por parte de alguien no autorizado.	Se trata de atacar al sistema cuando se descubre un punto débil en él. Pueden acceder al sistema e intentar incorporar información no deseada, asi como pueden llegar a acceder a servidores para robar información.	Es un programa que se propaga a través de la red. A diferencia de los viruses, no necesitan infectar un programa para propagarse.	Son programas que parecen inofensivos para el usuario, pero realmente tienen un propósito malicioso. Suelen usarse para tener acceso remoto a un dispositivo o infectar al mismo con viruses.	Se da este tipo de ataque cuando una persona se hace pasar por otra con fines maliciosos.	Ocurre cuando un sistema se colapsa debido a que intenta establecer muchas comunicaciones con el usuario.	Se caracteriza por el envío repetitivo de un mensaje de correo electrónico idéntico a un dirección particular.	Un tercero consigue información confidencial de un usuario con fines de lucro.

Figura 2.3: Tabla resumen artículo 3

Finalmente, en el último artículo se comentan las vulnerabilidades más comunes de Internet a las que se puede enfrentar un usuario y se especifican cuales son las acciones que deben llevarse a cabo para garantizar la máxima seguridad de los usuarios de la red. [24]

	Ataques	
	Vulnerabilidades comunes de los sistemas	Soluciones para garantizar la seguridad
Colin Tankard	Permitir a los usuarios usar contraseñas poco seguras.	Autenticación y autorización.
	Augmentan los problemas de privacidad a medida que se acumulan datos personales.	Monitorización de los sistemas.
	No encriptar las transmisiones de información.	Encriptación de las comunicaciones.
	Fallos en las interficies de la red.	Antes de la producción, evaluación de la seguridad y probar los nuevos productos.
	No usar encriptación cuando se descargan softwards en actualizaciones.	Segmentación de la red.

Figura 2.4: Tabla resumen artículo 4

3. Clasificación y descripción de casos según sus riesgos

Este proyecto se basa principalmente en el estudio de casos reales y sucesos relacionados con el uso de Internet, que hayan afectado a empresas o a usuarios particulares.

Para ver como se va a enfocar el proyecto, se ha decidido buscar cuáles son los escándalos de Internet de los que mas se ha hablado en las ultimas décadas, que han afectado a empresas o usuarios. Una vez se han seleccionado las noticias, se han clasificado según el tipo de riesgo que implican, basándose en las clasificaciones de los riesgos que se han podido extraer de los artículos estudiados con anterioridad. De aquí han salido los ocho riesgos de los que se hablan a lo largo de todo el trabajo. Finalmente, en los siguientes apartados se analizan las consecuencias y soluciones de los casos analizados, y se definen acciones comunes con el fin de evitar o prevenir que dichos casos ocurran de nuevo.

3.1. Suplantación de identidad

3.1.1. Leah Palmer

28 de febrero de 2015

“Ruth Palmer, de Brighton, descubrió una serie de perfiles falsos en Internet con imágenes suyas, pero bajo los nombres de otras personas.

Un *catfish* es un término que se usa en Internet para describir a la gente que pretende ser alguien que no es, usualmente con la intención de que un tercero se enamore de él.

En el caso de Ruth, el perfil falso llevaba el nombre de Leah Palmer y llevaban activos en redes sociales tales como Instagram y Twitter desde hacia mas de tres años.

El imitador estableció una serie de relaciones sociales y amorosas en línea con varias personas siempre usando el nombre e imágenes y vida de la víctima, Ruth. El estafador engañó a sus víctimas para que pensaran que al igual que Ruth, había emigrado de Brighton a Dubai.

Esta persona envió tarjetas de Navidad, tarjetas de cumpleaños e hizo reservas para cenas para sus amantes de Internet, todo al mismo tiempo que utilizó las imágenes y los detalles de Ruth de su vida.

También intercambiaron imágenes sexualmente explícitas con sus víctimas usando los

cuerpos de otras personas que obtuvieron mediante las redes.

Ruth se quejó a la policía de Sussex, pero su caso fue remitido a Action Fraud, el centro nacional de informes del Reino Unido por fraude y delitos relacionados con Internet. El servicio está a cargo de la Policía de la Ciudad de Londres, que trabaja junto con la Oficina Nacional de Inteligencia contra el Fraude.

Pero a pesar de la gravedad del caso, Action Fraud dijo que no hubo criminalidad." [25]

3.1.2. Perfil falso en Facebook

25 de junio de 2013

"La Guardia Civil ha detenido en Maracena, municipio del área metropolitana de Granada, a una joven de 23 años acusada de varios delitos, entre ellos difamación y revelación de secretos de particulares, al colgar en la red social Facebook fotografías de otra joven que esta tenía en su perfil de la red Tuenti.

La mujer ahora detenida creó un perfil falso en Facebook y se apropió de las fotografías que la víctima compartía con sus amigos en Tuenti, entre los que se encontraba ella, y les fue añadiendo comentarios obscenos e injuriosos, según informa el Instituto Armado.

El equipo de Policía Judicial de la Guardia Civil de Maracena se hizo cargo de investigar los hechos denunciados y una de las primeras pesquisas fue solicitar mediante sendos oficios judiciales a Facebook, en Estados Unidos, el número IP de la persona que creó el perfil.

Posteriormente se hizo la misma solicitud a la compañía telefónica que suministraba Internet a dicho número IP, el nombre del propietario de la línea, averiguando así que se trataba de un vecino de Maracena. Cuando la Guardia Civil le preguntó a la denunciante si conocía a alguien en esta dirección de Maracena, la joven, sorprendida, dijo que una conocida suya que en estos momentos salía con un chico que había sido novio suyo.

La Guardia Civil citó a esta joven en el Puesto de Maracena y al preguntarle si conocía el perfil de Facebook desde el que se habían vertido comentarios injuriosos contra otra chica del pueblo acabó confesando que había sido ella la autora de estos hechos tras unos comentarios que la víctima hizo al conocer que la joven ahora detenida tenía una relación con su ex novio. La joven, tras prestar declaración con su abogado, quedó en libertad." [26]

3.1.3. Hombre suplanta la identidad de su mujer

30 de octubre de 2018

“La Policía Nacional ha detenido a un hombre de 45 años en Lugo como autor de un delito de revelación de secretos y otro de violencia de género por pedir, a través de diversas redes de contactos, «secuestrar», «acosar» e incluso «violar» a su amante, cuya identidad suplantó en Internet, donde volcó datos personales. Según informó el Cuerpo Nacional de Policía, una mujer se presentó en la comisaría provincial de Lugo el pasado día 26 para denunciar que había «perfiles falsos» con fotografías suyas en diversas redes sociales.

Los agentes que se hicieron cargo de la investigación lograron identificar, tras revisar diversas conversaciones en varias redes de contactos, al supuesto autor de esa suplantación de identidad en Internet, que resultó ser un hombre con el que la denunciante mantenía una relación sentimental.” [27]

3.2. Privacidad

3.2.1. *Google Street View*

12 de marzo de 2013

“En un acuerdo judicial con 38 estados, el gigante de Internet accedió a destruir correos electrónicos, contraseñas e historiales web recogidos partir de las redes inalámbricas domésticas, mientras los vehículos de su servicio Street View tomaban fotografías de diferentes barrios entre 2008 y 2010.

"Este acuerdo aborda las cuestiones de privacidad y protege los derechos de las personas cuya información fue recogida sin su permiso", dijo el fiscal de Nueva York, Eric Schneiderman, en un comunicado.

"Los consumidores tienen derecho a proteger su información personal y financiera de un uso indebido y no deseado por parte de empresas como Google", agregó.

El acuerdo obliga a Google a destruir la información personal recopilada mientras los vehículos de Street View recorrían el país fotografiando los barrios para captar imágenes callejeras de 360 grados que ahora ofrece con su servicio Google Maps.

Google ha dejado de recoger datos y se ha comprometido a no hacerlo sin previo aviso y consentimiento, según el comunicado.” [28]

3.2.2. Escándalos de privacidad – Facebook

29 de diciembre 2018

“En marzo, Facebook se enfrentó a la mayor crisis de su historia cuando se conoció que la

consultora británica Cambridge Analytica había accedido a datos de 50 millones de usuarios de la red social, cifra que más tarde se elevó a 87 millones de personas. Cambridge Analytica usó esta información de carácter personal, adquirida sin el consentimiento de los usuarios, para realizar campañas segmentadas con el fin de influir en el voto de los electores en las presidenciales de Estados Unidos." [29]

3.2.3. Datos expuestos por Play Station *Network*

27 de abril de 2011

"Una intrusión a la red de Sony expuso los datos de 77 millones de cuentas de usuario.

La empresa descubrió un acceso no autorizado al sistema, que habría extraído los siguientes datos de los usuarios: nombre, dirección (estado, ciudad y código postal), dirección de correo electrónico, fecha de nacimiento y contraseña y usuario de PlayStation *Network*. Sin embargo, la empresa tampoco descartó que se hayan extraído otros datos más sensibles como el historial de compras o los datos de las tarjetas de crédito, ya que manifestó que "no podemos obviar esa posibilidad"." [30]

3.3. *Cookies*

3.3.1. NSA utiliza *cookies* para identificar objetivos a espiar

11 de diciembre de 2013

"La Agencia de Seguridad Nacional (NSA) de Estados Unidos recurre a las '*cookies*' de Google para consultar la actividad previa del usuario y conocer sus gustos con el fin de identificar los objetivos a espiar.

Según una investigación del diario estadounidense «The Washington Post», unas diapositivas de la NSA proporcionadas por el excontratista de la NSA Edward Snowden confirmarían que la agencia estuvo utilizando estas técnicas de rastreo para identificar objetivos a *hackear* y reforzar la vigilancia.

La NSA y el GCHQ (la agencia de inteligencia del Reino Unido) han encontrado «un uso particular» para un mecanismo de seguimiento específico de Google, conocido como la *cookie* PREF, que incluye códigos numéricos que permiten identificar el navegador de un usuario.

Además del seguimiento, esta cookie permitiría aislar las comunicaciones de una persona

entre el mar de datos de Internet con el objetivo de enviar un software capaz de *hackear* el ordenador de esa persona.

La NSA habría utilizado esta técnica para seguir a personas bajo sospecha o, incluso, para localizarles a través de la conexión a Internet de su terminal móvil, rastreando la ubicación de cada dispositivo." [31]

3.3.2. *Cookies* pueden costar dinero

6 de agosto de 2010

"La mayoría de los usuarios de la red saben que los sitios web colocan *cookies* en los dispositivos (es cómo recuerdan su nombre y detalles de dirección). Pero ¿de alguna manera lo rastrean, elevan los precios cuando regresa a un sitio web para realizar una compra, sabiendo que ha estado allí y está interesado en el artículo?

La primera vez que un usuario buscó un vuelo, el precio del mismo era de £ 187, pero al volver a la web solo unos minutos más tarde, el precio había cambiado a £ 212.

Las aerolíneas usan un modelo llamado "precios dinámicos". Las *cookies* en su ordenador le indicaron al sitio web que el usuario ya había estado buscando ese vuelo para tomar una decisión.

La pagina web recordaba los detalles de la búsqueda del usuario, conocía el destino que estaba buscando y, una vez más, le indicaba £ 212 por el vuelo. Una vez borradas las *cookies* y eliminado el historial de navegación, comenzando de nuevo el proceso de reserva, el sitio web ya no conocía los datos y no rellenó ninguno de los campos de información. El precio del vuelo entonces descendió a £ 187." [32]

3.3.3. Verizon usa *supercookies* sin consentimiento

9 de marzo de 2016

"Verizon Wireless insertó *supercookies* imposibles de borrar en las sesiones de navegación de sus usuarios.

Las *súpercookie* son mucho más difíciles de borrar y no pueden evadirse con una sesión de navegación privada. Pueden recolectar información sobre la actividad web en forma anónima, ya sea para que la propia compañía la use o la venda a terceros para campañas publicitarias dirigidas.

Verizon no aclaró estas prácticas entre diciembre de 2012 y octubre de 2014, violando una regulación de 2010 de la Comisión de Comunicación Federal (Federal Communications

Commission o FCC).” [33]

3.4. Ciberataques

3.4.1. Sony CD Spyware

19 de noviembre de 2005

“Mark Russinovich, un investigador de seguridad informática descubrió que Sony BMG CD instalaba en los ordenadores un software anti piratería secreto basado en un *rootkit*, para evitar la copia de sus CDs originales. El *rootkit* se usaba para ocultar la existencia de su software de gestión de derechos digitales.

En forma de *rootkit* indetectable para los antivirus, este sistema transmitía información de la IP del usuario del ordenador cuando este lo reproducía en él (incluso sin intenciones de copiarlo).” [34]

3.4.2. Yahoo sufre ataque *hacker*

22 de octubre de 2016

“La información de 500 millones de cuentas de la empresa estadounidense se puso a la venta en el mercado negro.

Yahoo desveló la existencia de una “masiva” brecha en la seguridad de su servicio de correo electrónico producida en 2014 y que afectó a más de 500 millones de cuentas.

El robo de datos lo realizó un *hacker* autodenominado Peace. El atacante obtuvo datos de los correos como nombres de usuarios, contraseñas y fechas de nacimiento de cuentas del año 2012.” [35]

3.4.3. Robo digital de cuentas – supermercados Tesco

7 de noviembre de 2016.

“A algunos usuarios les sustrajeron hasta 600 libras y se suspendieron las compras *online*.

Tesco Bank, propiedad de la cadena de supermercados del mismo nombre, la mayor del Reino Unido tiene siete millones de clientes. 40.000 cuentas sufrieron ataques digitales, que en 20.000 casos consistieron en robos de dinero. Alguien entró en las cuentas por medios informáticos y se llevó el dinero de los clientes.

Una posibilidad sobre lo que pudo haber ocurrido es que una red de delincuentes grabase a

las víctimas en los cajeros y accediese a sus claves. Otra opción es que un empleado de Tesco Bank hubiese accedido a la base de datos y hubiese filtrado a los piratas informáticos la información." [36]

3.5. Phishing

3.5.1. Estafa falso abono Mercadona

14 de enero de 2019

"La Guardia Civil publicó alertas para advertir de una estafa propagada por las redes sociales, correos electrónicos y aplicaciones de mensajería móvil en la que se empleaba el nombre de Mercadona para ofrecer un falso bono por importe de cien euros. El fraude detectado por los cuerpos de seguridad persigue la obtención de datos personales y bancarios.

Los estafadores incluyen un enlace que solicita contraseñas y cuentas bancarias, en lo que conoce en la jerga de los delitos informáticos como *phishing*." [37]

3.5.2. Fraude vales descuentos Zara

25 de septiembre de 2017

"A través de WhatsApp, circuló una campaña falsa de cupones de 500 euros de regalo para gastar en una popular tienda, Zara. Este mensaje incluía un enlace acortado que llevaba al usuario hasta una falsa encuesta.

Al hacer clic en el enlace, el usuario era dirigido a una fraudulenta página web en la que se le animaba a participar en una sencilla encuesta para poder ganar 500 euros a gastar en el citado comercio.

Tras completarla, el fraude obligaba a la víctima a propagar la estafa. Era, entonces, cuando el usuario tenía que introducir sus datos personales, como dirección de correo electrónico o número de teléfono, como paso final para conseguir el suculento premio que, evidentemente, nunca llegaría. Los objetivos que perseguía este fraude era robar los datos personales de los usuarios." [38]

3.5.3. Robo en Argentina a causa del *phising*

7 de septiembre de 2017

"Los atacantes crearon una réplica de la página principal de la Banca Internet Provincia (BIP), que lucía muy similar a la original.

Utilizaron la técnica de los ataques homográficos, en los que se cambia algún carácter de la

URL para que a simple vista parezca la original. En este caso, informa La Nación, suplantaron la “a” por la “s”, y crearon un sitio con la dirección bancsprovincia.bancsInternet.com.ar.

A primera vista, más de un usuario pasaría por alto el error y accedería con sus credenciales sin dudarlo. Y eso fue lo que hizo el contador Paolo Salinas, que se desempeñaba en el cargo desde hace 18 años y se encargaba de emitir los pagos.

Salinas ingresaba al sistema de BIP cada día buscando la URL en Google. Pero los atacantes habían aplicado técnicas de Black Hat SEO para posicionar su sitio falso (la réplica) entre los primeros resultados de búsqueda de términos relacionados. Así que, sin saberlo, el contador inició sesión en el sitio fraudulento y entregó sus credenciales a los estafadores.

Una vez que se ingresaban credenciales y estas eran enviadas al cibercriminal, el sitio redirigía a la versión original para no despertar sospechas. Así, el usuario podía creer que debido a un problema el sistema no tomó la clave y entonces, la vuelve a ingresar.” [39]

3.6. La reputación *online*

3.6.1. Hotel Villa Venecia valorado el mejor de la comunidad de Benidorm

29 de enero de 2016

“El exclusivo establecimiento de cinco estrellas ubicado en el casco antiguo de Benidorm se posicionó durante 2015 como el primero de los 21 hoteles de cinco estrellas de la región en reputación *online*. Este hecho puso de manifiesto la buena imagen *online* del hotel creada sobre todo con las opiniones que los clientes vertieron sobre él en la red, portales de opinión y agencias *online*. Entre estas menciones, el 99% de las opiniones positivas recibidas destacaban la labor del personal del hotel, lo que reforzaba el esfuerzo de los empleados y la apuesta de la cadena por la atención al cliente.” [40]

3.6.2. El efecto de la reputación *online* en Tripadvisor

27 de noviembre de 2015

“Los clientes de hoteles, restaurantes y otras atracciones escriben aproximadamente 115 comentarios por minuto en el sitio de opiniones, que desde su creación en 2000 no deja de crecer y agregar nuevas funcionalidades.

Un estudio conducido por la Universidad de Dublín, Irlanda, examinó las críticas de hoteles en Las Vegas entre 2007 y 2009 y las comparó con las opiniones de los hoteles de Irlanda durante el mismo período de tiempo.

Mientras que en Las Vegas las críticas se mantuvieron aproximadamente constantes durante el período analizado, en Irlanda, mercado turístico al que Tripadvisor había llegado recientemente, las críticas *online* crecieron de 3,6 a 3,8 burbujas.

El hallazgo fue que los gerentes de hoteles irlandeses se hicieron eco de las críticas recibidas y actuaron en consecuencia para obtener mejores opiniones en Tripadvisor, lo que fue mejorando la calidad de servicio ofrecida y consecuentemente realimentando en forma positiva a los huéspedes y sus nuevas críticas." [41]

3.6.3. Ese tuit te puede costar el trabajo

23 de febrero de 2016

"Cada vez más empresas revisan las redes sociales de sus empleados y de los candidatos a un puesto de trabajo.

Una foto desafortunada o un comentario inoportuno en cualquiera de las redes sociales como Twitter o Facebook puede suponer un motivo de descarte en un proceso de selección de personal.

Un 88% de los responsables de recursos humanos de las compañías reconoce que consulta la reputación *online* de los posibles empleados antes de contratarlos. De echo, un 28% de los participantes en la encuesta aseguró haber rechazado ya a algún candidato por lo que encontró en sus perfiles." [42]

3.7. La ciberdelincuencia

3.7.1. Redes Wifi en aeropuertos y demás lugares públicos

26 de julio de 2018

"Empresas de ciberseguridad aseguran que este tipo de conexiones pueden ser utilizadas por delincuentes para robar información como claves de cuentas bancarias y correos electrónicos.

El impacto que han generado los dispositivos móviles en la vida de sus usuarios ha sido tal que incluso almacenan información sensible como claves de cuentas bancarias.

Una de las modalidades que utilizan los ciberdelincuentes es utilizar las redes wifi públicas, en zonas concurridas como aeropuertos y centros comerciales, como anzuelos para que las personas entren en su red y así llegar a espiar o instalar virus en los celulares de sus víctimas.

Parte de las estrategias que utilizan los delincuentes es crear una red que aparenta ser la oficial del sitio en el cual se encuentra la persona." [43]

3.7.2. ¿Puede un *hacker* dejar sin luz a Ucrania?

2 de noviembre de 2018

"Durante unas horas cerca de 230.000 personas quedaron sin electricidad en Ucrania. La raíz de este mal no se debía a una saturación de la central eléctrica, tampoco a factores naturales ni errores humanos. Alguien, desde un ordenador decidió con tan solo un clic afectar a toda una población.

A este ciberataque se le conoció como Black Energy, uno de los casos más sonados al momento de hablar sobre afecciones a compañías que proveen servicios indispensables, también conocidas como infraestructuras críticas.

Un año más tarde, el país volvió a ser víctima de un ciberataque de este tipo. El responsable del nuevo apagón fue otra amenaza denominada como Industroyer.

Anton Cherepanov desveló al que sería el principal grupo cibercriminal responsable de ataques a infraestructuras críticas en la actualidad, Telebots.

El grupo de Cherepanov descubrió que los códigos maliciosos empleados para afectar a los ucranianos eran similares, lo que de entrada hizo sospechar al investigador de que un grupo en concreto fue el responsable de ambos ataques." [44]

3.7.3. Cibercriminales filtran datos de 14.000 tarjetas de crédito en Chile

27 de Julio de 2018

"Las autoridades chilenas investigaban la filtración de una base de datos de alrededor de 14.000 tarjetas de crédito con información confidencial de unos 19 emisores bancarios y no bancarios, algunos de ellos extranjeros, informaron fuentes oficiales.

El grupo de cibercriminales ShadowBrockers que apareció por primera vez en 2016 cuando publicaron filtraciones que afectaron a la Agencia de Seguridad Nacional (NSA)

estadounidense, se adjudicó el robo y la divulgación en redes sociales de los números de las tarjetas, el código de seguridad y su fecha de expiración ocurrido el miércoles.

Según el ministro, el robo de la información de las tarjetas no se produjo en el sistema bancario. Las autoridades manejaban las hipótesis de que los *hackers* se introdujeron por una cuenta internacional de Correos de Chile o desde los servidores de algún comercio. Sin embargo, los atacantes explicaron que obtuvieron los datos "mediante portales de pago directamente asociados a sus bancos".

El superintendente de bancos, Mario Farren, admitió hoy que no hay garantías de impedir que estas situaciones se repitan.

La filtración se produjo dos meses después que unos piratas informáticos robaron diez millones de dólares al Banco de Chile, que su mayor parte aparecieron más tarde en cuentas de Hong Kong. Tras ese incidente, el Gobierno pidió ayuda al Fondo Monetario Internacional para fortalecer la seguridad informática del sistema financiero." [45]

3.8. Big data

3.8.1. Cómo Netflix usó el *big data* para crear un éxito

17 de abril de 2017

"En 2013 se lanzó House Of Cards, una serie producida por Netflix para su plataforma en *streaming* inspirada en una serie británica retrasmitida por la BBC en el año 1990.

Todos en Netflix estaban seguros del éxito de House Of Cards antes incluso de la emisión del primer capítulo ya que la decisión de producir dicho título, así como cada momento y detalle de la propia grabación y del guion, están basados en los resultados obtenidos de un algoritmo que había analizado previamente todos los gustos y preferencias de los usuarios de Netflix.

Por lo tanto, fue una serie creada desde el momento cero, para el gozo y disfrute de sus usuarios. Fue así como el *big data* dio a Netflix la receta perfecta para crear todo un éxito tanto en audiencia como en reconocimiento.

Tal fue la influencia del *big data* en House Of Cards, que Netflix incluso sabía según los gustos de sus usuarios, a qué personajes tenía que "matar", incluidos protagonistas. De esta manera fue como el *big data* influyó en el desenlace incluso de los episodios finales con el objetivo de mantenernos "enganchados" hasta el final." [46]

3.8.2. Cómo reinventar un modelo de negocio

28 de octubre de 2015

"Farecast es una empresa estadounidense fundada en 2003 que, a partir de miles de millones de registros, era capaz de calcular la probabilidad de que un billete de avión subiera o bajara de precio, y estimaba el mejor momento para comprar. En 2009 Microsoft pagó más de 100 millones de dólares por esta compañía. La tecnología de predicción de precios es aplicable no sólo a los billetes de avión, también a las habitaciones de hotel y a muchos otros productos y servicios. Sólo evaluando esa cantidad tan enorme de datos es posible estimar probabilidades con acierto." [47]

3.8.3. La reelección de Obama

12 de abril de 2018

"Tras su primer mandato, el presidente de los EE. UU., Barack Obama, decidió utilizar *big data* para su reelección en 2012. Un centenar de personas trabajaron en el departamento de analítica de la campaña, algunas de ellas exclusivamente centrados en la interpretación de los datos recibidos. Tras un primer análisis, los esfuerzos de la campaña se enfocaron en tres aspectos: registro (recoger datos de los votantes convencidos), persuasión (dirigirse a los dudosos de una forma eficaz) y voto del electorado (asegurarse de que los partidarios fueran a ejercer el voto sí o sí). Y, por primera vez, los tres equipos más importantes de las campañas electorales: el de campo, el digital y el de comunicación, trabajaron con una estrategia unificada con los respectivos datos de cada uno.

El motor de todo, la plataforma inteligente utilizada fue HP Vertica. Entre las acciones más efectivas que permitía esta plataforma estaban: recoger datos a pie de campo y realizar una valoración muy rápida vía notificaciones email por parte del equipo *online* (se mejoraba en tiempo y eficiencia); o detectar los nichos en los que funcionaría mejor la publicidad en TV cruzando datos de los votantes con otros demográficos, audiencias, precios de publicidad, programas… (se mejoró en impacto y segmentación). Con su analítica, el equipo de Obama optimizó la comunicación y mejoró la respuesta del electorado afín, permitiendo no malgastar recursos, tiempo y dinero en los votantes que no eran partidarios de su partido." [48]

4. Consecuencias

En este apartado se muestran cuales han sido los efectos que se derivan de las noticias anteriormente explicadas y que han supuesto un riesgo para usuarios y empresas.

4.1. Suplantación de identidad

4.1.1. Leah Palmer

A causa de los perfiles falsos expuestos en Internet, se difamaron fotos personales por las redes sociales sin el consentimiento de la persona protagonista de las fotografías. Pudo tratarse de fotos íntimas de la persona afectada.

A su vez, afectó a las personas con las que el *catfish* intercambió información y se comunicó. Estas víctimas dieron información personal y hasta imágenes suyas (más o menos íntimas). También se vieron afectadas las personas que rodeaban socialmente a la víctima cuya identidad había sido suplantada.

4.1.2. Perfil falso en Facebook

La joven que cometió el delito quedó en libertad, aún y habiendo difamado información personal de la persona afectada sin su consentimiento. A su vez, esa joven también divulgó comentarios obscenos e injuriosos haciéndose pasar por la víctima.

4.1.3. Hombre suplanta la identidad de su mujer

A causa de la suplantación de identidad de su mujer, se difamó tanto información personal de la víctima como imágenes suyas comprometidas para atraer conversaciones con el género masculino. Quien se hacía pasar por la mujer, solicitaba sexo, lo que ocasionó que la víctima encontrara a hombres en cada uno de los lugares donde iba como en la vía pública donde intentaban hablar con ella.

4.2. Privacidad

4.2.1. *Google Street View*

A causa de la grabación de imágenes de propiedades privadas expuestas al público sin el consentimiento de las personas afectadas, los ciudadanos pierden su privacidad. Además, se produce una obtención de datos personales sin consentimiento del usuario.

4.2.2. Escándalos de privacidad – Facebook

El hecho de que Cambridge Analytica accediese a los datos de 87 millones de usuarios implicó que estos datos personales se usaran para otros fines. Este escándalo afectó también a la reputación de Facebook, que sufrió en Bolsa una fuerte caída y supuso el comienzo de una campaña, que anima a los usuarios a darse de baja en la red social. La fuga de datos provocó la apertura de investigaciones sobre las prácticas de la compañía en materia de tratamiento e intercambio de datos.

4.2.3. Datos expuestos por Play Station *Network*

A causa de la intrusión a la red de Sony se obtuvieron datos personales de los usuarios de Play Station (nombre, dirección, estado, ciudad, código postal, dirección de correo electrónico, fecha de nacimiento, contraseña y usuario de Play Station *Network*.).

También se consiguieron los datos de tarjetas de crédito de los mismos usuarios de Play Station.

4.3. *Cookies*

4.3.1. NSA utiliza *cookies* para identificar objetivos a espiar

Debido al uso de *cookies* de Google por parte de la NSA, aparecieron anuncios y ofertas con objetivos comerciales. A su vez, se conocieron los datos (como intereses etc.) de la persona afectada y todas las comunicaciones del afectado se perdieron entre el mar de datos de Internet. Además, se pudo rastrear la ubicación de cada dispositivo.

4.3.2. *Cookies* pueden costar dinero

A causa del uso de *cookies*, se modificaban los datos en Internet según los intereses de la persona afectada. Así, aparecían anuncios y ofertas con objetivos comerciales y los precios se incrementaron al realizar compras por Internet.

Con ellas también se rastreaban los dispositivos del usuario afectado (ubicación, páginas web consultadas etc.)

4.3.3. Verizon usa *supercookies* sin consentimiento

Verizon Wireless tuvo que pagar un millón de dólares por haber insertado *supercookies* imposibles de borrar en las sesiones de navegación de sus usuarios.

4.4. Ciberataques

4.4.1. Sony CD Spyware

Cada ordenador que intentó reproducir un disco Sony BMG protegido contra la copia, era susceptible a ser invadido por virus y otros programas maliciosos. Por ello, Sony pagó 150 dólares a cada usuario afectado.

4.4.2. Yahoo sufre ataque *hacker*

El atacante que consiguió entrar en las cuentas de los usuarios de Yahoo intentó vender los datos de unas 200 millones de cuentas. El valor de esta venda de datos ascendió a unos 1800 dólares.

4.4.3. Robo digital de cuentas – supermercados Tesco

Los clientes reportaron pérdidas de hasta 600 euros.

4.5. Phising

4.5.1. Estafa falso abono Mercadona

Los estafadores consiguieron obtener los datos personales y bancarios de forma fraudulenta de aquellos usuarios que cayeron en la estafa e ingresaron sus datos en la página web falsa.

4.5.2. Fraude vales descuentos Zara

Los estafados pudieron ser inducidos a instalarse aplicaciones maliciosas, ser suscritos a SMS Premium y sus datos ser utilizados por terceros para dar de alta perfiles falsos en páginas web de citas (suplantación de identidad).

La venta de una lista de correos electrónicos con un millón de registros se pudo vender en el mercado negro por más de 6.000 euros.

4.5.3. Robo en Argentina a causa del *phising*

Con la contraseña, los estafadores pudieron comenzar a hacer las transferencias falsas con las que robaron 3,5 millones de pesos al municipio implicado.

4.6. Reputación *online*

4.6.1. Hotel Villa Venecia valorado el mejor de la comunidad de Benidorm

El hecho de que el Hotel fuera considerado el mejor de su comunidad, pudo ayudar a que el establecimiento incrementara su número de reservas al tener una buena reputación. También aumentaron por ello los precios del mismo.

4.6.2. El efecto de la reputación *online* en Tripadvisor

La unidad de consultoría estadística de LMU Múnich junto con otras empresas, midieron cómo reaccionaban los clientes y cómo afectaban a las reservas las críticas de 5 estrellas en Tripadvisor y un ranking más elevado.

Este estudio detectó que una mayor cantidad de críticas de 5 burbujas, un mayor porcentaje de recomendaciones y un ranking mayor, resultaban en mayor cantidad de reservas.

Una mejora del 10% en el ranking de Tripadvisor representó un incremento en las reservas del 4,6% en Europa y hasta un 5,7% en la región Asia-Pacífico. Claramente un mejor ranking incrementó la visibilidad de la propiedad y canalizó mayor cantidad de reservas para el hotel en cuestión.

Asimismo, un mayor porcentaje de opiniones de 5 burbujas tuvo mayor impacto en las reservas que el porcentaje de recomendaciones del hotel en Europa. Pero lo contrario ocurrió en Asia-Pacífico, donde el puntaje promedio influyó en mayor medida que la cantidad de críticas del más alto puntaje.

4.6.3. Ese tuit te puede costar el trabajo

Un uso adecuado de las redes sociales puede ayudar al candidato a mejorar su reputación *online* y ganar muchos puntos a la hora de buscar empleo. En cambio, exponer en las redes opiniones políticas, religiosas, etc. puede provocar que el responsable de realizar un contrato de trabajo escoja a otro candidato para el puesto.

4.7. Ciberdelincuencia

4.7.1. Redes Wifi en aeropuertos y demás lugares públicos

Al conectarse a una red pública, el usuario se expone al robo de información personal y confidencial (claves de cuentas bancarias, correos electrónicos etc.). Los ciberdelincuentes

pueden espiar y secuestrar información de las víctimas, así como instalar virus en los teléfonos móviles, tabletas u ordenadores de los usuarios afectados.

4.7.2. ¿Puede un *hacker* dejar sin luz a Ucrania?

A causa del ciberataque sufrido tuvo lugar un apagón general de luz y electricidad en todo Ucrania. Este afectó a toda la población y comercios y medianas y pequeñas empresas etc. de Ucrania. A su vez afectó y dio acceso a datos de las infraestructuras del país. Se produjo una infiltración de códigos maliciosos en los computadores con el fin de secuestrar información y pedir un rescate a cambio.

4.7.3. Cibercriminales filtran datos de 14.000 tarjetas de crédito en Chile

Los cibercriminales consiguieron acceder a los datos confidenciales de tarjetas de crédito de 14.000 usuarios y filtrarlos. Consiguieron el número de las tarjetas de crédito, el código de seguridad y su fecha de expiración. Con todos esos datos se pudo hacer uso de las cuentas y tarjetas de los usuarios afectados. Estos usuarios perdieron dinero y datos confidenciales. Hubo entonces, una pérdida confianza por parte de las personas que hacen uso del sistema financiero afectado.

4.8. Big data

4.8.1. Cómo Netflix usó el *big data* para crear un éxito

Netflix consiguió convertir en un éxito House Of Cards, la serie exclusiva de esta plataforma. Por tanto, se supo que la serie tenía el éxito asegurado incluso antes de la emisión del primer capítulo.

4.8.2. Cómo reinventar un modelo de negocio

A partir del cálculo de probabilidades, se logró encontrar el mejor precio tanto en vuelos, habitaciones de hoteles etc. Todo ello con el simple hecho de evaluar miles de registros.

4.8.3. La reelección de Obama

Gracias al análisis de todos los datos recogidos de la población estadounidense, se consiguió una optimización de la comunicación y una mejora de la respuesta del electorado. A su vez eso implicó una reducción del malgasto de recursos, tiempo y dinero en los votantes que no eran partidarios de su partido.

5. Soluciones

A continuación, se presentan las soluciones que se han llevado a cabo, así como todas las acciones que deberían o podrían realizarse en cada situación estudiada con el fin de solucionar dicho ataque o riesgo sufrido.

5.1. Suplantación de identidad

5.1.1. Leah Palmer

Ruth Palmer, la víctima, denunció el caso de suplantación de identidad. Aun así, el caso se clasificó como no criminal, con lo que la persona que se hizo pasar por ella no fue condenada. Se debería crear una ley que defienda a la persona afectada y castigue al usuario provocador.

5.1.2. Perfil falso en Facebook

El primer recurso que se llevó a cabo fue cerrar la cuenta falsa. Para solucionar estos casos son necesarias leyes que castiguen al usuario que comete el delito. Si fuera preciso, proporcionar ayuda psicológica a la víctima.

5.1.3. Hombre suplanta la identidad de su mujer

La primera solución que se le dio al caso fue el cierre de la cuenta falsa. Se declaró al responsable de la cuenta falsa como autor de un delito de revelación de secretos y violencia de género.

La existencia de casos de este tipo pone en evidencia la necesidad de una ley que castigue al usuario que comete el delito. De ser necesario, se le daría ayuda psicológica y protección física a la víctima en todo momento.

5.2. Privacidad

5.2.1. *Google Street View*

Antes de realizar grabaciones y fotografías a propiedades privadas, se debe avisar de ello. Es necesario pues, llegar a un acuerdo entre ciudadanos y compañía antes de realizar

captura de imágenes y vídeos. Para reforzar la seguridad de los ciudadanos, se tendrían que difuminar y evitar que se lean matrículas de coches y otros aspectos personales.

5.2.2. Escándalos de privacidad – Facebook

Para que escándalos como éste no ocurran, se recomienda usar la autenticación "doble factor" y evitar contraseñas obvias y repetitivas combinando caracteres, letras y números. Se debe además evitar poner información no estrictamente necesaria.

5.2.3. Datos expuestos por Play Station *Network*

Para que no vuelvan a suceder escándalos como este se recomienda usar la autenticación de doble factor y evitar compartir información no estrictamente necesaria. En cuanto a las contraseñas, se recomienda usar una distinta para cada ocasión (aplicación, página web, etc.), evitar que estas sean obvias y repetitivas, y combinar caracteres, letras y números al escogerlas.

5.3. Cookies

5.3.1. NSA utiliza *cookies* para identificar objetivos a espiar

Si la NSA obtiene información de los usuarios a partir de las *cookies* de Google y las empresas conocen sus movimientos, están legalmente obligadas a denunciarlo.

Para evitar lo ocurrido, se recomienda tomar ciertas medidas sencillas de seguridad como son mantener las aplicaciones actualizadas en todos los dispositivos, evitar tener el localizador activado cuando este no sea estrictamente necesario, tener en cuenta todas las alertas comunicadas por el navegador e instalar un software antivirus y mantenerlo en todo momento. Además, es muy importante ir borrando las *cookies* cada cierto tiempo.

5.3.2. *Cookies* pueden costar dinero

La acción más importante que puede evitar que la página web suba los precios de los vuelos es borrar las *cookies* una vez se haya buscado la información deseada, o utilizar sesiones de navegación privada.

5.3.3. Verizon usa *supercookies* sin consentimiento

El hecho de insertar *supercookies* en las sesiones de navegación de los usuarios de Verizon requirió que los usuarios aceptaran (sin posibilidad al rechazo) que se compartieran sus datos con terceros.

La compañía tuvo que notificar a sus clientes sobre sus programas de publicidad dirigida y, a su vez, que pagar una importante multa.

5.4. Ciberataques

5.4.1. Sony CD Spyware

Dejar de comercializar los discos de Sony con el *rootkit* integrado debería ser la solución más adecuada.

5.4.2. Yahoo sufre ataque *hacker*

Una vez las cuentas de Yahoo fueron *hackeadas*, la solución más efectiva fue restaurar las contraseñas de los usuarios. El objetivo principal de las empresas debería ser garantizar la protección de los usuarios, para que los *hackers* no se vuelvan a encontrar con una brecha en el sistema de seguridad.

5.4.3. Robo digital de cuentas – supermercados Tesco

Tras el ciberataque que afectó 40.000 cuentas e incluso implicó robo de dinero para algunos clientes, el banco se comprometió a cubrir todas las pérdidas por la actividad fraudulenta.

5.5. Phising

5.5.1. Estafa falso abono Mercadona

La OSI (oficina de seguridad internauta) recomienda utilizar Google Alerts para comprobar si se usan los datos personales de forma fraudulenta y contactar con la operadora de telefonía para bloquear los números SMS Premium.

5.5.2. Fraude vales descuentos Zara

Además de las pautas que se comentan para el caso de *phishing* anterior, se recomienda estar informado sobre las últimas amenazas, bien siguiendo en redes sociales a la Policía Nacional y la Guardia Civil, o de forma puntual a las marcas y empresas a las que se refieren en este tipo de reclamos, para comprobar su veracidad. Es importante también utilizar soluciones antivirus en dispositivos móviles y ordenadores, y utilizar los sistemas de autenticación en dos pasos que eviten un sencillo robo de contraseña.

5.5.3. Robo en Argentina a causa del *phishing*

Es necesario y ampliamente recomendable verificar que la página donde se está operando sea la oficial para así evitar cualquier caso de robo, fraudulencia o afectación de datos por parte de páginas web falsas con aspecto similar sino idéntico a la original.

5.6. Reputación *online*

5.6.1. Hotel Villa Venecia valorado el mejor de la comunidad de Benidorm

La formación de personal y el mantenimiento de las instalaciones, así como su restauración a medida que se van deteriorando, es crucial para mantener la posición que se le ha otorgado al hotel e incluso intentar mejorarla.

5.6.2. El efecto de la reputación *online* en Tripadvisor

Tener en cuenta todas las opiniones de los clientes, ayudará a poder mantener o mejorar la reputación *online* del establecimiento. Invertir tiempo en hacer una buena selección del personal según las necesidades y los requerimientos del local afectará positivamente la e-reputación, así como tratar de mantener las instalaciones del establecimiento al nivel que se espera según su calidad.

5.6.3. Ese tuit te puede costar el trabajo

Para tener una buena reputación *online*, es recomendable revisar las publicaciones de las cuentas en los distintos perfiles de Internet y hacer limpieza de ellas, así como eliminar los perfiles que no se utilicen. Una foto de perfil adecuada y la actualización de información siempre que se dé un cambio novedad que se quiera comunicar son de vital importancia. Aun así, hay que tener cuidado con expresar las opiniones en las redes. No debería haber problema con expresarlas siempre y cuando éstas sean respetuosas.

5.7. La ciberdelincuencia

5.7.1. Redes Wifi en aeropuertos y demás lugares públicos

Una de las más importantes sugerencias para evitar ser víctima de un ciberataque como estos es abstenerse, en lo posible, de no conectarse a una de estas redes. Pero si la opción es inevitable, la ESET, compañía de seguridad informática, recomienda verificar que la red a la cual se intenta acceder sea la verídica e intentar no acceder a servicios confidenciales como aplicaciones bancarias o correos electrónicos. Por último, es una buena apuesta

tener instalado un antivirus en el teléfono, para así reducir las posibilidades de ser atacados.

5.7.2. ¿Puede un *hacker* dejar sin luz a Ucrania?

Con tal de evitar que se repitan casos similares, es necesario que las compañías conozcan el caso y estén preparadas para afrontar estas situaciones. Para ello el empleo de antivirus, firewall y copias de seguridad puede ser de gran ayuda.

Es importante mencionar la existencia del Convenio de Budapest o Convenio sobre ciberdelincuencia, cuyo objetivo es hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

5.7.3. Cibercriminales filtran datos de 14.000 tarjetas de crédito en Chile

Una vez los cibercriminales han filtrado los datos de las tarjetas de crédito, se deben bloquear de inmediato las cuentas vinculadas a las tarjetas afectadas. Otras soluciones para evitar que lo ocurrido vuelva a suceder es invertir en ciberseguridad, y aumentar las medidas de seguridad que existen hasta el momento. Tras este incidente en concreto, el Gobierno pidió ayuda al Fondo Monetario Internacional para fortalecer la seguridad informática del sistema financiero.

5.8. Big data

Por lo que hace al apartado de *big data*, este no presenta soluciones. Esto es debido a que los casos tratados son situaciones concretas y muy distintas entre ellas a las que se ha llegado gracias a los avances de las tecnologías de Internet. Se presentan situaciones en las que el uso del *big data* ha permitido causar ciertos cambios en las redes. No obstante, en ningún momento los hechos tratados exigen de soluciones ya que, como se ha comentado, no son casos en que se sufra ataques que deben evitarse o impedir, sino situaciones a las que se ha podido llegar por medio del *big data*.

6. Resumen de soluciones y consecuencias comunes

Una vez analizadas las noticias que se han seleccionado para cada tipo de riesgo, vistas las consecuencias que ha tenido cada escándalo y que medidas se han llevado a cabo para solucionar los problemas causados, se procede a hacer una recopilación de cuales son las consecuencias y soluciones que se pueden sacar en común para cada uno de los tipos de riesgos descritos.

Tipo	Consecuencias comunes	Soluciones comunes
Suplantación de identidad	Información personal difamada sin consentimiento. Fotografías personales difamadas sin consentimiento. Comentarios obscenos e injuriosos haciéndose pasar por la víctima. Afectación de las personas que rodean socialmente a la víctima cuya identidad ha estado suplantada.	Denuncia del caso. Cierre de la cuenta falsa. Ayuda psicológica (si necesario) de la víctima. Necesidad de una ley que castigue al usuario que comete el delito.
Privacidad	Uso y obtención de datos personales de clientes de la empresa afectada. Afectación de los clientes de la	Usar la autenticación “doble factor”. Evitar contraseñas obvias y

	empresa. Afectación de la empresa.	repetitivas. Combinar caracteres, letras y números al escoger contraseñas. Evitar poner información no estrictamente necesaria. Emplear recursos para evitar que se puedan apreciar con claridad aspectos personales como matrículas, códigos etc.
Cookies	Aparición de anuncios y ofertas con objetivos comerciales. Conocimiento de datos como intereses etc. de la persona afectada. Modificación de datos en Internet según tus intereses. Incremento de precios al realizar compras por Internet. Rastreo de los dispositivos del usuario afectado (ubicación, páginas web	Mantener dispositivos actualizados en todas las aplicaciones. No olvidar de ir borrando las *cookies.* Evitar tener localizador activado cuando este no es estrictamente necesario. Usar contraseñas seguras. Evitar el uso de la misma contraseña para todas las páginas web.

	consultadas…)	Tener en cuenta las alertas comunicadas por tu navegador. Instalar software antivirus y mantenerlo en todo momento.
Ciberataques	Se obtienen los datos personales de las personas afectadas. Las personas afectadas pierden dinero.	Dejar de comercializar los discos de Sony con el *rootkit* integrado. Se restauraron las contraseñas de los usuarios. El banco se comprometió a cubrir todas las pérdidas por la actividad fraudulenta.
Phising	Se obtienen datos personales de forma fraudulenta. Se venden los datos personales de las víctimas. Se insertan virus en los dispositivos de las personas afectadas. Las personas afectadas pierden dinero.	Comprobar con Google Alerts si se obtienen datos personales de forma fraudulenta. Bloquear los números SMS Premium. Verificar que la pagina en la que se navega es la oficial. Utilizar soluciones antivirus.
Reputación *online*	Más críticas de 5 estrellas ayudan a obtener mejores rankings en Tripadvisor, y mayores rankings	El punto de partida para tener una reputación *online* impoluta es conocer las necesidades e intereses de nuestro target y plasmar las respuestas en contenidos

	implican más visibilidad y más reservas. Mejorar la reputación *online* permite obtener mas reservas a precios mas altos. Uso adecuado de las redes puede ayudar a un candidato a ganar puntos para conseguir un empleo, o perderlo si es inadecuado.	apropiados y de calidad. Hay que tener en cuenta la opinión que se da a una tercera persona, pues tu trabajo o tu negocio se puede ver afectado. Dar siempre las opiniones de forma respetuosa. Si la reputación es buena intentar mantenerla e incluso mejorarla. Mantener la información lo mas actualizada posible.
Ciberdelincuencia	Acceso a información y datos personales y confidenciales de los ciudadanos y personas afectadas. Espionaje y secuestro de información de las víctimas. Pérdida de confianza hacia el sistema o origen del problema por parte de la sociedad afectada.	- Necesidad de que las compañías y la sociedad conozca el caso. Aumentar las medidas de seguridad y prudencia por parte de los ciudadanos. Incrementar la inversión en ciberseguridad. Emplear antivirus, *firewalls* y copias de seguridad.
Big data	Cada caso presenta consecuencias, no obstante, estas no son comunes ni pueden relacionarse entre ellas. A su vez, el *big data* no presenta soluciones, ya que los	

	casos tratados son unas situaciones concretas muy distintas entre ellas a las que se ha llegado gracias a los avances de las tecnologías de Internet.

Figura 6.1: Tabla resumen de soluciones y consecuencias comunes

7. Leyes que regulan los riesgos en Internet

Todas las leyes relativas a la protección de las personas físicas se encuentran definidas en el Boletín Oficial del Estado (BOE) [49]. Por lo que respecta a este apartado en concreto, su última modificación fue realizada el 27 de abril de 2016. A continuación, se resumen brevemente los apartados que conciernen en mayor medida a este trabajo.

7.1. Leyes en el marco Unión Europea

Las normas de protección de datos de la UE garantizan la protección de los datos personales en todos los casos en que se recojan los mismos: por ejemplo, al comprar por Internet, presentar una solicitud de empleo o pedir un préstamo bancario. Estas normas se aplican tanto a empresas y organizaciones (públicas y privadas) con sede en la UE como a las que tienen su sede fuera de ella y ofrecen bienes y servicios en la UE, como Facebook o Amazon, siempre que dichas empresas soliciten o reutilicen datos personales de ciudadanos de la Unión Europea. [50]

7.1.1. Las normas de protección de datos de la Unión Europea

Las normas de protección de datos de la UE, también conocidas como Reglamento general de protección de datos (RGPD) aprobado en diciembre de 2015, describen las diferentes situaciones en que una empresa o una organización está autorizada para recoger o reutilizar la información personal.

Dichas situaciones son las siguientes:

La celebración de un contrato: por ejemplo, un contrato de suministro de bienes o servicios (es decir, al comprar por Internet) o un contrato de trabajo.

El cumplimiento de una obligación legal: por ejemplo, cuando el tratamiento de tus datos constituye un requisito legal, si el empleador ofrece información sobre tu salario mensual al organismo de seguridad social para que tengas cobertura de la seguridad social.

La protección de tus intereses vitales.

La realización de una tarea pública, en particular todo lo relacionado con las tareas de las administraciones públicas, como escuelas, hospitales, municipios, etc.

Y la satisfacción de intereses legítimos: por ejemplo, si tu banco utiliza tus datos personales para comprobar si puedes optar a una cuenta de ahorros con un tipo de interés más elevado.

En todas las demás situaciones, la empresa u organización debe solicitar una autorización (denominada "consentimiento") antes de poder recoger o reutilizar los datos personales.

7.1.2. Leyes que regulan el uso de *cookies*

Una situación similar es el caso de las *cookies*. Cualquier sitio web que quiera utilizar *cookies* tiene que obtener antes el consentimiento del usuario para instalar una cookie en su ordenador o dispositivo móvil. No está permitido que un sitio web simplemente informe acerca de las *cookies* o explique cómo se pueden desactivar.

Aun así, no todas las *cookies* requieren el consentimiento del usuario. Las *cookies* que se utilizan exclusivamente para efectuar la transmisión de una comunicación no requieren consentimiento. Aquí se incluyen, por ejemplo, las *cookies* que se utilizan para "repartir la carga" (permitiendo que las solicitudes de un servidor web se repartan entre un conjunto de máquinas en lugar de dirigirse a una sola).

Las *cookies* que son estrictamente necesarias para proporcionar un servicio *online* que se ha solicitado expresamente no requieren de consentimiento. Aquí se incluyen, por ejemplo, las *cookies* utilizadas al rellenar un formulario *online* o al usar una cesta de la compra cuando se compra por Internet.

7.1.3. Leyes que regulan los ciberataques y ciberseguridad

En el caso de las de las leyes que regulan los ciberataques, la legislación en materia de ciberseguridad plantea un equilibrio entre los derechos individuales (privacidad o secreto de las comunicaciones) y la efectividad del marco legal con que cuentan las fuerzas de seguridad.

La legislación en el ámbito de la ciberseguridad tiene dos objetivos principales: securizar el ciberespacio (sistemas de información y personas) y proporcionar instrumentos jurídicos efectivos a las autoridades y fuerzas de seguridad para la investigación y persecución de la delincuencia y terrorismo.

La UE presentó la Directiva relativa a la criminalización de ataques contra los sistemas de información (aprobada en agosto de 2013) y la Directiva sobre la Seguridad de las Redes y de la Información (Directiva NIS), aprobada en julio de 2016. La Directiva NIS es el elemento central de la estrategia de ciberseguridad europea. Su objetivo es el de garantizar un nivel mínimo de seguridad en las redes y Sistemas de información utilizados por operadores de servicios esenciales y por proveedores de servicios digitales de Internet.

La Directiva de la Unión Europea (UE) sobre ciberdelincuencia tiene por objeto combatir la ciberdelincuencia y fomentar la seguridad de la información mediante leyes nacionales más estrictas, penas más severas y una mayor cooperación entre las autoridades competentes.

Los principales tipos de infracciones penales que abarca la presente Directiva son los ataques contra los sistemas de información, que van desde ataques de «denegación de servicio», concebidos para dejar fuera de servicio un servidor, hasta la interceptación de datos y ataques de *botnets*.

Para combatir mejor la ciberdelincuencia, la Directiva pide una mayor cooperación internacional entre los servicios encargados de la aplicación de la ley y las autoridades judiciales.

A este fin, los países de la Unión Europea deben: tener un punto de contacto nacional operativo, hacer uso de la red existente de puntos de contacto operativos disponibles veinticuatro horas al día, siete días a la semana, contestar en el plazo de ocho horas a las solicitudes urgentes de ayuda para indicar si se dará una respuesta y cuándo puede darse y recoger datos estadísticos sobre ciberdelincuencia.

7.2. Leyes en el marco Español

Por lo que hace al caso concreto de España, existen dos leyes principales que regulan la privacidad. Estas son la Ley Orgánica de protección de Datos Personales (LOPD) y la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).

7.2.1. Ley Orgánica de protección de Datos Personales

La LOPD establece el régimen jurídico aplicable al tratamiento de datos de carácter personal y las condiciones en las que se deben recoger, tratar o ceder dichos datos para no infringir los derechos fundamentales y las libertades públicas de los ciudadanos. [51]

7.2.2. Ley de Servicios de la Sociedad de la Información y Comercio Electrónico

La LSSI establece las obligaciones a cumplir en caso de tener una página web o una tienda *online* encaminadas a proteger los derechos de los consumidores. Entre ellas están las de redactar un Aviso legal, Política de Privacidad y Política de *Cookies*. [51]

8. Impacto ambiental

Por lo que respecta a este proyecto, es necesario remarcar que no tiene en sí un gran impacto ambiental, al tratarse de un trabajo puramente de investigación y búsqueda de artículos.

No obstante, si que puede considerarse que el tiempo empleado para la búsqueda de información y artículos ha sido primordialmente realizado a través de la red de Internet. Esta consume gran cantidad de energía, ya sea por medio de ordenadores, teléfonos móviles, tabletas, etc. A su vez el trabajo debe ser impreso, el gasto de papel es un hecho que no podemos obviar dada la gran extensión de páginas que el proyecto contiene.

Finalmente, por el hecho de ser un trabajo conjunto, es decir, realizado por parejas, ha sido necesario concretar reuniones entre los miembros del proyecto para poner en común ideas y trabajar conjuntamente en múltiples ocasiones. Para ello se ha tenido que utilizar transporte (público y privado) que ha ocasionado gasto energético, de gasolina y, por lo tanto, que ha generado contaminación ambiental.

9. Planificación del trabajo

En la figura 9.1 se muestra el diagrama de Gantt correspondiente a la planificación de este trabajo.

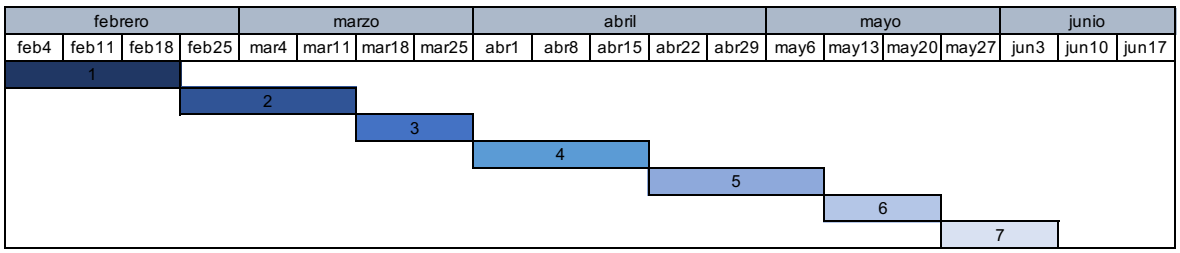

Figura 9.1: Diagrama de Gantt de la planificación del trabajo de fin de grado

Cada punto corresponde a una fase del proyecto:

1. Análisis de artículos relacionados con los riesgos de Internet.
2. Análisis de noticias y escándalos relacionados con riesgos de Internet.
3. Clasificación de las noticias según los tipos de riesgos.
4. Análisis de consecuencias y soluciones de cada noticia.
5. Búsqueda de soluciones y consecuencias comunes.
6. Análisis de leyes que afectan en el tema.
7. Redacción y conclusiones.

10. Presupuesto

En este apartado se contabilizarán las horas dedicadas al proyecto juntamente con el valor económico del trabajo realizado por los miembros de este trabajo de fin de grado.

Se computan todas las horas que se han dedicado a la redacción del trabajo, así como a la búsqueda de información, análisis de datos, estudio de artículos, etc. Es por ello, que se concluye que cada una de nosotras ha dedicado alrededor de 300 horas en la elaboración del trabajo. Teniendo en cuenta nuestros honorarios (20 €/hora) y que el total de horas dedicadas son 600, el presupuesto de elaboración de este proyecto asciende a 12000 €.

En la siguiente tabla se detallan los costes según las fases del proyecto.

Tareas	Precio/hora	Berta de Moragas (horas)	Carla Pascual (horas)	Total horas	Total precio
Análisis de artículos	20 €	50	50	100	2.000 €
Análisis de noticias	20 €	50	50	100	2.000 €
Clasificación de las noticias	20 €	33	33	66	1.320 €
Análisis de consecuencias y soluciones	20 €	50	50	100	2.000 €
Búsqueda de soluciones y consecuencias comunes	20 €	50	50	100	2.000 €
Análisis de leyes	20 €	33	33	66	1.320 €
Redacción y conclusiones	20 €	34	34	68	1.360 €
TOTAL	Variable	300	300	600	12.000 €

Figura 10.1: Tabla del presupuesto del proyecto

11. Conclusiones

Cualquier acción realizada en la red se transforma de inmediato en pública. Esta premisa que parece simple, no lo es, porque además de ser inmediatamente visible, cada uno de nuestros actos va construyendo nuestra marca personal o de empresa. Es realmente importante tomar conciencia de la importancia de prestar atención a todo lo que publicamos en las redes.

Y, aunque existen medidas de seguridad que intentan cubrir todos y cada uno de los riesgos a los que el mundo esta expuesto, se ha podido demostrar que estas todavía son muy escasas. Es decir, los gobiernos, los países y empresas deben buscar e investigar nuevos métodos más sofisticados y eficientes.

A su vez, las propias leyes no siempre actúan como deberían, es decir, no siempre actúan como lo esperado en el caso de, por ejemplo, suplantación de identidad. Por ello un llamamiento a estudiar e intentar modificar y re aprobar leyes para el buen funcionamiento y defensa de la sociedad es de mayor importancia.

Tras definir y conocer las soluciones que se les puede dar a cada una de las problemáticas y riesgos que el uso de las tecnologías de internet implica, nos hemos dado cuenta de que aun y existiendo acciones o mejor dicho recomendaciones que nos pueden ayudar a evitar dichos conflictos, estas no nos permiten atacar los problemas de raíz. Es decir, sí podemos intentar prevenir situaciones como las descritas a lo largo del trabajo, pero la amplitud y profundidad que abarca el mundo de la tecnología hace que sea de gran dificultad poder controlar y encontrar solución 100% efectiva a todos y cada uno de los posibles ataques que se pueden generar.

Por ello y sintetizando todas las soluciones anteriores, recomendamos y creemos que actualmente es de mayor eficiencia tener precaución con los enlaces que recibimos o a los que somos redirigidos diariamente y son de dudosa procedencia, ya que podrían tener amenazas informáticas. También es necesario tener cuidado con las actualizaciones que exigen o piden ciertas aplicaciones ya que algunas no son necesarias para el funcionamiento de las mismas y podrían debilitar la seguridad informática de nuestros dispositivos. Es recomendable configurar de forma segura nuestra privacidad, así como intentar introducir la mínima información personal posible en las redes. No añadir usuarios desconocidos a las redes sociales y usar contraseñas seguras, es decir, que sean diferentes para cada uno de los lugares web y que, a su vez, sean no predecibles puede ser una barrera de protección más ante ataques informáticos. Por último, no dudar en denunciar cualquier caso en el que

nuestra seguridad se vea afectada es de vital importancia.

11.1. ¿De qué nos ha servido el grado para el trabajo?

Cabe mencionar que este trabajo de fin de grado no es un proyecto dichamente técnico como muchos podrían esperarse tras haber cursado el grado de ingeniería en tecnologías industriales. Este proyecto se ha basado en un proceso de mucha búsqueda y un largo análisis y clasificación de información.

Consideramos que el perfil técnico que tenemos ambas se ha visto reflejado en la manera como hemos organizado y analizado cada uno de los artículos y noticias. Como primer recurso para poder analizar, comparar y clasificar datos e información se ha usado Microsoft Excel, ya que el uso de tablas (recurso mucho más técnico que una redacción) nos ha permitido estructurar todo el contenido de forma concisa y precisa.

Creemos que ha sido en ese aspecto donde se ha visto reflejado nuestro estudio en el grado de ingeniería cursado y se ha plasmado el perfil técnico que nos define. Con los cuatro años de estudios hemos aprendido a sintetizar y estructurar ideas y así lo hemos reflejado a la hora de analizar y extraer la información más importante de cada uno de los casos y sucesos tratados.

Bibliografía

[1] Gobiernodecanarias [en línea]. Canarias: [Consulta 15/05/2019]. Disponible en <http://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/suplantacion-identidad/>

[2] Enciclopèdia [en línea]. [Consulta 30/05/2019] Disponible en <https://www.enciclopedia.cat/EC-GDLC-e00176859.xml >

[3] Claxon Express [en línea]. [Consulta 20/05/2019] Disponible en <https://claxonpress.com/mas-informacion-sobre-las-cookies/>

[4] Caser [en línea]. [Consulta 07/03/2019] Disponible en <https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos>

[5] Gobierno de canarias [en línea]. Canarias: [Consulta 15/05/2019]. Disponible en <http://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/phishing/>

[6] Cyberclick [en línea]: 31/03/2019 [Consulta 15/04/2019]. Disponible en <https://www.cyberclick.es/numerical-blog/reputacion-online-que-es-y-como-cuidarla>

[7] Sistemius [en línea]: A Coruña, 02/12/2018. [Consulta 16/05/2019]. Disponible en <https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos.html>

[8] Powerdata [en línea]: España [Consulta 11/04/2019]. Disponible en <https://www.powerdata.es/big-data>

[9] Avast [en línea]: [Consulta 30/05/2019]. Disponible en <https://www.avast.com/es-es/c-rootkit >

[10] Tripadvisor [en línea]: [Consulta 30/05/2019]. Disponible en <https://tripadvisor.mediaroom.com/es-about-us>

[11] Real Academia Española [en línea]. España. Disponible en <https://dle.rae.es/?id=LvskgUG>

[12] Real Academia Española [en línea]. España. Disponible en <https://dle.rae.es/?id=WT8tAMI>

[13] Real Academia Española [en línea]. España. Disponible en <https://dle.rae.es/?id=VXs6SD8>

[14] La Enciclopèdia [en línea]. [Consulta 28/05/2019]. Disponible en <https://www.enciclopedia.cat/EC-GEC-0517644.xml >

[15] Google [en línea]. [Consulta 07/03/2019] Disponible en <https://www.google.com/streetview/#!/ (07/03/2019)>

[16] Verizon [en línea]. [Consulta 20/05/2019]. Disponible en <https://www.verizon.com/about/our-company/history-and-timeline >

[17] Apple [en línea]. [Consulta 28/05/2019]. Disponible en <https://support.apple.com/es-es/HT204915>

[18] Real Academia Española [en línea]. España. Disponible en <https://dle.rae.es/?id=buVODur>

[19] Roble [en línea]. [Consulta 21/03/2019] Disponible en <http://roble.pntic.mec.es/jprp0006/tecnologia/4eso_informatica/peligros_Internet/0peligros_Internet.htm>

[20] Kaspersky [en línea]. Madrid: 25/04/2013 [Consulta 02/05/2019] Disponible en <https://www.kaspersky.es/blog/que-es-un-botnet/755/>

[21] Mohamed Abomhara y Geir M. Køien, 2015, Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Vol. 4. [Consulta 04/06/2019]. Disponible en: <https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4#rsec2.3.5>

[22] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, Sara Kiesler, 2015, My Data Just Goes Everywhere-User Mental Models of the Internet and Implications for Privacy and Security, Usenix. Pittsburgh, PA:. [Consulta 05/06/2019]. Disponible en: <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf>

[23] Ankalarao Konakalla1, Bhavani Veeranki2 , 2013, Evolution of Security Attacks and Security Technology, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 11. [Consulta 09/06/2019]. Disponible en: <https://ijcsmc.com/docs/papers/November2013/V2I11201366.pdf>

[24] Colin Tankard, 2015, The security issues of the Internet of Things. Computer Fraud & Security. [Consulta 09/06/2019]. Disponible en: <http://bayanbox.ir/view/5510623574700797444/rahpu.ir-TNC98.pdf>

[25] theargus [en línea]. United Kingdom: Ben Leo, 28/02/2015. [Consulta 20/02/2019]. Disponible en

<https://www.theargus.co.uk/news/11824900.You_ve_stolen_my_life__Brighton_woman_tells_shocking_story_of_online__catfish__impersonator/?ref=mr>

[26] El Mundo [en línea]. Granada, Andalucía: José A. Cano, 25/06/2013. [Consulta 20/02/2019]. Disponible en: <https://www.elmundo.es/elmundo/2013/06/25/andalucia/1372180481.html>

[27] ABC [en línea]. Granada, Andalucía: José A. Cano, 25/06/2013. [Consulta 20/02/2019]. Disponible en <https://www.abc.es/espana/galicia/abci-suplanta-identidad-amante-Internet-para-rapten-y-violen-201810301122_noticia.html>

[28] Infobae [en línea]. Argentina: [Consulta 21/03/2019]. Disponible en: <https://www.infobae.com/2013/03/12/700622-google-llego-un-acuerdo-el-escandalo-street-view/>

[29] El País [en línea]: [Consulta 21/02/2019]. Disponible en <https://www.elpais.com.uy/vida-actual/claves-entender-escandalo-politico-facebook-cambridge-analytica.html >

[30] El País [en línea]: París: Marc Bassets, 05/09/2017. [Consulta 12/03/2019]. Disponible en <https://elpais.com/internacional/2017/09/05/actualidad/1504593518_526226.html>

[31] ABC [en línea]: Sevilla: Anónimo, 11/12/2013. [Consulta 22/02/2019]. Disponible en <https://www.abc.es/tecnologia/20131211/abci-google-cookies-201312111019.html >

[32] The Guardian [en línea]. Patrick Collinson. Inglaterra. [Consulta 20/02/2019]. Disponible en: <https://www.theguardian.com/money/blog/2010/aug/07/computer-cookies-booking-online >.

[33] We live security [en línea]. Kyle Ellison. [Consulta 20/02/2019]. Disponible en: <https://www.welivesecurity.com/la-es/2016/03/09/verizon-multada-supercookies/>.

[34] The New York Times [en línea]. Estados unidos: Dan Mitchell. [Consulta 21/02/2019]. Disponible en: <https://www.nytimes.com/2005/11/19/business/media/the-rootkit-of-all-evil.html>.

[35] El País Economía [en línea]. Madrid, España: Anónimo. [Consulta 21/02/2019]. Disponible en: <https://cincodias.elpais.com/cincodias/2016/09/22/empresas/1474556439_747931.html>.

[36] ABC Economía [en línea]. Sevilla, España: Luis Ventoso.[Consulta 21/02/2019]. Disponible en: <https://www.abc.es/economia/abci-robo-digital-cuentas-20000-clientes-banco-supermercados-tesco-201611071228_noticia.html>.

[37] ABC Comunidad [en línea]. Valencia, España: Anónimo. .[Consulta 19/02/2019]. Disponible en:< https://www.abc.es/espana/comunidad-valenciana/abci-guardia-civil-y-mossos-alertan-nueva-estafa-falso-bono-mercadona-201901140841_noticia.html>.

[38] ABC Redes [en línea]. Sevilla, España: Ana I. Martínez. [Consulta 19/02/2019]. Disponible en: <https://www.abc.es/tecnologia/redes/abci-whatsapp-regresa-fraude-vales-descuento-zara-201609051749_noticia.html>

[39] We Live Security [en línea]: Sabrina Pagnotta, 07/08/2017. [Consulta 20/02/2019]. Disponible en <https://www.welivesecurity.com/la-es/2017/08/07/confirman-phishing-robo-argentina/>

[40] Diarioinformacion [en línea]: 29/01/2016. [Consulta 31/03/2019]. Disponible en <https://www.diarioinformacion.com/benidorm/2016/01/29/villa-venecia-hotel-benidorm-mejor/1721656.html>

[41] Inteli hoteles [en línea]. 27/11/2015. [Consulta 31/03/2019]. Disponible en <http://intelihoteles.com/el-efecto-de-la-reputacion-online-en-tripadvisor/>

[42] La opinión de Málaga [en línea]. Málaga: David Navarro, 23/02/2016. [Consulta 2/04/2019]. Disponible en <https://www.laopiniondemalaga.es/finanzas-personales/2016/02/23/tuit-costar-trabajo/831039.html>

[43] El espectador [en línea]: España: Diego Ojeda, 26/07/2018. [Consulta 2/04/2019]. Disponible en < https://www.elespectador.com/tecnologia/cuidado-con-las-redes-wifi-en-aeropuertos-y-demas-lugares-publicos-articulo-802617>

[44] El espectador [en línea]: España: Diego Ojeda, 22/11/2017. [Consulta 2/04/2019]. Disponible en <https://www.elespectador.com/tecnologia/los-posibles-ataques-informaticos-detras-del-caso-uber-articulo-724604>

[45] Ecommerce news [en línea]: España: Vicente Ramirez, 17/04/2017. [Consulta 11/04/2019]. Disponible en <https://ecommerce-news.es/hause-of-cards-y-el-big-data-58199>

[46] Expansión [en línea]: Madrid, España: Elena Arrieta, 28/10/2015. [Consulta 11/04/2019]. Disponible en <http://www.expansion.com/economia-digital/innovacion/2015/10/28/5630a18022601d44628b4616.html>

[47] BBVA [en línea]: España: 12/04/2018. [Consulta 11/04/2019]. Disponible en <https://www.bbva.com/es/ejemplos-reales-uso-big-data/>

[48] El tiempo [en línea]: España: Con Agencias, 27/07/2018 [Consulta 25/04/2019]. Disponible en <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/filtracion-de-datos-de-tarjetas-de-credito-en-chile-248540>

[49] PuroMarketing [en línea]: 21/01/2012 [Consulta 01/04/2019]. Disponible en: <https://www.puromarketing.com/10/12031/consecuencias-reputacion-online-gestionada-pueden-irreparables.html>

[50] Boletín Oficial del Estado [en línea]: 27/04/2016. [Consulta 30/05/2019]. Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

[51] Europa [en línea]: 24/01/2019. [Consulta 20/04/2019]. Disponible en: <https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_es.htm>

[52] Ley de protección datos [en línea]: [Consulta 20/05/2019]. Disponible en: <https://ayudaleyprotecciondatos.es/2016/10/21/privacidad-internet-redes-sociales/>